ID: 553271
Sample Name: kGl1qp3Ox8.exe
Cookbook: default.jbs
Time: 15:30:16
Date: 14/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report kGl1qp3Ox8.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 5
Yara Overview 5
Dropped Files 5
Memory Dumps 6
Unpacked PEs 6
Sigma Overview 7
System Summary: 7
Jbx Signature Overview 7
AV Detection: 7
Networking: 7
Key, Mouse, Clipboard, Microphone and Screen Capturing: 7
E-Banking Fraud: 7
System Summary: 7
Data Obfuscation: 7
Persistence and Installation Behavior: 8
Malware Analysis System Evasion: 8
Anti Debugging: 8
Lowering of HIPS / PFW / Operating System Security Settings: 8
Stealing of Sensitive Information: 8
Remote Access Functionality: 8
Mitre Att&ck Matrix 8
Behavior Graph 9
Screenshots 10
Thumbnails 10
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 11
Unpacked PE Files 11
Domains 13
URLs 13
Domains and IPs 14
Contacted Domains 14
URLs from Memory and Binaries 14
Contacted IPs 14
Public 14
Private 14
General Information 14
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASN 15
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
Static File Info 48
General 48
File Icon 48
Static PE Info 48
General 48
Entrypoint Preview 48
Data Directories 48
Sections 48
Resources 49
Imports 49
Version Infos 49
Possible Origin 49
Network Behavior 49
Code Manipulations 49
Statistics 49
Behavior 49
System Behavior 49
Analysis Process: kGl1qp3Ox8.exe PID: 6940 Parent PID: 2940 49
General 49
File Activities 50

File Created 50
File Deleted 50
File Written 50
File Read 50
Registry Activities 50
Key Value Created 50
Analysis Process: NNNBSubeVPxRXeeZnGu7gQkK.exe PID: 2468 Parent PID: 6940 50
General 50
File Activities 50
File Created 50
File Written 50
Analysis Process: kXM34tDnyQtIWwfvEKDMhvoQ.exe PID: 5892 Parent PID: 6940 50
General 50
File Activities 51
File Created 51
File Written 51
File Read 51
Registry Activities 51
Analysis Process: DFhRro1WrdTF3ZDuGSOCgEWZ.exe PID: 5124 Parent PID: 6940 51
General 51
File Activities 51
File Created 51
File Read 51
Analysis Process: eULKoZpb_80D8HrRwSiJF82y.exe PID: 5184 Parent PID: 6940 51
General 51
File Activities 51
File Created 51
File Written 52
File Read 52
Registry Activities 52
Analysis Process: gw2BglocGXw_yTn_uJ3zXLrN.exe PID: 5480 Parent PID: 6940 52
General 52
File Activities 52
Registry Activities 52
Key Created 52
Key Value Created 52
Analysis Process: VxkVtHpwGFsrs3Al2PFI1pOG.exe PID: 5524 Parent PID: 6940 52
General 52
Analysis Process: XzPWSUxlao64h10K0Z7pfPtI.exe PID: 4760 Parent PID: 6940 52
General 53
Analysis Process: P65Nqt8GfRApLpFwJ9bOb7YH.exe PID: 4928 Parent PID: 6940 53
General 53
Analysis Process: fyqi7uQSxz8XM3xkvrctriED.exe PID: 6000 Parent PID: 6940 53
General 53
Analysis Process: e5SEitbuPomqfmRpQ1nXQBM2.exe PID: 5968 Parent PID: 6940 53
General 53
Analysis Process: _Phvk0uQfXOn269qFdHTiuOG.exe PID: 6596 Parent PID: 6940 54
General 54
Analysis Process: JiryxVDn0P_ka7w2xP8PdulD.exe PID: 6640 Parent PID: 6940 54
General 54
Analysis Process: Ne0JuwDw1Qp0B7KETuyFd5jI.exe PID: 5192 Parent PID: 6940 54
General 54
Analysis Process: 56lWdY4eqRTdJgfAC3WHYY1z.exe PID: 5860 Parent PID: 6940 55
General 55
Analysis Process: sCI8qb6amvGp4AhJGUUX5nQx.exe PID: 6096 Parent PID: 6940 55
General 55
Analysis Process: dce6bd67-7e1f-466b-94f1-f9f5c2acf9dd.exe PID: 4148 Parent PID: 5892 56
General 56
Analysis Process: svchost.exe PID: 1040 Parent PID: 560 56
General 56
Analysis Process: P65Nqt8GfRApLpFwJ9bOb7YH.tmp PID: 580 Parent PID: 4928 56
General 56
Analysis Process: powershell.exe PID: 3832 Parent PID: 6596 57
General 57
Analysis Process: conhost.exe PID: 4868 Parent PID: 3832 57
General 57
Analysis Process: explorer.exe PID: 3440 Parent PID: 5524 57
General 57
Analysis Process: 4c91d8e5-f330-473d-bea7-49691b483a08.exe PID: 6828 Parent PID: 5892 58
General 58
Analysis Process: 01913ed7-c54a-4682-ba7f-2339dfb12dae.exe PID: 644 Parent PID: 5184 58
General 58
Analysis Process: SiJXWwfMYK4L8VTC7HncQkab.exe PID: 3640 Parent PID: 6940 58
General 58
Analysis Process: 0y_alCQBJv4J1LDnCOe55cop.exe PID: 5100 Parent PID: 6940 59
General 59
Analysis Process: C1aYSYmMy9tQLrifaCN41EQ8.exe PID: 3556 Parent PID: 6940 59
General 59
Analysis Process: NhzjvwxrwXd3QBEl8Ly0lN5e.exe PID: 1316 Parent PID: 6940 59
General 59
Analysis Process: nnaUz9XFoo0RBkjZ4wuMqrTl.exe PID: 6632 Parent PID: 6940 60
General 60
Analysis Process: _____djskjT76(((.exe PID: 4460 Parent PID: 580 60
General 60
Disassembly 60
Code Analysis 60

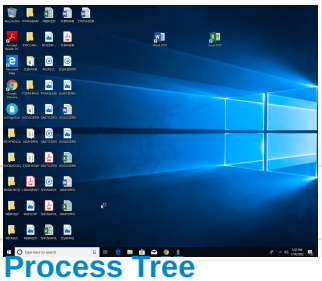
Windows Analysis Report kGl1qp3Ox8.exe

Overview

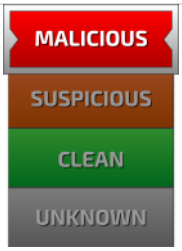
General Information

Sample Name:	kGl1qp3Ox8.exe
Analysis ID:	553271
MD5:	7ebf41b7e0d2447.
SHA1:	6e9c110ed531f72.
SHA256:	15cea3c23e9d0f1..
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection



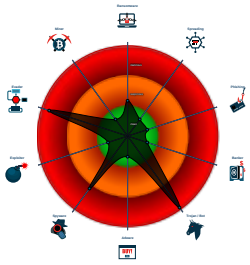
RedLine SmokeLoader Vidar onlyLogger

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

Signatures

- Yara detected RedLine Stealer
- Yara Genericmalware
- Yara detected SmokeLoader
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for subm…
- Yara detected onlyLogger
- Antivirus / Scanner detection for sub…
- Yara detected Vidar stealer
- Multi AV Scanner detection for dropp…
- Disable Windows Defender real time…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- kGl1qp3Ox8.exe (PID: 6940 cmdline: "C:\Users\user\Desktop\kGl1qp3Ox8.exe" MD5: 7EBF41B7E0D24473F2AD0B25E354F615)
  - NNNBSubeVPxRXeeZnGu7gQkK.exe (PID: 2468 cmdline: "C:\Users\user\Pictures\Adobe Films\NNNBSubeVPxRXeeZnGu7gQkK.exe" MD5: 3F22BD82EE1B38F439E6354C60126D6D)
  - kXM34tDnyQtIWwfvEKDMhvoQ.exe (PID: 5892 cmdline: "C:\Users\user\Pictures\Adobe Films\kXM34tDnyQtIWwfvEKDMhvoQ.exe" MD5: 0C70224F09C65619BC9D6AFC456294C9)
    - dce6bd67-7e1f-466b-94f1-f9f5c2acf9dd.exe (PID: 4148 cmdline: "C:\Users\user\AppData\Local\Temp\dce6bd67-7e1f-466b-94f1-f9f5c2acf9dd.exe" MD5: 748DBD76B3D32F174DEBD3BD296A2C4D)
    - svchost.exe (PID: 1040 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
    - 4c91d8e5-f330-473d-bea7-49691b483a08.exe (PID: 6828 cmdline: "C:\Users\user\AppData\Local\Temp\4c91d8e5-f330-473d-bea7-49691b483a08.exe" MD5: 309F89D4E7F28E93B0CB02D7A5806F6C)
    - 70bb7193-ad9a-4e0f-ae94-6f57b7571a61.exe (PID: 1040 cmdline: "C:\Users\user\AppData\Local\Temp\70bb7193-ad9a-4e0f-ae94-6f57b7571a61.exe" MD5: 978137D4F66C79D0EC1B931A7BE4BC63)
  - DFhRro1WrdTF3ZDuGSOCgEWZ.exe (PID: 5124 cmdline: "C:\Users\user\Pictures\Adobe Films\DFhRro1WrdTF3ZDuGSOCgEWZ.exe" MD5: DDFE3C0D174EC565750DCACEF9A52363)
  - eULKoZpb_80D8HrRwSiJF82y.exe (PID: 5184 cmdline: "C:\Users\user\Pictures\Adobe Films\eULKoZpb_80D8HrRwSiJF82y.exe" MD5: A9DED7D6470F741B9F4509863665F74C)
    - 01913ed7-c54a-4682-ba7f-2339dfb12dae.exe (PID: 644 cmdline: "C:\Users\user\AppData\Local\Temp\01913ed7-c54a-4682-ba7f-2339dfb12dae.exe" MD5: 9734ED168A74A29DC30C2273FE7AEDDC)
    - a8155a24-6afe-4a8d-b55c-3e9f9c8f0596.exe (PID: 5804 cmdline: "C:\Users\user\AppData\Local\Temp\a8155a24-6afe-4a8d-b55c-3e9f9c8f0596.exe" MD5: 87487BB57FA27A114D4569F951F532AC)
  - gw2BglocGXw_yTn_uJ3zXLrN.exe (PID: 5480 cmdline: "C:\Users\user\Pictures\Adobe Films\gw2BglocGXw_yTn_uJ3zXLrN.exe" MD5: 0162C08D87055722BC49265BD5468D16)
  - VxkVtHpwGFsrs3Al2PFI1pOG.exe (PID: 5524 cmdline: "C:\Users\user\Pictures\Adobe Films\VxkVtHpwGFsrs3Al2PFI1pOG.exe" MD5: 61931A7DE1769BC844394F161F1DE150)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - XzPWSUxlao64h10K0Z7pfPtI.exe (PID: 4760 cmdline: "C:\Users\user\Pictures\Adobe Films\XzPWSUxlao64h10K0Z7pfPtI.exe" MD5: 6D87BD5B6C8585B0FECB45BAD7F3D92B)
  - P65Nqt8GfRApLpFwJ9bOb7YH.exe (PID: 4928 cmdline: "C:\Users\user\Pictures\Adobe Films\P65Nqt8GfRApLpFwJ9bOb7YH.exe" MD5: 3A9664DAD384F41DCDC1272ED31171E0)
    - P65Nqt8GfRApLpFwJ9bOb7YH.tmp (PID: 580 cmdline: "C:\Users\user\AppData\Local\Temp\is-FNG8T.tmp\P65Nqt8GfRApLpFwJ9bOb7YH.tmp" /SL5="$C03EA, 312591,228864,C:\Users\user\Pictures\Adobe Films\P65Nqt8GfRApLpFwJ9bOb7YH.exe" MD5: 7FC94D54F886839996FB02FBBE1B42C8)
      - _____djskjT76(((.exe (PID: 4460 cmdline: "C:\Users\user\AppData\Local\Temp\is-MBHBG.tmp_____djskjT76(((.exe" /S /UID=2710 MD5: 16B30C7902FC1B0A34744C95A64E332B)
  - fyqi7uQSxz8XM3xkvrctriED.exe (PID: 6000 cmdline: "C:\Users\user\Pictures\Adobe Films\fyqi7uQSxz8XM3xkvrctriED.exe" MD5: 7A14B5FC36A23C9FF0BAF718FAB093CB)
    - D9C.tmp.exe (PID: 3980 cmdline: "C:\Users\user\AppData\Roaming\D9C.tmp.exe" MD5: 8C0449C168C009C9DC860902E0F1CA66)
  - e5SEitbuPomqfmRpQ1nXQBM2.exe (PID: 5968 cmdline: "C:\Users\user\Pictures\Adobe Films\e5SEitbuPomqfmRpQ1nXQBM2.exe" MD5: 3ECFD5D9F991294510E111DCF96357FD)
  - _Phvk0uQfXOn269qFdHTiuOG.exe (PID: 6596 cmdline: "C:\Users\user\Pictures\Adobe Films_Phvk0uQfXOn269qFdHTiuOG.exe" MD5: DECA67F083AE99A6BB5E9F8E8F31550C)
    - powershell.exe (PID: 3832 cmdline: PowerShell Get-MpComputerStatus MD5: 95000560239032BC68B4C2FDFCDEF913)
      - conhost.exe (PID: 4868 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - JiryxVDn0P_ka7w2xP8PdulD.exe (PID: 6640 cmdline: "C:\Users\user\Pictures\Adobe Films\JiryxVDn0P_ka7w2xP8PdulD.exe" MD5: 5348327DE92D40720D25952A88613986)
  - Ne0JuwDw1Qp0B7KETuyFd5jI.exe (PID: 5192 cmdline: "C:\Users\user\Pictures\Adobe Films\Ne0JuwDw1Qp0B7KETuyFd5jI.exe" MD5: 3A6EBD3377AFDB9EFC2195E7B6A00A69)
  - 56lWdY4eqRTdJgfAC3WHYY1z.exe (PID: 5860 cmdline: "C:\Users\user\Pictures\Adobe Films\56lWdY4eqRTdJgfAC3WHYY1z.exe" MD5: D08898F15B9373D16001E84A320628E5)
  - sCI8qb6amvGp4AhJGUUX5nQx.exe (PID: 6096 cmdline: "C:\Users\user\Pictures\Adobe Films\sCI8qb6amvGp4AhJGUUX5nQx.exe" MD5: 503A913A1C1F9EE1FD30251823BEAF13)
  - SiJXWwfMYK4L8VTC7HncQkab.exe (PID: 3640 cmdline: "C:\Users\user\Pictures\Adobe Films\SiJXWwfMYK4L8VTC7HncQkab.exe" MD5: DD3C57E2520A47D634E5FAAC52782FDA)
  - 0y_alCQBJv4J1LDnCOe55cop.exe (PID: 5100 cmdline: "C:\Users\user\Pictures\Adobe Films\0y_alCQBJv4J1LDnCOe55cop.exe" MD5: 3ECFD5D9F991294510E111DCF96357FD)
  - C1aYSYmMy9tQLrifaCN41EQ8.exe (PID: 3556 cmdline: "C:\Users\user\Pictures\Adobe Films\C1aYSYmMy9tQLrifaCN41EQ8.exe" MD5: 2DBF77866712D9EBD57EC65E7C1598A8)
  - NhzjvwxrwXd3QBEl8Ly0lN5e.exe (PID: 1316 cmdline: "C:\Users\user\Pictures\Adobe Films\NhzjvwxrwXd3QBEl8Ly0lN5e.exe" MD5: 67848A34646ADF30BCC92518C0AE1BD1)
  - nnaUz9XFoo0RBkjZ4wuMqrTl.exe (PID: 6632 cmdline: "C:\Users\user\Pictures\Adobe Films\nnaUz9XFoo0RBkjZ4wuMqrTl.exe" MD5: FAB86F0D2562E6CD30D8CBC915A05ECC)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\11111.exe	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
C:\Users\user\Documents\Ei8DrAmaYu9K8ghN89CsjOW1.dll	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x16591c:$xo1: \xD0\x9D\xF2\x9D\xE7\x9D\xF4\x9D\xF1\x9D\xF1\x9D\xFC\x9D\xB2\x9D\xA8\x9D\xB3\x9D\xAD\x9D • 0x167754:$xo1: \xD0\xF2\xE7\xF4\xF1\xF1\xFC\xB2\xA8\xB3\xAD
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\PL_Client[1].bmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x16591c:$xo1: \xD0\x9D\xF2\x9D\xE7\x9D\xF4\x9D\xF1\x9D\xF1\x9D\xFC\x9D\xB2\x9D\xA8\x9D\xB3\x9D\xAD\x9D • 0x167754:$xo1: \xD0\xF2\xE7\xF4\xF1\xF1\xFC\xB2\xA8\xB3\xAD
C:\Users\user\Pictures\Adobe Films\SiJXWwfMYK4L8VTC7HncQkab.exe	JoeSecurity_Generic_malware	Yara Generic_malware	Joe Security	
C:\Users\user\Pictures\Adobe Films\SiJXWwfMYK4L8VTC7HncQkab.exe	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
Click to see the 2 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
0000001D.00000000.569672179.00007FF65A410000.00000002.00020000.sdmp	JoeSecurity_Generic_malware	Yara Generic_malware	Joe Security	
00000012.00000000.573252466.000000000670000.00000040.00000001.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x3c860:$xo1: cATGBBO\x01\x1B\x1E
00000012.00000000.573252466.000000000670000.00000040.00000001.sdmp	JoeSecurity_onlyLogger	Yara detected onlyLogger	Joe Security	
00000009.00000003.518327651.00000000020E0000.00000004.00000001.sdmp	JoeSecurity_onlyLogger	Yara detected onlyLogger	Joe Security	
0000001D.00000000.547428729.00007FF65A410000.00000002.00020000.sdmp	JoeSecurity_Generic_malware	Yara Generic_malware	Joe Security	
Click to see the 26 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.3.kGl1qp3Ox8.exe.4157b9e.151.unpack	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x41a:$x1: https://cdn.discordapp.com/attachments/ • 0x4da:$x1: https://cdn.discordapp.com/attachments/ • 0x59a:$x1: https://cdn.discordapp.com/attachments/ • 0x65a:$x1: https://cdn.discordapp.com/attachments/ • 0x71a:$x1: https://cdn.discordapp.com/attachments/ • 0x7da:$x1: https://cdn.discordapp.com/attachments/ • 0x89a:$x1: https://cdn.discordapp.com/attachments/ • 0x95a:$x1: https://cdn.discordapp.com/attachments/ • 0xa1a:$x1: https://cdn.discordapp.com/attachments/ • 0xada:$x1: https://cdn.discordapp.com/attachments/ • 0xb9a:$x1: https://cdn.discordapp.com/attachments/ • 0xc5a:$x1: https://cdn.discordapp.com/attachments/ • 0xd1a:$x1: https://cdn.discordapp.com/attachments/ • 0xdda:$x1: https://cdn.discordapp.com/attachments/ • 0xe9a:$x1: https://cdn.discordapp.com/attachments/ • 0xf5a:$x1: https://cdn.discordapp.com/attachments/ • 0x119a:$x1: https://cdn.discordapp.com/attachments/ • 0x125a:$x1: https://cdn.discordapp.com/attachments/ • 0x131a:$x1: https://cdn.discordapp.com/attachments/ • 0x13da:$x1: https://cdn.discordapp.com/attachments/ • 0x149a:$x1: https://cdn.discordapp.com/attachments/
1.3.kGl1qp3Ox8.exe.41f4f2c.17.unpack	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x103c:$x1: https://cdn.discordapp.com/attachments/ • 0x1cc4:$x1: https://cdn.discordapp.com/attachments/ • 0x67f4:$x1: https://cdn.discordapp.com/attachments/ • 0x2d784:$x1: https://cdn.discordapp.com/attachments/ • 0x2d83c:$x1: https://cdn.discordapp.com/attachments/ • 0x2d8f4:$x1: https://cdn.discordapp.com/attachments/ • 0x2d9ac:$x1: https://cdn.discordapp.com/attachments/ • 0x2da64:$x1: https://cdn.discordapp.com/attachments/ • 0x2e304:$x1: https://cdn.discordapp.com/attachments/ • 0x2ee84:$x1: https://cdn.discordapp.com/attachments/
1.3.kGl1qp3Ox8.exe.40db8f8.57.raw.unpack	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x9310:$x1: https://cdn.discordapp.com/attachments/ • 0x9f98:$x1: https://cdn.discordapp.com/attachments/ • 0xac20:$x1: https://cdn.discordapp.com/attachments/ • 0xb8a8:$x1: https://cdn.discordapp.com/attachments/ • 0xc530:$x1: https://cdn.discordapp.com/attachments/ • 0xde40:$x1: https://cdn.discordapp.com/attachments/

Source	Rule	Description	Author	Strings
16.3.JiryxVDn0P_ka7w2xP8PdulD.exe.860000.0.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
16.3.JiryxVDn0P_ka7w2xP8PdulD.exe.860000.0.unpack	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
Click to see the 72 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Svchost Process

Sigma detected: Non Interactive PowerShell

Sigma detected: Windows Processes Suspicious Parent Directory

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Yara Genericmalware

Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Networking:

Yara detected onlyLogger

Creates HTML files with .exe extension (expired dropper behavior)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected SmokeLoader

E-Banking Fraud:

Yara Genericmalware

System Summary:

PE file has a writeable .text section

PE file contains section with special chars

PE file has nameless sections

Data Obfuscation:

Obfuscated command line found

Persistence and Installation Behavior:

Drops PE files to the document folder of the user

Malware Analysis System Evasion:

Tries to evade analysis by execution special instruction which cause usermode exception

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

Checks if the current machine is a virtual machine (disk enumeration)

Anti Debugging:

Tries to detect sandboxes and other dynamic analysis tools (window names)

Hides threads from debuggers

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

Lowering of HIPS / PFW / Operating System Security Settings:

Disable Windows Defender real time protection (registry)

Stealing of Sensitive Information:

Yara detected RedLine Stealer

Yara Genericmalware

Yara detected SmokeLoader

Yara detected Vidar stealer

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

Tries to steal Crypto Currency Wallets

Yara detected WebBrowserPassView password recovery tool

Remote Access Functionality:

Yara detected RedLine Stealer

Yara Genericmalware

Yara detected SmokeLoader

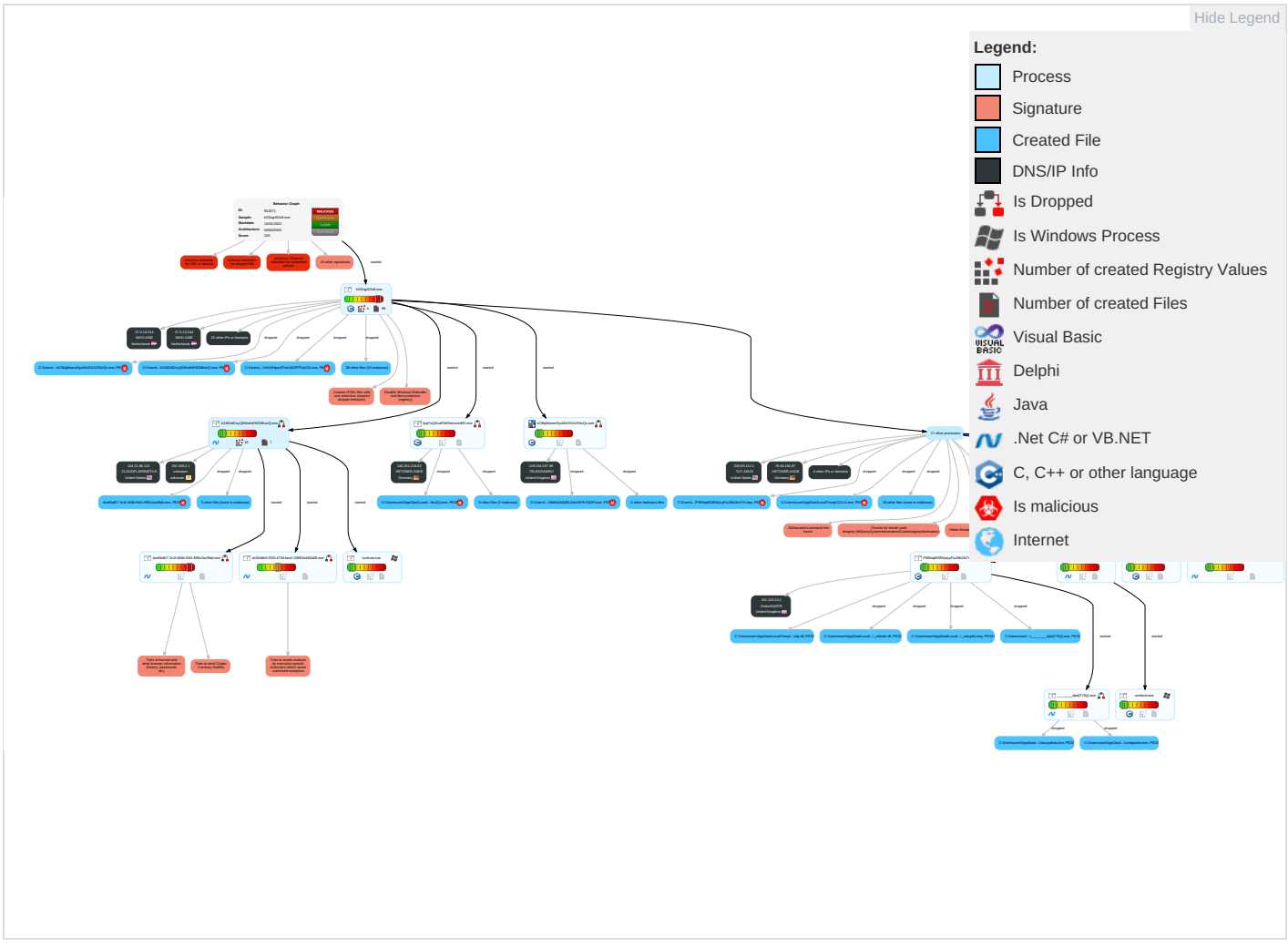
Yara detected Vidar stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comman and Cont
Valid Accounts	Command and Scripting Interpreter 1 3	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress T Transfer
Default Accounts	Service Execution 2	Windows Service 4	Bypass User Access Control 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 2 1	Exfiltration Over Bluetooth	Encrypted Channel
Domain Accounts	At (Linux)	Logon Script (Windows)	Windows Service 4	Obfuscated Files or Information 4 1	Security Account Manager	File and Directory Discovery 1 2	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration	Steganog

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comman and Cont
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 1 2	Software Packing 5 1	NTDS	System Information Discovery 1 2 4	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Imperson
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Security Software Discovery 7 6 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Bypass User Access Control 1	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonl Used Por
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 1 2	Proc Filesystem	Virtualization/Sandbox Evasion 3 6 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicatio Layer Pro
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 3 6 1	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Prot
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 1 2	Network Sniffing	System Owner/User Discovery 3	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Trans Protocols
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Proto

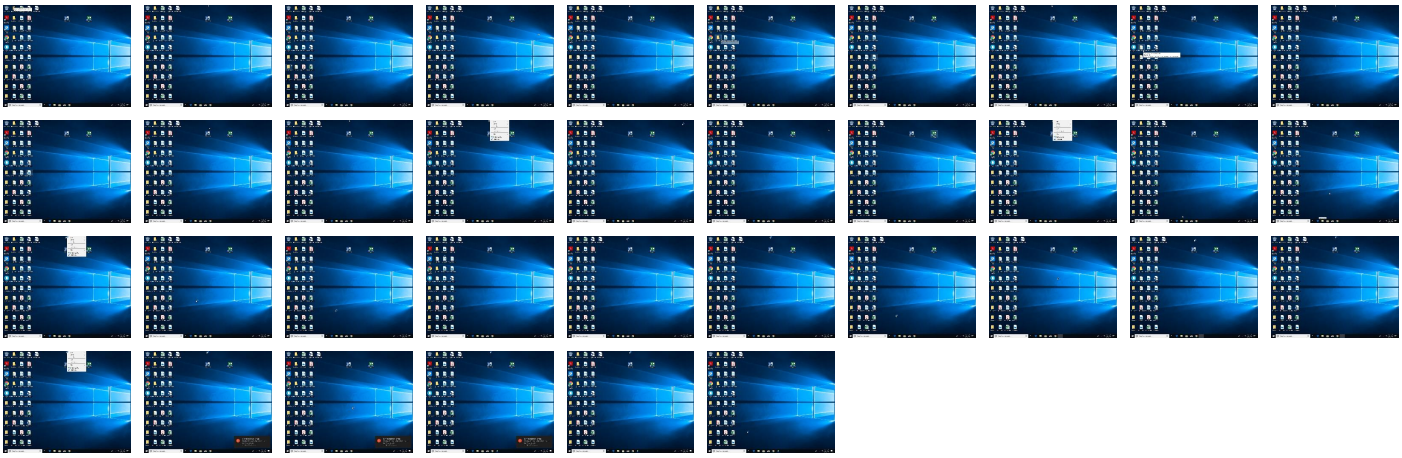
Behavior Graph



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
kGl1qp3Ox8.exe	37%	Metadefender		Browse
kGl1qp3Ox8.exe	67%	ReversingLabs	Win32.Downloader.SmallAgent	
kGl1qp3Ox8.exe	100%	Avira	HEUR/AGEN.1103434	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\NiceProcessX64[1].bmp	100%	Avira	TR/Agent.dttsn	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\fw3[1].exe	100%	Avira	TR/Kryptik.jfkdo	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\fw4[1].exe	100%	Avira	HEUR/AGEN.1144987	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\f[1].exe	100%	Avira	TR/Redcap.loame	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\Cube_WW14[1].bmp	100%	Avira	TR/Dldr.Agent.rrgit	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\RobCleanerInstlr758214[1].exe	100%	Avira	HEUR/AGEN.1144918	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\HR[1].exe	100%	Avira	HEUR/AGEN.1142105	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\Service[1].bmp	100%	Avira	TR/Dldr.Agent.dghsp	
C:\Program Files (x86)\PowerControl\PowerControl_Svc.exe	100%	Avira	TR/Dldr.Agent.dghsp	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\RobCleanerInstlr943210[1].exe	100%	Avira	HEUR/AGEN.1144918	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\appforpr2[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\NiceProcessX64[1].bmp	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\fw3[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\f[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\file3[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\ferrari[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\RobCleanerInstlr758214[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\Service[1].bmp	100%	Joe Sandbox ML		
C:\Program Files (x86)\PowerControl\PowerControl_Svc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\RobCleanerInstlr943210[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\file[1].exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\PowerControl\PowerControl_Svc.exe	49%	Metadefender		Browse
C:\Program Files (x86)\PowerControl\PowerControl_Svc.exe	89%	ReversingLabs	Win32.Trojan.Tasker	
C:\ProgramData\freebl3.dll	0%	Metadefender		Browse
C:\ProgramData\freebl3.dll	0%	ReversingLabs		
C:\ProgramData\mozglue.dll	3%	Metadefender		Browse
C:\ProgramData\mozglue.dll	0%	ReversingLabs		
C:\ProgramData\msvcp140.dll	0%	Metadefender		Browse
C:\ProgramData\msvcp140.dll	0%	ReversingLabs		
C:\ProgramData\softokn3.dll	0%	Metadefender		Browse
C:\ProgramData\softokn3.dll	0%	ReversingLabs		
C:\Users\user\AppData\LocalLow\sqlite3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\LocalLow\sqlite3.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\NiceProcessX64[1].bmp	14%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\NiceProcessX64[1].bmp	70%	ReversingLabs	Win64.Packed.Generic	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\Service[1].bmp	49%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\Service[1].bmp	89%	ReversingLabs	Win32.Trojan.Tasker	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
32.3.NhzjvwxrwXd3QBEl8Ly0lN5e.exe.4b20000.1.unpack	100%	Avira	TR/Crypt.EPACK.Gen2		Download File
8.0.eULKoZpb_80D8HrRwSiJF82y.exe.db0000.3.unpack	100%	Avira	HEUR/AGEN.1144918		Download File
1.0.kGl1qp3Ox8.exe.11f0000.0.unpack	100%	Avira	HEUR/AGEN.1103434		Download File
19.0.sCI8qb6amvGp4AhJGUUX5nQx.exe.da0000.2.unpack	100%	Avira	HEUR/AGEN.1202301		Download File
16.3.JiryxVDn0P_ka7w2xP8PdulD.exe.860000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.3.kGl1qp3Ox8.exe.4256600.186.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
1.3.kGl1qp3Ox8.exe.4256600.190.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
27.0.4c91d8e5-f330-473d-bea7-49691b483a08.exe.400000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.0.sCI8qb6amvGp4AhJGUUX5nQx.exe.da0000.1.unpack	100%	Avira	HEUR/AGEN.1202301		Download File
28.0.01913ed7-c54a-4682-ba7f-2339dfb12dae.exe.b80000.0.unpack	100%	Avira	HEUR/AGEN.1210067		Download File
6.0.kXM34tDnyQtlWwfvEKDMhvoQ.exe.8d0000.1.unpack	100%	Avira	HEUR/AGEN.1144918		Download File
30.0.0y_alCQBJv4J1LDnCOe55cop.exe.140000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.0.NNNBSubeVPxRXeeZnGu7gQkK.exe.7ff62bf00000.4.unpack	100%	Avira	HEUR/AGEN.1130812		Download File

Source	Detection	Scanner	Label	Link	Download
1.3.kGl1qp3Ox8.exe.7e21ca0.66.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
34.3.nnaUz9XFoo0RBkjZ4wuMqrTl.exe.2430000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
6.0.kXM34tDnyQtIWwfvEKDMhvoQ.exe.8d0000.3.unpack	100%	Avira	HEUR/AGEN.1144918		Download File
29.0.SiJXWwfMYK4L8VTC7HncQkab.exe.7ff65a4ccb30.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.3.kGl1qp3Ox8.exe.4256600.208.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
19.2.sCI8qb6amvGp4AhJGUUX5nQx.exe.da0000.0.unpack	100%	Avira	HEUR/AGEN.1202301		Download File
8.0.eULKoZpb_80D8HrRwSiJF82y.exe.db0000.0.unpack	100%	Avira	HEUR/AGEN.1144918		Download File
1.3.kGl1qp3Ox8.exe.40db528.161.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
31.1.C1aYSYmMy9tQLrifaCN41EQ8.exe.cd0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
31.0.C1aYSYmMy9tQLrifaCN41EQ8.exe.cd0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.3.56IWdY4eqRTdJgfAC3WHYY1z.exe.6c0000.0.unpack	100%	Avira	HEUR/AGEN.1131354		Download File
30.1.0y_alCQBJv4J1LDnCOe55cop.exe.140000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
29.0.SiJXWwfMYK4L8VTC7HncQkab.exe.7ff65a320000.3.unpack	100%	Avira	HEUR/AGEN.1208921		Download File
14.0.e5SEitbuPomqfmRpQ1nXQBM2.exe.b30000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.0.eULKoZpb_80D8HrRwSiJF82y.exe.db0000.2.unpack	100%	Avira	HEUR/AGEN.1144918		Download File
12.0.P65Nqt8GfRApLpFwJ9bOb7YH.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
34.0.nnaUz9XFoo0RBkjZ4wuMqrTl.exe.400000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
27.1.4c91d8e5-f330-473d-bea7-49691b483a08.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.3.kGl1qp3Ox8.exe.7e21ca0.91.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
27.0.4c91d8e5-f330-473d-bea7-49691b483a08.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
34.0.nnaUz9XFoo0RBkjZ4wuMqrTl.exe.400000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.0.P65Nqt8GfRApLpFwJ9bOb7YH.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
18.0.56IWdY4eqRTdJgfAC3WHYY1z.exe.670e50.7.unpack	100%	Avira	HEUR/AGEN.1131354		Download File
27.3.4c91d8e5-f330-473d-bea7-49691b483a08.exe.800000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.0.01913ed7-c54a-4682-ba7f-2339dfb12dae.exe.b80000.2.unpack	100%	Avira	HEUR/AGEN.1210067		Download File
28.0.01913ed7-c54a-4682-ba7f-2339dfb12dae.exe.b80000.1.unpack	100%	Avira	HEUR/AGEN.1210067		Download File
34.0.nnaUz9XFoo0RBkjZ4wuMqrTl.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
31.0.C1aYSYmMy9tQLrifaCN41EQ8.exe.cd0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.0.sCI8qb6amvGp4AhJGUUX5nQx.exe.da0000.0.unpack	100%	Avira	HEUR/AGEN.1202301		Download File
5.0.NNNBSubeVPxRXeeZnGu7gQkK.exe.7ff62bf00000.2.unpack	100%	Avira	HEUR/AGEN.1130812		Download File
1.3.kGl1qp3Ox8.exe.4256600.196.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.0.P65Nqt8GfRApLpFwJ9bOb7YH.exe.400000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
34.1.nnaUz9XFoo0RBkjZ4wuMqrTl.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.0.sCI8qb6amvGp4AhJGUUX5nQx.exe.da0000.3.unpack	100%	Avira	HEUR/AGEN.1202301		Download File
28.0.01913ed7-c54a-4682-ba7f-2339dfb12dae.exe.b80000.3.unpack	100%	Avira	HEUR/AGEN.1210067		Download File
29.0.SiJXWwfMYK4L8VTC7HncQkab.exe.7ff65a320000.6.unpack	100%	Avira	HEUR/AGEN.1208921		Download File
1.3.kGl1qp3Ox8.exe.4260820.172.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
12.1.P65Nqt8GfRApLpFwJ9bOb7YH.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
27.0.4c91d8e5-f330-473d-bea7-49691b483a08.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.0.P65Nqt8GfRApLpFwJ9bOb7YH.exe.400000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
31.3.C1aYSYmMy9tQLrifaCN41EQ8.exe.2fa0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
31.0.C1aYSYmMy9tQLrifaCN41EQ8.exe.cd0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.0.kXM34tDnyQtIWwfvEKDMhvoQ.exe.8d0000.0.unpack	100%	Avira	HEUR/AGEN.1144918		Download File
8.0.eULKoZpb_80D8HrRwSiJF82y.exe.db0000.1.unpack	100%	Avira	HEUR/AGEN.1144918		Download File
29.0.SiJXWwfMYK4L8VTC7HncQkab.exe.7ff65a320000.0.unpack	100%	Avira	HEUR/AGEN.1208921		Download File
14.1.e5SEitbuPomqfmRpQ1nXQBM2.exe.b30000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.3.kGl1qp3Ox8.exe.4260820.168.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.0.e5SEitbuPomqfmRpQ1nXQBM2.exe.b30000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
29.0.SiJXWwfMYK4L8VTC7HncQkab.exe.7ff65a4ccb30.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.3.e5SEitbuPomqfmRpQ1nXQBM2.exe.2c10000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
35.0._____djskjT76(((.exe.560000.0.unpack	100%	Avira	HEUR/AGEN.1126168		Download File
18.0.56IWdY4eqRTdJgfAC3WHYY1z.exe.670e50.5.unpack	100%	Avira	HEUR/AGEN.1131354		Download File
31.0.C1aYSYmMy9tQLrifaCN41EQ8.exe.cd0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.3.kGl1qp3Ox8.exe.4256600.182.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
1.3.kGl1qp3Ox8.exe.4256600.187.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
14.0.e5SEitbuPomqfmRpQ1nXQBM2.exe.b30000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
12.3.P65Nqt8GfRApLpFwJ9bOb7YH.exe.21cc000.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
6.0.kXM34tDnyQtIWwfvEKDMhvoQ.exe.8d0000.2.unpack	100%	Avira	HEUR/AGEN.1144918		Download File
5.0.NNNBSubeVPxRXeeZnGu7gQkK.exe.7ff62bf00000.0.unpack	100%	Avira	HEUR/AGEN.1130812		Download File
30.3.0y_alCQBJv4J1LDnCOe55cop.exe.2a20000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
30.0.0y_alCQBJv4J1LDnCOe55cop.exe.140000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
30.0.0y_alCQBJv4J1LDnCOe55cop.exe.140000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.0.e5SEitbuPomqfmRpQ1nXQBM2.exe.b30000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
34.0.nnaUz9XFoo0RBkjZ4wuMqrTl.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
1.3.kGl1qp3Ox8.exe.4259d40.181.unpack	100%	Avira	HEUR/AGEN.1145233		Download File
29.0.SiJXWwfMYK4L8VTC7HncQkab.exe.7ff65a4ccb30.7.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
10.3.VxkVtHpwGFsrs3Al2PFI1pOG.exe.9d0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
27.0.4c91d8e5-f330-473d-bea7-49691b483a08.exe.400000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
30.0.0y_alCQBJv4J1LDnCOe55cop.exe.140000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://212.193.30.45/WW/file8.exeaz:	100%	Avira URL Cloud	malware	
http://2.56.59.42/service/communication.php-9	0%	Avira URL Cloud	safe	
http://212.193.30.45/WW/file5.exeJr	100%	Avira URL Cloud	malware	
http://stylesheet.faseaegasdfase.com/hp8/g1/rtst1053.exeL	0%	Avira URL Cloud	safe	
http://212.193.30.29/WW/file1.exeC:	100%	Avira URL Cloud	malware	
http://212.193.30.29/WW/file4.exe0.exe	100%	Avira URL Cloud	malware	
http://xmtbsj.com/setup.exe	100%	Avira URL Cloud	malware	
http://212.193.30.45/WW/file8.exeC:	100%	Avira URL Cloud	malware	
http://212.193.30.29/WW/file1.exe$	100%	Avira URL Cloud	malware	
http://whatisart.top/	100%	Avira URL Cloud	malware	
http://https://innovicservice.net/assets/vendor/counterup/RobCleanerInstlr943210.exe3	0%	Avira URL Cloud	safe	
http://www.hhiuew33.com/	0%	Avira URL Cloud	safe	
http://stylesheet.faseaegasdfase.com/hp8/g1/rtst1053.exea	0%	Avira URL Cloud	safe	
http://https://innovicservice.net:80/assets/vendor/counterup/RobCleanerInstlr943210.exe	0%	Avira URL Cloud	safe	
http://212.193.30.45/WW/file7.exeet	100%	Avira URL Cloud	malware	
http://212.193.30.45/WW/file8.exe	100%	Avira URL Cloud	malware	
http://stylesheet.faseaegasdfase.com/hp8/g1/rtst1053.exe	100%	Avira URL Cloud	malware	
http://212.193.30.45/WW/file10.exe6r	100%	Avira URL Cloud	malware	
http://https://innovicservice.net/assets/vendor/counterup/RobCleanerInstlr758214.exe	0%	Avira URL Cloud	safe	
http://www.innosetup.com/	0%	URL Reputation	safe	
http://onepiece.s3.pl-waw.scw.cloud/pub-carousel/ShareFolder.exe	0%	Avira URL Cloud	safe	
http://https://watertecindia.com/watertec/fw4.exe	100%	Avira URL Cloud	malware	
http://185.215.113.208/	100%	Avira URL Cloud	malware	
http://212.193.30.45/WW/file8.exem	100%	Avira URL Cloud	malware	
http://212.193.30.29/WW/file3.exet	100%	Avira URL Cloud	malware	
http://https://innovicservice.net/assets/vendor/counterup/RobCleanerInstlr758214.exeC:	0%	Avira URL Cloud	safe	
http://https://watertecindia.com/watertec/f.exexe	0%	Avira URL Cloud	safe	
http://45.144.225.57/WW/sfx_123_310.exeEzF	100%	Avira URL Cloud	malware	
http://https://dpcapps.me/	100%	Avira URL Cloud	malware	
http://212.193.30.29/WW/file1.exe	100%	Avira URL Cloud	malware	
http://tg8.cllgxx.com/sr21/siww1047.exe	0%	Avira URL Cloud	safe	
http://212.193.30.45/WW/file7.exeC:	100%	Avira URL Cloud	malware	
http://212.193.30.29/WW/file2.exexe;y	100%	Avira URL Cloud	malware	
http://joinarts.top/check.php?publisher=ww2C:	0%	Avira URL Cloud	safe	
http://2.56.59.42/base/api/getData.php	100%	Avira URL Cloud	malware	
http://212.193.30.45/WW/file10.exeSyH	100%	Avira URL Cloud	malware	
http://tg8.cllgxx.com/sr21/siww1047.exe&	0%	Avira URL Cloud	safe	
http://https://WINHTTP.dllLater	0%	Avira URL Cloud	safe	
http://212.193.30.45/proxies.txt	100%	Avira URL Cloud	malware	
http://https://innovicservice.net/assets/vendor/counterup/RobCleanerInstlr758214.exeH	0%	Avira URL Cloud	safe	
http://https://innovicservice.net/assets/vendor/counterup/RobCleanerInstlr758214.exeE	0%	Avira URL Cloud	safe	
http://212.193.30.45/WW/file5.exepr	100%	Avira URL Cloud	malware	
http://212.193.30.29/download/Cube_WW14.bmp	100%	Avira URL Cloud	malware	
http://212.193.30.45/WW/file9.exe	100%	Avira URL Cloud	malware	
http://212.193.30.29/WW/file2.exeC:	100%	Avira URL Cloud	malware	
http://https://innovicservice.net/assets/vendor/counterup/RobCleanerInstlr943210.exe	0%	Avira URL Cloud	safe	
http://https://ipgeolocation.io/	0%	URL Reputation	safe	
http://45.144.225.57/WW/sfx_123_310.exeE	100%	Avira URL Cloud	malware	
http://https://innovicservice.net/assets/vendor/counterup/RobCleanerInstlr758214.exe.	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
85.209.157.230	unknown	Netherlands		18978	ENZUINC-US	false
172.67.177.36	unknown	United States		13335	CLOUDFLARENETUS	false
212.193.30.45	unknown	Russian Federation		57844	SPD-NETTR	false
212.193.30.29	unknown	Russian Federation		57844	SPD-NETTR	false
162.159.135.233	unknown	United States		13335	CLOUDFLARENETUS	false
149.154.167.99	unknown	United Kingdom		62041	TELEGRAMRU	false
8.8.8.8	unknown	United States		15169	GOOGLEUS	false
91.224.22.193	unknown	Russian Federation		197695	AS-REGRU	false
78.46.160.87	unknown	Germany		24940	HETZNER-ASDE	false
148.251.234.83	unknown	Germany		24940	HETZNER-ASDE	false
45.144.225.57	unknown	Netherlands		35913	DEDIPATH-LLCUS	false
37.0.10.214	unknown	Netherlands		198301	WKD-ASIE	false
2.56.59.42	unknown	Netherlands		395800	GBTCLOUDUS	false
31.41.45.12	unknown	Russian Federation		56577	ASRELINKRU	false
104.21.88.113	unknown	United States		13335	CLOUDFLARENETUS	false
172.67.133.215	unknown	United States		13335	CLOUDFLARENETUS	false
34.117.59.81	unknown	United States		139070	GOOGLE-AS-APGoogleAsiaPacificPteLtdSG	false
103.235.105.121	unknown	India		17439	NETMAGIC-APNetmagicDatacenterMumbaiIN	false
188.165.5.107	unknown	France		16276	OVHFR	false
52.218.104.171	unknown	United States		16509	AMAZON-02US	false
35.205.61.67	unknown	United States		15169	GOOGLEUS	false
149.28.78.238	unknown	United States		20473	AS-CHOOPAUS	false
208.95.112.1	unknown	United States		53334	TUT-ASUS	false
151.115.10.1	unknown	United Kingdom		12876	OnlineSASFR	false
37.0.10.244	unknown	Netherlands		198301	WKD-ASIE	false
185.215.113.208	unknown	Portugal		206894	WHOLESALECONNECTIONSNL	false
45.136.151.102	unknown	Latvia		18978	ENZUINC-US	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	553271
Start date:	14.01.2022
Start time:	15:30:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 19s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	kGl1qp3Ox8.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	42
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@72/126@0/28
EGA Information:	• Successful, ratio: 4%
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 32.5% • Quality standard deviation: 32.5%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:32:55	API Interceptor	30x Sleep call for process: powershell.exe modified
15:33:04	API Interceptor	3x Sleep call for process: SiJXWwfMYK4L8VTC7HncQkab.exe modified
15:33:09	API Interceptor	33x Sleep call for process: dce6bd67-7e1f-466b-94f1-f9f5c2acf9dd.exe modified
15:33:14	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run msuupd C:\Users\user\AppData\Roaming\msuupd.exe
15:33:16	Task Scheduler	Run new task: PowerControl HR path: C:\Program s>Files (x86)\PowerControl\PowerControl_Svc.exe
15:33:18	Task Scheduler	Run new task: PowerControl LG path: C:\Program s>Files (x86)\PowerControl\PowerControl_Svc.exe
15:33:32	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run msuupd C:\Users\user\AppData\Roaming\msuupd.exe
15:33:57	Task Scheduler	Run new task: Telemetry Logging path: C:\Users\user\AppData\Roaming\Microsoft\Protect\oobeldr.exe
15:33:58	Autostart	Run: HKLM64\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce system recover "C:\Program Files (x86)\autoit3\Sutaeloquly.exe"
15:34:16	Autostart	Run: HKLM64\Software\Microsoft\Windows\CurrentVersion\Run RegHost C:\Users\user\AppData\Roaming\Microsoft\RegHost.exe
15:34:19	Task Scheduler	Run new task: services32 path: C:\Windows\system32\services32.exe
15:34:40	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\z8K2kNXRJNBi.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\PowerControl\PowerControl_Svc.exe	
Process:	C:\Users\user\Pictures\Adobe Films\sCl8qb6amvGp4AhJGUUX5nQx.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	394752
Entropy (8bit):	6.344671929286929
Encrypted:	false
SSDEEP:	12288:X7ww87egHPRKA/oKRefRUGe0ISuPKq/wOBp/Bi:X7ww87NKA/lY60S/wOBlk
MD5:	503A913A1C1F9EE1FD30251823BEAF13
SHA1:	8F2AC32D76A060C4FCFE858958021FEE362A9D1E
SHA-256:	2C18D41DFF60FD0EF4BD2BC9F6346C6F6E0DE229E872E05B30CD3E7918CA4E5E
SHA-512:	17A4249D9F54C9A9F24F4390079043182A0F4855CBDAEC3EF7F2426DC38C56AA74A245CEEFD3E8DF78A96599F82A4196DC3E20CC88F0AEE7E73D058C3933699
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 49%, Browse • Antivirus: ReversingLabs, Detection: 89%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....[xtt...'...'...'.r.&...'.r.&...'.v.&...'.v.&...'.v.&5..'.r.&...'.r.&...'...'c..'.v.&...'.v.'...'.v.&...'Rich...'.....PE..L...0.a..... .....0....@.....@.....@.....@...d.....%.....8.....P...@.....0.....text...o..... ....`.rdata..N....0.....$.....@..@.data.....@....rsrc.....@..@.reloc...%.....&.....@..B.....

C:\ProgramData\freebl3.dll	
Process:	C:\Users\user\Pictures\Adobe Films\JiryxVDn0P_ka7w2xP8PdulD.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	334288
Entropy (8bit):	6.807000203861606
Encrypted:	false
SSDEEP:	6144:C8YBC2NpfYjGg7t5xb7WOBOLFwh8yGHrIrvqqDL6XPowD:CbG7F35BVh8yIZqn65D
MD5:	EF2834AC4EE7D6724F255BEAF527E635
SHA1:	5BE8C1E73A21B49F353C2ECFA4108E43A883CB7B
SHA-256:	A770ECBA3B08BBABD0A567FC978E50615F8B346709F8EB3CFACF3FAAB24090BA
SHA-512:	C6EA0E4347CBD7EF5E80AE8C0AFDCA20EA23AC2BDD963361DFAF562A9AED58DCBC43F89DD826692A064D76C3F4B3E92361AF7B79A6D16A75D9951591AE354D2
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$...../...AV..AV..AV...V..AV].@W..AV.1.V..AV].BW..AV].DW..AV].EW..AV..@W..AVO.@W..AV..@V.AVO.BW..AVO.EW..AVO.AW..AVO.V..AVO.CW..AVRich..AV.....PE..L....b.[.....'!.....f.....).....p.....s....@.....p...P.....@..x.....P.....0...T.....@.....8.....text...t..... ..`.rdata.....@..@.data...,H.....@....rsrc...x....@.....@..@.reloc.....P.....@..B.....

C:\ProgramData\mozglue.dll	
Process:	C:\Users\user\Pictures\Adobe Films\JiryxVDn0P_ka7w2xP8PdulD.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	137168
Entropy (8bit):	6.78390291752429

C:\ProgramData\mozglue.dll	
Encrypted:	false
SSDEEP:	3072:7Gyzk/x2Wp53pUzPoNpj/kVghp1qt/dXDyp4D2JJJvPhrSeTuk:6yQ2Wp53iO/kVghp12/dXDyyD2JJJvPR
MD5:	8F73C08A9660691143661BF7332C3C27
SHA1:	37FA65DD737C50FDA710FDBDE89E51374D0C204A
SHA-256:	3FE6B1C54B8CF28F571E0C5D6636B4069A8AB00B4F11DD842CFEC00691D0C9CD
SHA-512:	0042ECF9B3571BB5EBA2DE893E8B2371DF18F7C5A589F52EE66E4BFBAA15A5B8B7CC6A155792AAA8988528C27196896D5E82E1751C998BACEA0D92395F66AD 9
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U..;..;..;....;.W...;...8..;...?..;..:..;..:..>..;..:..;..:.w.;...?..;...>..;..:..;... ...;...9..;.Rich.;.....PE..L...._.[......"!.....z.....@.....3....@A.....@...t.....,.... ..x.....0..h.....T.....T.... ...h...@.....l.....text...x.....z..... ..`.rdata..^e.....f...~.....@..@.data.....@....didat..8.....@....rsrc...x.... ....@..@.reloc..h....0.....@..B.....

C:\ProgramData\msvcp140.dll	
Process:	C:\Users\user\Pictures\Adobe Films\JiryxVDn0P_ka7w2xP8PdulD.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	440120
Entropy (8bit):	6.652844702578311
Encrypted:	false
SSDEEP:	12288:Mlp4PwrPTlZ+/wKzY+dM+gjZ+UGhUgiW6QR7t5s03Ooc8dHkC2es9oV:Mlp4PePozGMA03Ooc8dHkC2ecl
MD5:	109F0F02FD37C84BFC7508D4227D7ED5
SHA1:	EF7420141BB15AC334D3964082361A460BFDB975
SHA-256:	334E69AC9367F708CE601A6F490FF227D6C20636DA5222F148B25831D22E13D4
SHA-512:	46EB62B65817365C249B48863D894B4669E20FCB3992E747CD5C9FDD57968E1B2CF7418D1C9340A89865EADDA362B8DB51947EB4427412EB83B35994F932FD39
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A.....V5=.....A....;....."...;.....;.....;.....;.....;.....;.....;-...;..... Rich.....PE..L....8'Y....."!.....P..... .....az....@A.....C.....R..,.....x..8?.....4:...f..8.....(..@.....P..... @..@.....text...r..... ..`.data....(... .....@....idata..6....P..... .....@..@.didat..4....p.....6.....@....rsrc.....8.....@ ..@.reloc..4:.....<...<.....@..B.....

C:\ProgramData\nss3.dll	
Process:	C:\Users\user\Pictures\Adobe Films\JiryxVDn0P_ka7w2xP8PdulD.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1223160
Entropy (8bit):	6.7696081765209755
Encrypted:	false
SSDEEP:	24576:Sb5zzlswYNYLVJAwfpeYQ1Dw/fEE8DhSJVIVkyAkgO6JV/jbHpls4MSRSMxkoo:4zW5ygDwnEZI6jgHjblMSRSMqH
MD5:	2F4056F1EAA038128F4F8BB6792BD7A3
SHA1:	6553C6C489BB404E7B9871C82B1B139E32ABE9A2
SHA-256:	01490C87425501C7AB9EA00DAC4CCF79BA47B014EEBDA4FAE812F874F452E16F
SHA-512:	16F2ECFE96443D439E85BB177C05C27B58029FF50DB3109DEE88687583429FFB78723FD6AB05BA5226EEAF5EF3FD0143EA05F5D67478485AD866EFB9A4239CC
Malicious:	false
Antivirus:	
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#.4.g.Z.g.Z.g.Z.n...s.Z..[.e.Z..B..c.Z..Y.j.Z..._.m.Z..^.l.Z.E.[.o.Z..[.d .Z.g.[..Z..^.m.Z..Z.f.Z....f.Z..X.f.Z.Richg.Z.....PE..L....b.[....."!.....w.....@.....@.....=..T.....p.....}.. p...T.....@.....text..... ..`.rdata...R.....T.....@..@.data...tG..`..."...B.....@....rsrc...p.....d..... .....@..@.reloc...}.....~...h.....@..B.....

C:\ProgramData\softokn3.dll	
Process:	C:\Users\user\Pictures\Adobe Films\JiryxVDn0P_ka7w2xP8PdulD.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	144848
Entropy (8bit):	6.539750563864442
Encrypted:	false

C:\ProgramData\softokn3.dll	
SSDEEP:	3072:UAf6suip+d7FEk/oJz69sFaXeu9CoT2nIVFetBWsqeFwdMIo:p6PbsF4CoT2OeU4SMB
MD5:	A2EE53DE9167BF0D6C019303B7CA84E5
SHA1:	2A3C737FA1157E8483815E98B666408A18C0DB42
SHA-256:	43536ADEF2DDCC811C28D35FA6CE3031029A2424AD393989DB36169FF2995083
SHA-512:	45B56432244F86321FA88FBCCA6A0D2A2F7F4E0648C1D7D7B1866ADC9DAA5EDDD9F6BB73662149F279C9AB60930DAD1113C8337CB5E6EC9EED5048322F65F78
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l$...JO..JO..JO.u.O..JO?oKN..JO?oIN..JO?oON..JO?oNN ..JO.mKN..JO-nKN..JO..KO~.JO-nNN..JO-nJN..JO-n.O..JO-nHN..JORich..JO.....PE..L....b.[....."!.....b.....P.....@..... .....0..x.....@..`.....T.....(...@.....l.....text..... ..`.rdata...D.....F.....@..@.data..... .....@ ....rsrc...x....0.....@..@.reloc..`....@.....@..B..... .....

C:\Users\user\AppData\LocalLow\frAQBc8Wsa	
Process:	C:\Users\user\Pictures\Adobe Films\NhzjvwxrwXd3QBEl8Ly0lN5e.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\LocalLow\sqlite3.dll	
Process:	C:\Users\user\Pictures\Adobe Films\NhzjvwxrwXd3QBEl8Ly0lN5e.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	916735
Entropy (8bit):	6.514932604208782
Encrypted:	false
SSDEEP:	24576:BJDwWdxW2SBNTjlY24eJoyGttl3+FZVpsq/2W:BJDvx0BY24eJoyctl3+FTX
MD5:	F964811B68F9F1487C2B41E1AEF576CE
SHA1:	B423959793F14B1416BC3B7051BED58A1034025F
SHA-256:	83BC57DCF282264F2B00C21CE0339EAC20FCB7401F7C5472C0CD0C014844E5F7
SHA-512:	565B1A7291C6FCB63205907FCD9E72FC2E11CA945AFC4468C378EDBA882E2F314C2AC21A7263880FF7D4B84C2A1678024C1AC9971AC1C1DE2BFA4248EC0F984
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....t\.....!.....Z.....p.....a..... ....H.... .....0...3.....text...XX.....Z.....`.P`.data.....p.....`.....@.`..rdata..... ...|.....@.`@.bss....(.....`..edata... ....."..... .....@.0@.idata..H.....@.0..CRT....,.....@.0..tls.... .....@.0..rsrc..... .....@.0..reloc...3...0...4.....@.0B/4.....p.....@.@B/19.....@..B/31..... .....@..B/45.....@..... .@..B/57.....`.....@.0B/70.....i....p.....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\0y_alCQBJv4J1LDnCOe55cop.exe.log	
Process:	C:\Users\user\Pictures\Adobe Films\0y_alCQBJv4J1LDnCOe55cop.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2291
Entropy (8bit):	5.3192079301865585
Encrypted:	false
SSDEEP:	48:MOfHK5HKXAHKhBHKdHKB1AHKzvQTHmYHKhQnoPtHoxHImHKoLHG1qHjHKdHAH5HX:vq5qXAqLqdqUqzcGYqhQnoPtlxHbqoL1

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\0y_alCQBJv4J1LDnCOe55cop.exe.log	
MD5:	A7F9412A837C84B4327D1242FEE4A56B
SHA1:	A8B66D25A5D1E392F6CA60317F82E1B25A9144B8
SHA-256:	5AA1E542EE4C3532DF5476BB06D70FBB2A8A0AB766BC63B490139244641DCE23
SHA-512:	EBFB1723B283D485EC075C3B09757C0998138F79ABF22162302A98D9A0589425309A3DEA32B21EAB78E8FCB965C1F97AF1A6E752BD97D1E898E8EBE185C74F6
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"SMDiagnostics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.IdentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.ServiceModel.Internals, Version=4.0.0.0, Culture=

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\4c91d8e5-f330-473d-bea7-49691b483a08.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\4c91d8e5-f330-473d-bea7-49691b483a08.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2291
Entropy (8bit):	5.3192079301865585
Encrypted:	false
SSDEEP:	48:MOfHK5HKXAHKhBHKdHKB1AHKzvQTHmYHKhQnoPtHoxHImHKoLHG1qHjHKdHAH5HX:vq5qXAqLqdqUqzcGYqhQnoPtIxHbqoL1
MD5:	A7F9412A837C84B4327D1242FEE4A56B
SHA1:	A8B66D25A5D1E392F6CA60317F82E1B25A9144B8
SHA-256:	5AA1E542EE4C3532DF5476BB06D70FBB2A8A0AB766BC63B490139244641DCE23
SHA-512:	EBFB1723B283D485EC075C3B09757C0998138F79ABF22162302A98D9A0589425309A3DEA32B21EAB78E8FCB965C1F97AF1A6E752BD97D1E898E8EBE185C74F6
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"SMDiagnostics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.IdentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.ServiceModel.Internals, Version=4.0.0.0, Culture=

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\C1aYSYmMy9tQLrifaCN41EQ8.exe.log	
Process:	C:\Users\user\Pictures\Adobe Films\C1aYSYmMy9tQLrifaCN41EQ8.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2291
Entropy (8bit):	5.3192079301865585
Encrypted:	false
SSDEEP:	48:MOfHK5HKXAHKhBHKdHKB1AHKzvQTHmYHKhQnoPtHoxHImHKAHKoLHG1qHqHAH5HX:vq5qXAqLqdqUqzcGYqhQnoPtIxHbqAq4
MD5:	4D17D01FD6FA0E9BB2B16E5F2F4AADD2
SHA1:	79A4E3B8C521919B1D857187CEF9713AD9E789F2
SHA-256:	ABB9FFE483BDA1231E9B52D88AC6D5714771377F974ED4059D569974D10F3622
SHA-512:	E63ECB9A083BFB5B7342AEA45A321F9A8506219EAF97D216F46470086CB0BC4146F727E91321C209EF168682EB86F08D73E7DC3A55E4EA246675CBE221A0CF4
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"SMDiagnostics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.IdentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"System.ServiceModel.Internals, Version=4.0.0.0, Culture=

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\e5SEitbuPomqfmRpQ1nXQBM2.exe.log	
Process:	C:\Users\user\Pictures\Adobe Films\e5SEitbuPomqfmRpQ1nXQBM2.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2291
Entropy (8bit):	5.3192079301865585
Encrypted:	false
SSDEEP:	48:MOfHK5HKXAHKhBHKdHKB1AHKzvQTHmYHKhQnoPtHoxHImHK1HxLHG1qHjHKdH5HX:vq5qXAqLqdqUqzcGYqhQnoPtIxHbq1RW
MD5:	58E50B3666584608A0EE88C5D36B394C

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\e5SEitbuPomqfmRpQ1nXQBM2.exe.log	
SHA1:	567E8A7EAC9EFD78134B726D55E9E44B86621BA8
SHA-256:	1D166DB9B8A16529F40FC396C42E720E84A9C2E6F5F0E3AB03378CF022428C2E
SHA-512:	E9924505D211545EA1E5A730EE56DC5C3AED290933C3FC4F5770185C56E4855285880542CF41E53B9E5CBACD54FA062C03ABAB2CB1E9FE46FDD7ACBCC16817 2
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0 .0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.n i.dll",0..2,"SMDiagnostics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.IdentityModel, Version=4.0.0.0, Culture=neutral, Pub licKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assem bly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\S ystem.Xml.ni.dll",0..2,"System.ServiceModel.Internals, Version=4.0.0.0, Culture=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\1234_1401[1].bmp	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	data
Category:	dropped
Size (bytes):	560756
Entropy (8bit):	7.5877881931432
Encrypted:	false
SSDEEP:	12288:RucQyfp3amzb8oRg/gnEzJyybdrS5JUoLXb+T:RucQytLnvg/gEzFxrS5JLQ
MD5:	0028D805C1F08B508639D640606FA76A
SHA1:	8CBF679A096986A379E3F26CC543BD52590D3514
SHA-256:	08BDF729CAEBE8EF33B5FDF0C39DB4FC8F15ED97B69E0C0F241A54C26810FF22
SHA-512:	1D30D7F41FDB514F5C4581E866D04D5AC8F71C2676EE89F3C8A2BADB8F0AA92B4A105F6734DE9F368C1E7CD908DC26AAFE20056EC026068E84E17ACD10D961 9
Malicious:	false
Reputation:	unknown
Preview:	...]....uq.1.>...-.....@..?~MFB.kt..mS.....Ky...k.P..^.[Z.....L..... .....Y\.....}.....].....}..... .....].....B.....].....}..... .....#5.....(.q.X...#K2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\404[1].htm	
Process:	C:\Users\user\Pictures\Adobe Films\fyqi7uQSxz8XM3xkvrctriED.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines
Category:	dropped
Size (bytes):	28096
Entropy (8bit):	4.455344386920121
Encrypted:	false
SSDEEP:	768:Ie/50UM+skkFG1DFG1PQ9TPMdxgvXQ9TPYQ9TPcQ9TPnQ9TP+0teK84X:Ie/GMX
MD5:	3ACC9ACFA3C32744AD8A400D278B784E
SHA1:	317C7E5232E7F8D8715B8D735DC3255A2B71D692
SHA-256:	E2D9F681926DDC80B7F1E16E84A2C5B7AA64DBD4C0CF4842DEEB4F6A7EF63A7D
SHA-512:	B47826CA4E55038E26BF396B4358A76DB90E7151473C508B090896D4328AE76185127C022485270327AA32F8152F6598ABEC902C8BED0F7FE7B733F5D7A41128
Malicious:	false
Reputation:	unknown
Preview:	.<!DOCTYPE html>.<html class="wide wow-animation" lang="en">. <head>. <title>404</title>. <meta name="format-detection" content="telephone=no">. <meta name="viewport" content="width=device-width, height=device-height, initial-scale=1.0, maximum-scale=1.0, user-scalable=0">. <meta http-equiv="X-UA-Compatible" content="IE=edge">. <meta charset="utf-8">.<link rel="icon" href="images/favicon.ico" type="image/x-icon">. Stylesheets-->. <link rel="stylesheet" type="text/css" href="//fonts.googleapis.com/css?family=Roboto:100,300,300i,400,500,600,700,900%7CRaleway:500">. <link rel="stylesheet" href="css/bootstrap.css">. <link rel ="stylesheet" href="css/fonts.css">. <link rel="stylesheet" href="css/style.css" id="main-styles-link">.. . Global site tag (gtag.js) - Google Analytics -->.<script async src="https://www.googletagmanager.com/gtag/js?id=UA-172526370-1"></script>.<script>. window.dataLayer = window.dataLayer || [];. function gtag(){dataLa

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\LeGXxX6[1].bmp	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	data
Category:	dropped
Size (bytes):	1384452
Entropy (8bit):	6.290704675603068
Encrypted:	false
SSDEEP:	24576:fNIi1zBkFfpjq3Y4pIP2+nOX+34ZvqIZebM:fNIi1VkFfpjnnOZqM
MD5:	B3E391535619BA87B6FAA1BC245F1724
SHA1:	B1C05727CDE9C1A83D18457D62D2EBBF65BB3C3D
SHA-256:	65F8AD57031866ACCEE8E775A39FED5271EA31B4AC497AD350B8215E03161BD5
SHA-512:	5F8C83CC598E7064093A5F9BBADD8D713BDE70007F5745C4FE82808D9F76184768FFE9F2DDAC40C9F81BC1ED35070990473FC609D24B8F02A44E48AD30C4746

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\LeGXxX6[1].bmp	
Malicious:	false
Reputation:	unknown
Preview:	...]..... bb..%.....'..).P.%..P.....k.....}.....#.....C.. .....Y.....C.....=.....A....f..... .A.....\.....c.....c.....c.....c.....c....7....N.....c....6.....Wc....7..... c....6.....c....1.....c....6....j.....c....6.....S.....6.....M.....)....(.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\NiceProcessX64[1].bmp	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	326144
Entropy (8bit):	6.2377498515628576
Encrypted:	false
SSDEEP:	6144:ej4R3H20xSWLE2Sgct82tCOcfX+A5yF17s:ejcG72Et8Vf81
MD5:	3F22BD82EE1B38F439E6354C60126D6D
SHA1:	63B57D818F86EA64EBC8566FAEB0C977839DEFDE
SHA-256:	265C2DDC8A21E6FA8DFAA38EF0E77DF8A2E98273A1ABFB575AEF93C0CC8EE96A
SHA-512:	B73E8E17E5E99D0E9EDFB690ECE8B0C15BEFB4D48B1C4F2FE77C5E3DAF01DF35858C06E1403A8636F86363708B80123D12122CB821A86B575B184227C760988
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 14%, Browse • Antivirus: ReversingLabs, Detection: 70%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l4.!.U.r.U.r.U.r.>.s.U.r.>.s.U.r.>.s.U.r.:.s.U.r.:.s.U.r.:.s$U.r.>.s.U.r .U.roU.r.:.s.U.r.:.r.U.r.:.s.U.rRich.U.r.....PE..d...\.<a....."....z.....|7.....@.....P.....`.....T...(....0..... ...@.....8.....0.....text....y.....z..... ..`.rdata..TM.....N...~.....@..@.data.....@....pdata..... .....@..@_RDATA..... .....@..@.rsrc.....0.....@..@.reloc.....@.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\Roll[1].bmp	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	data
Category:	dropped
Size (bytes):	1317252
Entropy (8bit):	6.8585793800543
Encrypted:	false
SSDEEP:	24576:GrbLONBrbBrbCrbPlD6uxZBN3f/eri5lFBOcqyta/:GrfOrrdrurzR6uxZeriLmjyK
MD5:	113E473C4E083B156B202CB4F77F6C98
SHA1:	CAC119891DF6EE84AAC83FD1F75C856FB89D813B
SHA-256:	66E9645B2411B2D0207EE5F17D43CA5E8987DA684751A804C221A738D3E983CB
SHA-512:	10F7A2670DEA6EF80737C9FB2B8C6C7DE214B333950C684C24098CF4CBF072D8DE7F2CD72F05E02FECBA2DE0EA49993A22E6A2618D559CA1D53A647AD113E AD
Malicious:	false
Reputation:	unknown
Preview:	...].....uq.1.>...-.....@..?~MFB.kt..mS.....Ky...k.P..^.[Z.....L..... .....1.....}.....q.....X.....q.....q..... .....].....q.....q.....}..... .....sZ.....U.4.N

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\Service[1].bmp	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	394752
Entropy (8bit):	6.344671929286929
Encrypted:	false
SSDEEP:	12288:X7ww87egHPRKA/oKRefRUGe0ISuPKq/wOBp/Bi:X7ww87NKA/lY60S/wOBlk
MD5:	503A913A1C1F9EE1FD30251823BEAF13
SHA1:	8F2AC32D76A060C4FCFE858958021FEE362A9D1E
SHA-256:	2C18D41DFF60FD0EF4BD2BC9F6346C6F6E0DE229E872E05B30CD3E7918CA4E5E
SHA-512:	17A4249D9F54C9A9F24F4390079043182A0F4855CBDAEC3EF7F2426DC38C56AA74A245CEEFD3E8DF78A96599F82A4196DC3E20CC88F0AEE7E73D058C3933699
Malicious:	**true**

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\Service[1].bmp	
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 49%, Browse • Antivirus: ReversingLabs, Detection: 89%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....[xtt...'...'...'.r.&...'.r.&...'.v.&...'.v.&...'.v.&5..'.r.&...'.r.&...'...'c..'.v.&...'.v.' ...'.v.&...'Rich...'.....PE..L...0.a..... .....0....@.....@.....@.....@...d.....%.....8.....P...@..... ....0.....text...o..... ....`.rdata..N....0.....$.....@..@.data.....@....rsrc.....@..@.reloc...%.....&..... .@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\help1201[1].bmp	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	data
Category:	dropped
Size (bytes):	412164
Entropy (8bit):	7.124273286585537
Encrypted:	false
SSDEEP:	6144:5FC2E1AQ2Cj5XVwC1/eUGu2k543yn/jbngcYvI3T0pjC060Dbfe1kG:502E1Tzj5XmA/e1uDy+jrgcqOcfeOG
MD5:	421AC3D4E41572BCC8FD94C7D35A2011
SHA1:	41466FDE501D99965F70A279A40CC98FB73BE1D5
SHA-256:	DEB1B5F3163C30D36A3D4895E0A644F5FD4D7F560923D6370C2F286C0A8F1665
SHA-512:	E3A0B39774515F9E39D0DE38375B7B3DC55810A31CFB08572BEF526F5BD19282EEEDA9A1D721A90A1D161C62591E18BDED5BBC3CED2058A86DD46A8D2C3B4 E1
Malicious:	false
Reputation:	unknown
Preview:	...]..... .....bb..%.....E.....'..).P.%..P.....VO.7!..7!..7!..e...7!..e...7!...Z..7!..7 .h7!..e...7!..e...7!..e...7!.....7!.....W.....} .....=.....w.....i.....]..... .....!..... .....].....].....w.....].....].....]..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\msvcp140[1].dll	
Process:	C:\Users\user\Pictures\Adobe Films\JiryxVDn0P_ka7w2xP8PdulD.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	440120
Entropy (8bit):	6.652844702578311
Encrypted:	false
SSDEEP:	12288:Mlp4PwrPTlZ+/wKzY+dM+gjZ+UGhUgiW6QR7t5s03Ooc8dHkC2es9oV:Mlp4PePozGMA03Ooc8dHkC2ecl
MD5:	109F0F02FD37C84BFC7508D4227D7ED5
SHA1:	EF7420141BB15AC334D3964082361A460BFDB975
SHA-256:	334E69AC9367F708CE601A6F490FF227D6C20636DA5222F148B25831D22E13D4
SHA-512:	46EB62B65817365C249B48863D894B4669E20FCB3992E747CD5C9FDD57968E1B2CF7418D1C9340A89865EADDA362B8DB51947EB4427412EB83B35994F932FD39
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A.....V5=.....A.....;.....".....;.....;.....;.....;.....;.....;.....;-...;..... Rich.....PE..L....8'Y.....!.....P..... .....az....@A.....C.....R.,.....x..8?.....4:...f..8.....(..@.....P..... @..@.....text...r..... ..`.data....(... .....@....idata..6....P..... .....@..@.didat..4....p.....6.....@....rsrc.....8.....@ ..@.reloc..4:.....<...<.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\new_v11[1].bmp	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	data
Category:	dropped
Size (bytes):	1321604
Entropy (8bit):	7.634805991513546
Encrypted:	false
SSDEEP:	24576:SKwBtbUcuCYbLLWDNQqfIeB07ioYZp0ScY3okGC9a7FgpSlKxxB5lLFiiTl3SMTA:SBGJDWDKqfIG2ioYv0FC9BLpjU3bwzDb
MD5:	8D472A02F6F4FE76CA3CDDC66E862E2C
SHA1:	DB00C682662BFA9325F9C85F715263713B1E05F5
SHA-256:	AC91EA65EB63CB8FB9FBA0A47B05C01F62D11398BE75A6595439CF83E37B11FC
SHA-512:	A4327171533421F7E2C1E2DEF6EC9B9AFA855B37BDA4B83D38E523ECA119F7DCC914661B7F6F0C9E2C653828212601AC1DF461D84E84EBB0FD4649F7900999F
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\new_v11[1].bmp	
Preview:	...]....uq.1.>...-.....@..?~MFB.kt..mS.....Ky...k.P..^.[Z.....L..... .....s.....}.....=.....1C.....u..... .....].....=.....}..... .....o b.a...[....%..*Z..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\3Y2ADQKS\stalkar_4mo[1].bmp	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	data
Category:	dropped
Size (bytes):	2363396
Entropy (8bit):	**7.999886009338604**
Encrypted:	**true**
SSDEEP:	49152:jBSz4y+TUB5AO5beZlmbwtpjRpzFEPszp1Rmv6mgREVUuaLfF7HId:j+pMuFJM1p5EkzpPm6xREVUBod
MD5:	936909AFD56C9E5A07A8611F751FF9CF
SHA1:	6CF7E70FA290D73322C3597BE8F693805B7E23D7
SHA-256:	F2A9256FB949A42729FC4764BEDF6F3669D942ED022FD7B9A316998B9B35ACC6
SHA-512:	9308E460DF9DB91970B086C8F99AFE50246CF995C47AABE580514172484F5456F096AE1E26D89DBCD85BABE52B6AE5AA8CDACBC5E0FE813EFFE975104AE132DD
Malicious:	false
Reputation:	unknown
Preview:	...].....bb..%.....'..).P.%..P.....D.....m.....M..... ....}....q..M.....q....m.%.....!.....e.....}.....}.....].....CTW'.... <g...1.....1....e.e.....i..W..`.e.....q....]S..I.(W.{..u..|.3-|....a*..x...r.%.eH.!.....+u). .0...Y9.u..u...>t;....|R?A#..Dh..I.ia..V.<.....$.Wy.k`.S.W#z,....}....E..B.:gqD.....^./h.....tn...W .....V..i.S..:.|.T.....6JS.}gC8E*{..%.rZ[h..rw"..>...6.....c=...J..~tjBU7.....Djm.s.>n...6.P`C5s.0..|. ..E..P.....8.<..;gqj<p....1^.....I>..f.A.....IBs.K.yFT^..X.:....=.8..>.B..A..... H.B.E:....F.....~..Qq....?....8.<

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\1234_1401[1].bmp	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	data
Category:	dropped
Size (bytes):	560756
Entropy (8bit):	7.5877881931432
Encrypted:	false
SSDEEP:	12288:RucQyfp3amzb8oRg/gnEzJyybdrS5JUoLXb+T:RucQytLnvg/gEzFxrS5JLQ
MD5:	0028D805C1F08B508639D640606FA76A
SHA1:	8CBF679A096986A379E3F26CC543BD52590D3514
SHA-256:	08BDF729CAEBE8EF33B5FDF0C39DB4FC8F15ED97B69E0C0F241A54C26810FF22
SHA-512:	1D30D7F41FDB514F5C4581E866D04D5AC8F71C2676EE89F3C8A2BADB8F0AA92B4A105F6734DE9F368C1E7CD908DC26AAFE20056EC026068E84E17ACD10D961 9
Malicious:	false
Reputation:	unknown
Preview:	...].....uq.1.>...-.....@..?~MFB.kt..mS.....Ky...k.P..^.[Z.....L..... .....Y\.....}.....].....}..... .....].....B.....].....}..... .....#5.....(.q.X...#K2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\Cube_WW14[1].bmp	
Process:	C:\Users\user\Pictures\Adobe Films\sCI8qb6amvGp4AhJGUUX5nQx.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	130048
Entropy (8bit):	6.425220045896409
Encrypted:	false
SSDEEP:	3072:Ix3W04qaxUUI4Y+TM4UzqlwGCD+IgQn0uG4PkWZNRgaWrSJSDhixGW2pldwuMmzA:IchAXD+UFkWDiwwixv+0uMmzv34
MD5:	4EDBAE4F41DBFFF3675A867FE06EA0DB
SHA1:	F6E91D1E642B7E9762B0ECC2E36B6FC489DA4A13
SHA-256:	0F61C7D939EA77FFF7EB409522338347B140BEB1C5977BD0FC84FF301DD31605
SHA-512:	7C65FB74664C142B3FB9BEE0BEB1F01B36D2EBAE592C864481B2D07C706DA9312F030BADE9721353CA298B985A24BAC8FC1F87A6BB39A10273A4A4E66AC835C8
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\Cube_WW14[1].bmp

Preview:

MZ......................@...!..L.!This program cannot be run in DOS mode....$.......B>cG._..._..._...4..._...4..._...4..._...0..._...0..._...0..*_...4..._..
._..X_...0..._...0..._..._..._...0..._..Rich._.................PE..L...c..a....................L...................@..........................@............@................................4...<.......(.................... ..T.
...a................................a..@..............0...........................polik.............................. ..`.data...D..........................@....idata.............................@..@.rsrc...(..........................@.
.@.reloc..T.... ....@..B...
....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\HR[1].exe

Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	636743
Entropy (8bit):	7.4622670958876185
Encrypted:	false
SSDEEP:	12288:8Qi3uAIKMYqN96m6UR0IrELWKlVwlpkTyL6Ka3EjiqxyNefotS10m:8Qi+PvNgHIALfGHkTVwiPk4Bm
MD5:	3A9664DAD384F41DCDC1272ED31171E0
SHA1:	D525F290DCF469F5B26654A4DB685092F8616509
SHA-256:	A85903FC9F06B4CCC4136FC573F6AFDFB6B90D555530F7259E4E8CB18616B724
SHA-512:	F7C3E6D561DF34C63E373C6CC715E1C13AB68013360F1694EEFAE6C896345ABD1135E60B5AA5D96FFD245AB7D24C9D856A7EAB58C9798D3B7B355E9DE16183 0
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	unknown

Preview:

MZP....................@...!..L.!..This program must be run under Win32..$7..
..........................PE..L....^B*...@.......................................@......@.............................P...
........................CODE....0.......................... ..`DATA....P..........................@...BSS.......................................idata..P..........................@....tls......................................rdata..........
....................@..P.reloc.............................@..P.rsrc..............................@..P............@.....................@..P...
....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\PL_Client[1].bmp

Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	data
Category:	dropped
Size (bytes):	1759748
Entropy (8bit):	6.609401987377134
Encrypted:	false
SSDEEP:	24576:RAoCuQN3sS4wWmp/wbJU3MaWtNA/8nk5quGviobr:RAqQN3sS4wWmpsqWtGguGvtP
MD5:	57F492DB3101CA040176C4CEACCC8C5E
SHA1:	4FB9A8FB0F97605FA31086D77E9D096F2C20FFD9
SHA-256:	9BFB00DFDF0BB2AD99D138F721260F2B3FB1BD7CDDEC20EC92291CF57EA63C4B
SHA-512:	A5A8CFF754D2024210C6AEE910661D6FF39210B392AD0C6331BC896E48A69F73E2DA1472BE8B5DADFA6CC3EDB3A6817F7EC05504CCB1B0B3837D7DDC8004F/ 0A
Malicious:	false
Yara Hits:	• Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\PL_Client[1].bmp, Author: Florian Roth
Reputation:	unknown

Preview:

...]............bb..%...'..).P.%..P...Q...Q...Q...P...Q...P/..Q...P...Q...Q...Q...P...Q...P...Q...P...Q...P...Q...Q:..QV..P..QV.-
Q...Q..EQ...QV..P...Q.......Q..............................|.........}............s......[...-...j..................-.......>.......................9.......
>................]..].........j..-...e.................................-..
....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\f[1].exe

Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	127488
Entropy (8bit):	6.620019563439738
Encrypted:	false
SSDEEP:	3072:M1UJhFefM7JlXBTPGymqI3rfgusNKKSZrFE6dHo:vFUM7NGy2DmNvCH
MD5:	7A14B5FC36A23C9FF0BAF718FAB093CB
SHA1:	DC1244688756E1E10A73C1FCBD2FCA1C3AF3565F
SHA-256:	7A1481A3EC2646610CC068CE5BBCC169D75B7B664F3DF1997823A374B1CF19A7
SHA-512:	BFE06EDB9F1928C8F7923D7FD6D3766DFF272D06F61FC4C40F1A531589D161DE435631C8B53D5D02A64AE4BEE695FB47DF6467A5B117C188813BB0CE8BE565
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\f[1].exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B../.qo|.qo|.qo|c.l}.qo|c.j}.qo|c.k}.qo|T.j}"qo|T.k}.qo|T.l}.qo|c.n}.qo| .qn|.qo|.qo|.qo|..m}.qo|Rich.qo|.....PE..L.....a.....r.....@.....0.....@.....$..... .....0 ...@.....text...7p.....r..... ..`.rdata..6`.....b...v.....@..@.data.....@....reloc..... .....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\file3[1].exe	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	1314720
Entropy (8bit):	7.612042225122131
Encrypted:	false
SSDEEP:	24576:t8f39B+OecSnrJYG4oPSidpXPQvzJetHu7MgUEjumXKHt:worJYGPd1PQ7JUaMjEygK
MD5:	2DBF77866712D9EBD57EC65E7C1598A8
SHA1:	25693E771D3D25112FFA7C38875DECD562AC808D
SHA-256:	2E382DCD1F433490E453D5E7E710D2BB821C2DF09F1E16B675EE060D46DA80D6
SHA-512:	609AA7242A8908AD7B59FD5F303492DDF435320106219D9E35F88B6A9976ADC72CA1E72CD17F714D349E430F8A0D330837C81AD947AC62E4DCD2C83D32A2DB
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(3...32.....f.....C'B{b.....+..R...d:.....Q..... ....PE..L...P.....0.....F..... ... .@.....+.....@.....0.....@...D..... ...data.... .....`.shared.....0.....@....rsrc....D...@...D.....@..@.CRT.....x...L.....@..... .....kg...}R..hI.>..H......

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\freebl3[1].dll	
Process:	C:\Users\user\Pictures\Adobe Films\JiryxVDn0P_ka7w2xP8PdulD.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	334288
Entropy (8bit):	6.807000203861606
Encrypted:	false
SSDEEP:	6144:C8YBC2NpfYjGg7t5xb7WOBOLFwh8yGHrIrvqqDL6XPowD:CbG7F35BVh8yIZqn65D
MD5:	EF2834AC4EE7D6724F255BEAF527E635
SHA1:	5BE8C1E73A21B49F353C2ECFA4108E43A883CB7B
SHA-256:	A770ECBA3B08BBABD0A567FC978E50615F8B346709F8EB3CFACF3FAAB24090BA
SHA-512:	C6EA0E4347CBD7EF5E80AE8C0AFDCA20EA23AC2BDD963361DFAF562A9AED58DCBC43F89DD826692A064D76C3F4B3E92361AF7B79A6D16A75D9951591AE354 4D2
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$...../...AV..AV..AV...V..AV].@W..AV.1.V..AV].BW..AV].DW..AV].EW.. AV..@W..AVO.@W..AV..@V.AVO.BW..AVO.EW..AVO.AW..AVO.V..AVO.CW..AVRich..AV.....PE..L....b.[.....''!.....f.....).....p.....s.... @.....p...P.....@..x.....P.....0...T.....@.....8.....text...t..... ..`.rdata.....@..@.data. ..,H.....@....rsrc...x....@.....@..@.reloc.....P.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\newt[1].bmp	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	data
Category:	dropped
Size (bytes):	457220
Entropy (8bit):	7.857060689412181
Encrypted:	false
SSDEEP:	12288:dl3cKvQB7bXXCx7il1PUYM91pEhTCbKRlsIhYFfL:dlGB77XCx7iHS9/EhTCmRlrYFD
MD5:	4A07E2790DDBE0A071C9753A35789156
SHA1:	71A0F9CD6605E82310B2A9DB71EECF6032B52B93
SHA-256:	5347691898EE93E549D9AFA5BA870FF736A7EC7DF72527A177E8670B176508FC
SHA-512:	3F1C06E367B2B650201B0E864249CD9DBF9A801E4AAB922D01E7AAE60EBF28EF2B9B8C902AF3C9DE75779C749F8C865D33869E8FD7BFBE280798EBD62822CD 9
Malicious:	false
Reputation:	unknown
Preview:	...].....bb..%.....'..).P.%..P.....).....)...v.).....).....O.....O.k.....O.....}.....}.....M... .....}.....=.....a..9.....U*.....M.....}..... ..}.....}.....}.....9.....}.....].....%...3.....}.....}.....}.....=...m.....}.....g.....}..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\real1302[1].bmp	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	data
Category:	dropped
Size (bytes):	766468
Entropy (8bit):	7.226214208526357
Encrypted:	false
SSDEEP:	12288:ISmrhMXAikYRM5FqlotURs7iVQAuwpC2/GshblciSptohmteoYegsxNu+zrc6rV3:9mrhxv5I+OJyQFPgcorxbzrdxNd1J
MD5:	06D50654B8D6980660E129868248E3C2
SHA1:	C19733A7221E1949A5A8DE96BECEF37D2B8E0D7C
SHA-256:	576CE22CDA267274D1A423A8CEC776D5D20341F815D3255E08D0D8274E409C25
SHA-512:	3485D466B52C57F0E73F4AB3669B9ED75F9987EFEF63743D86D47FE46C97B54A7C88B22996E864D6BAF0BEC7AB34C0E773D37176400B1939BF8B252F4E1D3421
Malicious:	false
Reputation:	unknown
Preview:	...]..........bb..%.....m.....'..).P.%..P.....J.....\.....[....V.....v.....K.....N.....}.... .....-.....5.....A.....}.....=..... .....e+.....].....C...I..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\9QTQHWWN\softokn3[1].dll	
Process:	C:\Users\user\Pictures\Adobe Films\JiryxVDn0P_ka7w2xP8PdulD.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	144848
Entropy (8bit):	6.539750563864442
Encrypted:	false
SSDEEP:	3072:UAf6suip+d7FEk/oJz69sFaXeu9CoT2nlVFetBWsqeFwdMIo:p6PbsF4CoT2OeU4SMB
MD5:	A2EE53DE9167BF0D6C019303B7CA84E5
SHA1:	2A3C737FA1157E8483815E98B666408A18C0DB42
SHA-256:	43536ADEF2DDCC811C28D35FA6CE3031029A2424AD393989DB36169FF2995083
SHA-512:	45B56432244F86321FA88FBCCA6A0D2A2F7F4E0648C1D7D7B1866ADC9DAA5EDDD9F6BB73662149F279C9AB60930DAD1113C8337CB5E6EC9EED5048322F65F78
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l$...JO..JO..JO.u.O..JO?oKN..JO?oIN..JO?oON..JO?oNN ..JO.mKN..JO-nKN..JO..KO~.JO-nNN..JO-nJN..JO-n.O..JO-nHN..JORich..JO.....PE..L....b.[.....''!.....b.....P.....@..... .....0..x.....@..`.....T.....(...@.....I.....text..... ..`.rdata...D.....F.....@..@.data..... .....@ ....rsrc...x....0.....@..@.reloc..`....@.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\27f_1401[1].bmp	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	data
Category:	dropped
Size (bytes):	781828
Entropy (8bit):	7.651511676343145
Encrypted:	false
SSDEEP:	12288:rflvzk/CDajDJO4kUDdfL5Br+j6aSTJQPuh/ZnE1hZ0DQUiBs6wQkcI3Jlee7H:rlv46OHgUDdD5MjXSTJwuhBnE1L0DQUA
MD5:	BF2EACD3AC9C12709881AA852DC60358
SHA1:	EEBE60C4775143199D1EB1F63D48675B45CCC289
SHA-256:	48B201629679F0E035CA613F27B1170CBEC03FC7975A5A6D789DCF6B8B926526
SHA-512:	E116F250E6CFEC842AC62DFC37FA8135BDDBC854FEF4D87C54DE876A384E52ACEF18D22703F4AC83C5EF82EA9AB1E5DD0A935C574F0B5AE8FF8A28B55AC026E3
Malicious:	false
Reputation:	unknown
Preview:	...]..........bb..%.....}.....'..).P.%..P.....8g.Q|...|...|...bTZ.f...bTL.....[.....|.....bTK.F...bT[.}...bT^.}.....|.....+.....}. .....m...1.....-#.....lv.....%.....q.....r.....m..... .....T.....i.....].....M.....].....w...}.....].....m.....].....%n.....'.....?..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\file[1].exe	
Process:	C:\Users\user\Pictures\Adobe Films\fyqi7uQSxz8XM3xkvrctriED.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	272384
Entropy (8bit):	4.939288121191688

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\file[1].exe	
Encrypted:	false
SSDEEP:	3072:TRgSGODomPPSmzU1U3LXkhvrQJcST/aDWrxpzbgqru:T2tmPPS51YohvrZST/guzbgwu
MD5:	C2EC5A75462D14AF2C509F3E61C0CA68
SHA1:	2A97AA969650C7C75E15F960C47EDF54BA36E78A
SHA-256:	DDAA51B7F3C2B6DD0E8BCCB4785B1C6D86A6D7E39FFB6C5A9B6F5F989B9838A3
SHA-512:	4526B6292559F542CE96E21B5E3211797895B0A9CF11DAC0BF5FBCA8AC90C7B0384B3DD6C7DB27AF89B16BFC6B22B7562F92A1F81388B2EF194FD1CD156822AE
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W..O6..O6..O6..QdR.S6..QdD..6..QdC.a6..h..L6..O6...6..QdM.N6..QdS.N6..QdV.N6..RichO6.....PE..L...b,._..... .....00.....0....@.....A.....f..(.....(.....1.....Y..@.....0.....text...C..... ....`.rdata...?...0...@...$.....@..@.data....V...p.....d.....@....rsrc...(.....Z.....@..@.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\fw3[1].exe	
Process:	C:\Users\user\Pictures\Adobe Films\fyqi7uQSxz8XM3xkvrctriED.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	350720
Entropy (8bit):	5.837263630193013
Encrypted:	false
SSDEEP:	6144:z0d0y3YN3kF+VkgVDZqWCinN4roRkv6KcEih31c2Kigl3y29:C0l03u2HvNUoyvmhZmC29
MD5:	8C0449C168C009C9DC860902E0F1CA66
SHA1:	5CF505891182ABCAFA951F13095446AF7C76080F
SHA-256:	E77A7FC7620DEF141DD138FE6192B9C34E800EBDC0A34B35D72B3289BACF6544
SHA-512:	B6929C8D093A323FF4505419963D5DB6228AAEE467266D085F903BBA018A8A95742180C4935169172A4FF93AAD46CAABBBA549BC97C09D1FF09971CA38FBEFB
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....2.....Rich.....PE..L.....a.....x.....@.....@.....d.....p..p.....@.....<..... .....text...rw.....x..... ..`.rdata..._.....`...|.....@..@.data...dw.....n.....@....reloc..p....p.....J.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\fw4[1].exe	
Process:	C:\Users\user\Pictures\Adobe Films\fyqi7uQSxz8XM3xkvrctriED.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	143872
Entropy (8bit):	6.074860303790983
Encrypted:	false
SSDEEP:	1536:+Rjag85YZeVUa7jLxJ6ErQN/0xttmbgSTuVLXylEYpxYlhwNLSNsWJd09dlt+mGM:+pgUabx5rTTtmcuuVLXq1wMf+mkQ
MD5:	5D88433ACCC7194A4B00EBF5ED3B89E9
SHA1:	D4F1FBB70BF3E1D456CB8F0A0E0E54A6F3B8122B
SHA-256:	A4CB0942DC11A1BB4BA19B67D25EF048A6CBCD08F46BC966D57C4CB5E0ACA42E
SHA-512:	AED23DA0D6F8CFFAB600C1A51F0984444C953A6BADC67E268DB2CA083D0158F2E418AF1407A935363F71FD88F8EDFE70D0D666B726C9FA230A75B923D598D2B
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....M.....L.....{.....{.....{...Rich.....PE..d.....a.....".....F.....x.....@.....`.....L.....p.....@.....d.....8..... ...8..... ...`..H.....text...pE.....F..... ..`.rdata..... `.....J.....@..@.data..... .....@....pdata.....@.....@..@_RDATA.....`.....&.....@..@.rsrc.....p.....(.....@..@.reloc..d.....*.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\mozglue[1].dll	
Process:	C:\Users\user\Pictures\Adobe Films\JiryxVDn0P_ka7w2xP8PdulD.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	137168
Entropy (8bit):	6.78390291752429

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\mozglue[1].dll	
Encrypted:	false
SSDEEP:	3072:7Gyzk/x2Wp53pUzPoNpj/kVghp1qt/dXDyp4D2JJJvPhrSeTuk:6yQ2Wp53iO/kVghp12/dXDyyD2JJJvPR
MD5:	8F73C08A9660691143661BF7332C3C27
SHA1:	37FA65DD737C50FDA710FDBDE89E51374D0C204A
SHA-256:	3FE6B1C54B8CF28F571E0C5D6636B4069A8AB00B4F11DD842CFEC00691D0C9CD
SHA-512:	0042ECF9B3571BB5EBA2DE893E8B2371DF18F7C5A589F52EE66E4BFBAA15A5B8B7CC6A155792AAA8988528C27196896D5E82E1751C998BACEA0D92395F66AD 9
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....U..;..;..;....;.W...;...8..;...?..;...:..;...>..;...:..;...:.w.;...?..;...>..;...;..;... ...;...9..;.Rich.;.....PE..L...._.[.....'!.....z.....@.....3....@A.....@...t.....,.... ..x.....0..h.....T.....T.... ...h...@.....l.....text....x.....z..... ..`.rdata..^e.....f...~.....@..@.data.....@....didat..8.....@....rsrc...x.... ....@..@.reloc..h....0.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\nss3[1].dll	
Process:	C:\Users\user\Pictures\Adobe Films\JiryxVDn0P_ka7w2xP8PdulD.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	827000
Entropy (8bit):	5.44591523391673
Encrypted:	false
SSDEEP:	24576:Sb5zzlswYNYLVJAwfpeYQ1Dw/fEE8DhSJVIV:4zW5ygDwnEZI
MD5:	1399B4F3D2FDA12A9EE27996FA72B6BA
SHA1:	EFE431EEB643B63A500A6D563A9A18618363ECC9
SHA-256:	E4434EE68044126E90FDE07295B859FE3CAF06033F771F80433E59C0D8011E4F
SHA-512:	049C20F93A4ABC55CD4171F3339397BA892816C0D6B645F84E7AF9111C07E7093BFA990B4D09677CD282E63B1A9FD305AA30A38590A9D3180D48139404198 64E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#.4.g.Z.g.Z.g.Z.n...s.Z..[.e.Z..B..c.Z..Y.j.Z..._.m.Z..^.l.Z.E.[.o.Z..[.d .Z.g.[..Z..^.m.Z..Z.f.Z....f.Z..X.f.Z.Richg.Z.....PE..L....b.[.....'!.....w.....@.....@.....=..T.....p.....}.. p...T.....@.....text..... ..`.rdata...R.....T.....@..@.data...tG..`..''...B.....@....rsrc...p.....d..... .....@..@.reloc...}.....~...h.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\russ[1].bmp	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	data
Category:	dropped
Size (bytes):	548532
Entropy (8bit):	7.669672806891924
Encrypted:	false
SSDEEP:	12288:3En3cQyfp3amz3/b+R2qtz6EGEzytnJ/AevLrap:3O3cQytLf+v5DGEzytnhAeH+
MD5:	9A318136E1125B55215EF5138044BA60
SHA1:	E797F2E3A14E1EA47817F92EDC792E0A8D440C09
SHA-256:	F8D62C83234CE668E787BBC4CD785929A94CFCFD65027B79AF2574F4D94C7371
SHA-512:	FE735DB74F56E03AC65D111CAC39E952367A74426E3FE93596BF9F7EE3B2D9CD5188905FBD982C0DCDF5E59DA37EDA1A0AA25439FE7D865DE60A15BC3F71D 8A
Malicious:	false
Reputation:	unknown
Preview:	...]....uq.1.>...-.....@..?~MFB.kt..mS.....Ky...k.P..^.[Z.....L..... .....-.....}.....>.....A..... .....].....x.....].q.....}..... .....R.F..].P.Y.....{...t...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\softer1401[1].bmp	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	data
Category:	dropped
Size (bytes):	1846420
Entropy (8bit):	7.924270784703104
Encrypted:	false
SSDEEP:	49152:RfucQyVj4K7efDARM9hCIzd24U1xe0om7kc8lbbTtq:RfayVjF7efDhYmd2hje0Joceftq
MD5:	2172158FCA5FF61D086C7C9758E6317A
SHA1:	1A2C933ADA88036A19A4E39C613B8120DA471147
SHA-256:	F216E94249C77DEEA8567A9D6A5C45F52A5F27135EDD22F58DC0DA5E27C44533

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\softer1401[1].bmp	
SHA-512:	D76212393B1A596FC18D6B1C1537E1F2DA86C0C5315FEB77639B83C727C5F3337900EC78B97DE4735C960754A5C8951DBBE3C8E2A43649E95F6D9E48B4852633
Malicious:	false
Reputation:	unknown
Preview:	...]....uq.1.>...-.....@..?~MFB.kt..mS.....Ky...k.P..^.[Z.....L..... .....A.....}.....=.....=..... .....]....n.....=.....g.....}..... .....X..O..K..t.}B..../...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\G62TDH9B\utube0501[1].bmp	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	data
Category:	dropped
Size (bytes):	7652145
Entropy (8bit):	**7.996937403275874**
Encrypted:	**true**
SSDEEP:	98304:0E6U8CakDBZapwJeLm+fKTMsdkUwVOfKNVeS6t9IGW/2InyF8pcDK0CjezHfQT/1:0jbClhYJKTvkUaVeSK9PtZ8qLowQuAF/
MD5:	3415D918A3144E485AC7B55DF36C480A
SHA1:	F7EE383DC873E629690A83E197250713F2CCB8E6
SHA-256:	28EAEE74D58DEB0B1AC344C924FACDB1F9CA2C7CFB675E05D9E15CBEDC72D2E0
SHA-512:	12F958617B99D353FBC2EDE5461E869A7DB12863C89B043382B9FB125DE2D07956126DDB2AE2C38DC541B7B234DC48864639F36EA3A309D8F15650D42DA4608
Malicious:	false
Reputation:	unknown
Preview:	...]....bb..%.....u.....'..).P.%..P.....@|.....2;.D.....2;.I..kkD....kkp.....j.x.....}.....-.. .....-.....yt.....-..e.....w.....-... .....y.....].....].....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\RobCleanerInstlr758214[1].exe	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	166912
Entropy (8bit):	4.954876939644459
Encrypted:	false
SSDEEP:	1536:nf7EzXSAH/axBSy+zotG3xKapfZVYB4gfOKKKKkcsHgcsV1JRJn2Qx:nf7EzCAHyXe0tG3ZBZVYfb5HNsV1c4
MD5:	0C70224F09C65619BC9D6AFC456294C9
SHA1:	975AA4311B2C4FEDE2DB8BD6293F5C54224348C7
SHA-256:	AC0B18AE0851CF5CB499BDCBA6BCE5D260F114768425AEED65CF6086B27A323D
SHA-512:	B72C10B8A3ED94E6E7796A562F860B9AD8F3815A3F3B9A24B98C56BD77A5318EDDCF69E41ADAD5975206C04E220107DF65BABDABF9DB98831BA567947B7936 2
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....e.....0..... ....@.. .....F... ..@.....S.... ..H.....H.....SH..RSn.|J... ...L.....@....text...`.....P..... ..`.rsr c...H.... .....@..@.reloc.....@..B..... ..`.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\RobCleanerInstlr943210[1].exe	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	166912
Entropy (8bit):	4.973976526445888
Encrypted:	false
SSDEEP:	3072:CwM8ll/9+Qa/PHsuH3EbSSSSSabsZGpu:9nQQQacuqSSSSSabsZG
MD5:	A9DED7D6470F741B9F4509863665F74C
SHA1:	FF1A2ABB33D9DD290C9349565586C6C1E445DC1E
SHA-256:	2F326116DF411C1C9AA3728E0C191FD0888FF63DB7DB08CC70DB1F1AEBE88347
SHA-512:	507D729DDC2533616A6DF372BB8C175D44DC5B68D0A455496DE34019FCF685A6EF6A36693CCB9417637CB9783CFD48EDB039274A7C51476FD39F98796B1D78D
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\RobCleanerInstlr943210[1].exe	
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....D.....0..... ....@.. .....N.. ..@.....S.... .....H.....`_...&.tJ... ...L.....@....text...`.....P..... ..`.rsrc..... .....@..@.reloc.....@..B..... ..`.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\appforpr2[1].exe	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	373248
Entropy (8bit):	6.026417129517382
Encrypted:	false
SSDEEP:	6144:EbWxj7XagNorsFTCp64vSMLjYgrkhnuzbgwu:2Wx3a1kO6SS6c9unn
MD5:	0162C08D87055722BC49265BD5468D16
SHA1:	901D7400D1F2BC4A87EDAFD58FEBFAC4891F9FE8
SHA-256:	92F1DF4DBB0E34C38083BB9516FB5C812175B5B73C9FDA81CA8047C5C38A1ABB
SHA-512:	193A12BAF5819BC58B310BFCC5E33EEDD06C130922596A6A4F8A16BC705A28FE3D8E75C689ECFBB970F21D66FEFA7830108F661F0E95586B4D87D1DEFB85A05F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....~...-...-...-..{-...-..m-...-..j-...-.@.-...-...-...-..d-...-..z-...-...-...-Rich...-..... .....PE..L...I.`.....0....@.....@.....U.....]..P....p..X.....1.....P..@.....0..... .....text...#..... ..`.rdata..b7...0...8.....@..@.data.....p.....T.....@....rsrc...X....p.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\ferrari[1].exe	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	433152
Entropy (8bit):	7.166162174008074
Encrypted:	false
SSDEEP:	12288:ouz/1nunbQIcdq0OjU1n8gDhIzClOeLa:8XcUToPyzW
MD5:	DDFE3C0D174EC565750DCACEF9A52363
SHA1:	167091D1ED0001FFBAF1AA0992DB07357006ECF6
SHA-256:	FC6FA06EA3FD29EE6A34A26BA80B0D67C46E297197BE91ECA1C973989B530EFF
SHA-512:	1CDA2E9700573E632247E3F40E103EBFB9E65E7F7BC4366A8481F0FEFDF81A72E4DC6F5DC6471687E79AF96091398A3C9C2C71FC580FC20D5A291E0C8A36B8A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....N..././.}{../.}m../..././.h/.}j../.}z../.}.../.Rich./.....P E..L...z.@_.....k.....@.....\O.....$...<.....0.....@.....@.....L..... .....text..... ..`.data.....@....gux.....@....tuyal.....@....fijut.....@....rsrc...0..... ..@..@.reloc..hG...@...H...T.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\file1[1].exe	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	1685504
Entropy (8bit):	6.162626507555483
Encrypted:	false
SSDEEP:	12288:x0jZxzTGn24nCgKrborzKb7HQt0XT6QVbacjAEoFLXlDh1vzx2ypFlbDCSj:xmKYg2crzKbzQtMGoAEcLXz1vl2aFD
MD5:	DECA67F083AE99A6BB5E9F8E8F31550C
SHA1:	0719EACB9382C830208B99776C96082D1DFC6AF7
SHA-256:	04E3D6D15BCA42B83260D9EAA3FEF9363566E3358BB8A3944510C9ABA67320BE
SHA-512:	496946415C7C94CEAB0FCF361E568A1AF35732B9E3E127E24DDC3E9E45F6E950DF088C8CC8424F790195690842BE8AE80AFE82C333A8138AB680D4D3FFA5EA4
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\file1[1].exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....."....8...d.....@.....`... ..... ...H.....text....6.....8..... ..`.rdata..`w...P...x...>.....@. .@.data...)....d.....@....idata.....@....reloc..... .....@..B.symtab.....B.rsrc.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\file2[1].exe	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	984576
Entropy (8bit):	5.886367576638868
Encrypted:	false
SSDEEP:	12288:8vit3tj7RziMXZT5szTN59w11xCfsmu6PSVaWSAeQQHUx1:/dx1fszTNU1H6smSIWZ7R
MD5:	6D87BD5B6C8585B0FECB45BAD7F3D92B
SHA1:	1C86B60CA044C4BD2D8D7BCA1988FA3F9AA3E998
SHA-256:	930A0D8A21AF9926F0F0863921840281516E48F4A7D2D701F3155BC459EA4047
SHA-512:	9A07A24A003FF14BD27201932529BF58ABB3F0C99D504A798D922BF92BEF47634540E473E90952FE319D53310895AABA3415132A893EEE9B7C51B244E7F3F47A
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0.....N.... ... .@.. .....`..... @.....O.... .....@..... ..... ..H.....text...T.... ..... ..`.rsrc..... .....@..@.reloc .....@.....@..B.....0.....H.....+.....@...X..t.....g.....y....(.B..*.s.;...P...**....(i...*f....(j...r...p(....(k...*f....ol...(m...ol...on.. .*.s.@...u...*f....ol...rM!.p(....on...*f....o....r.!.p(....on...*f....o....r.".p(....(k...*.....o....rk".p(....r...p(....r9..p(....(....on...*f....o....r.".p(....(k...*f....o....r8#.p(....(k...*f....o....r.#.p(....(k... *f....o....r-$.p(....(k...*.~....:#...rw$.p(.....#...(....o....s.....~....*.~....*.~

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\rtst1053[1].exe	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2139648
Entropy (8bit):	6.623110315066958
Encrypted:	false
SSDEEP:	49152:7rEOLD0xW+aJVXfxu3Eosp/qw7RV+uY/:023Jtosp/qw7yb
MD5:	DD3C57E2520A47D634E5FAAC52782FDA
SHA1:	73AF831AA23F72D82FE80E84B0C4411E6A9DCCB6
SHA-256:	03B887397102E717DE5EF8A0D4D0374BDF5347A85DDDC8C829714770142B8FDF
SHA-512:	37F0BE02B923B873DAA2CB98A49C42A1AB2DCB3B9A5422E7B5FECFEDF1A90CE2F00E375A41C1C0331A4B3E3B96B5FBDC267907966AA8406DED1970B42F3E62C
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Generic_malware, Description: Yara Generic_malware, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\rtst1053[1].exe, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\rtst1053[1].exe, Author: Joe Security
Reputation:	unknown
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....i..-..A-..A-..A9..@8..A9..@ ..A9..@...A...@...A...@,..A...@=.. A...@'..A...@...A9..@$..A-..A..A...@%..A...A,..A-.pA,..A...@,..ARich-..A.....PE..d.....a....."..... .....}.....@..... !.....`..... .....DJ..d.....J.....`..... ..#.. :..p.....:..(...:..0.....8.....text..... ..`.rdata...[.....\.....@..@.data.....`..^.. .N.....@....pdata..`.....@..@_RDATA.....4.....@..@.rsrc....J.....L...6.....@..@.reloc...#.... ..$.... .....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\setup[1].exe	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	320512
Entropy (8bit):	6.6868421454315765
Encrypted:	false
SSDEEP:	6144:2jGhd+nNOuD3VaUei9OYbsIEEHb7u5eQxNl:2ih4nNOmVMIzbT3Hb+eQ
MD5:	61931A7DE1769BC844394F161F1DE150
SHA1:	B8FE574BA64DC007E8C7979EDD66325D47F3385E
SHA-256:	3CAA10E8DF47D43DF65A31406FC1DFABB529655906DDF4722C673EACE87A0583
SHA-512:	E26DAE9DA25030301CA56944A8A187350C2367330704CF4ED3B7D095A539843CF66F851B415B809BD55592EE697B950A0DB248BD4AA6DFB55571865BFD868EC
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\setup[1].exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....N..././.}{../.}m../..././.h/.}j../.}z../.}.../.Rich./.....PE..L....sh _.....@.....D.....<.....0.....@.....L.....text..... ..`.data.....@....buwice.....@....nok.....@....movezu.....@....rsrc...0.....@..@.re loc..ZF.....H.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\sfx_123_310[1].exe	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2059890
Entropy (8bit):	6.610570975992159
Encrypted:	false
SSDEEP:	24576:08qXhDyUY86L1xqRMjgEo5QfBU7HfLGLhBExe6KY/LJ6Wjv74xJ4s:084cxSyFpULadBa/dbjv74xJ4s
MD5:	3A6EBD3377AFDB9EFC2195E7B6A00A69
SHA1:	2B1F1B36DBC62D52D98F989E6BB90487DCCB3A12
SHA-256:	E85F82C94A0EC6FEDCC459C5CEEE48E5F56C2708C704890420EE56E7C240F0B7
SHA-512:	84162FDD1E423A6D6EBD0A834940DC5E78D1A11AA15BA3983D33314CCFDF4A00CD593728E2FBDC2A3AB73A2B100513566ABCC0DB69DC2A6A401A64F98F8EE C26
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....}.m...m...m..#.a..m..#.c..m..#.b..m....W..m...3./.m...3./.m...3./.m.. .....m.....m...m..nm...3./.m...3./.m...3o..m...3./.m..Rich.m.....PE..L....B`.....b.....0?.....@.....@.....@.....4.....< .....`.. (.. ...T.....H...@..... .....text....a.....b..... ..`.rdata..$.....f.....@..@.data....M... .....@....dida t..\....p.....@....rsrc.....@..@.reloc.. (...`...*.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\vcruntime140[1].dll	
Process:	C:\Users\user\Pictures\Adobe Films\JiryxVDn0P_ka7w2xP8PdulD.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	83784
Entropy (8bit):	6.890347360270656
Encrypted:	false
SSDEEP:	1536:AQXQNgAuCDeHFtg3uYQkDqiVsv39niI35kU2yecbVKHHwhbfugbZyk:AQXQNVDeHFtO5d/A39ie6yecbVKHHwJF
MD5:	7587BF9CB4147022CD5681B015183046
SHA1:	F2106306A8F6F0DA5AFB7FC765CFA0757AD5A628
SHA-256:	C40BB03199A2054DABFC7A8E01D6098E91DE7193619EFFBD0F142A7BF031C14D
SHA-512:	0B63E4979846CEBA1B1ED8470432EA6AA18CCA66B5F5322D17B14BC0DFA4B2EE09CA300A016E16A01DB5123E4E022820698F46D9BAD1078BD24675B4B181E91 F
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....NE...E...E.....".G...L.^.N...E...l.....U.....V.....A....._.....D..... 2.D.....D...RichE.....PE..L....8'Y....."!..... .....@.....@A..... .....H?...0.....8.....@..... .....text..... ..`.data...D.....@....idata.....@..@.rsrc..... .....@..@.reloc.....0.....@..B.. ....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	14037
Entropy (8bit):	4.9555046258978965
Encrypted:	false
SSDEEP:	384:Vfib4GGVoGIpN6KQkj2Akjh4iUxwRdLYoV4fib41:VIGV3IpNBQkj25h4iUxwRdLYoV4j
MD5:	1B045E1975577D5143651EBA9B57CD51
SHA1:	2F460A4014618062DD62BA5E3E461F8559EB8D48
SHA-256:	7CFCAAB1865BB344C22FFE0DFBC16B6B5C4B0C2A8425A374670B3E81AD1DA4CC
SHA-512:	91E8CC2FC5CBD273938AC05CB0297772DBE44D187B88DA4CE64D6D16CFC75EA34352725737559E6D01CCB78CE2F36E8B2363307C0EF752515D529246AC4782
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Preview:	PSMODULECACHE.....P.e...S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo .....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscRe source.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.... ....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....7r8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriv eItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

C:\Users\user\AppData\Local\Temp\01913ed7-c54a-4682-ba7f-2339dfb12dae.exe	
Process:	C:\Users\user\Pictures\Adobe Films\eULKoZpb_80D8HrRwSiJF82y.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	340480
Entropy (8bit):	7.875512918506953
Encrypted:	false
SSDEEP:	6144:XjnvDkxx8ujS553hhe+NNO45EiT2//ncIgUfDxkOAM1ChsFso:TvwE5brQ+8nHHxPAM1C6Fs
MD5:	9734ED168A74A29DC30C2273FE7AEDDC
SHA1:	6D4598EC63247C41E28F4A242AE53EC731AEE166
SHA-256:	473B4D73DC74EED19D2AA100AACFBBC1B5186B78DEA9DFBF9EC0A7517622E86A
SHA-512:	C32F5C4BC5A9D8430C690E4484423384E6805AE51812F0F100177BA67B2A09B4671C8804E57E9A90B934B8B7B59E42EC66F8FA2E7F6F0419AC246CCFEC73954D
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....I.a.....\..... ....@.. ....@.....O...`.....H.....[O\C].R... ...T.....@....text...P.....X..... ..`.rsrc.....` .....(.....@..@.reloc.....@..B.....0..... ..`..... ....

C:\Users\user\AppData\Local\Temp\11111.exe	
Process:	C:\Users\user\Pictures\Adobe Films\SiJXWwfMYK4L8VTC7HncQkab.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	400896
Entropy (8bit):	6.6614853002356
Encrypted:	false
SSDEEP:	6144:ME+Z7EAXrvPRIxK0zBL/TIDC2dL3RltnfoBglM7zMUdsvk3zrAtc6zkizX:8Z7FXrPy4ix+LBltsgK7zXIqUkk
MD5:	7165E9D7456520D1F1644AA26DA7C423
SHA1:	177F9116229A021E24F80C4059999C4C52F9E830
SHA-256:	40CA14BE87CCEE1C66CCE8CE07D7ED9B94A0F7B46D84F9147C4BBF6DDAB75A67
SHA-512:	FE80996A7F5C64815C19DB1FA582581AA1934EA8D1050E686B4F65BCDD000DF1DECDF711E0E4B1DE8A2AA4FCB1AC95CEBB0316017C42E80D8386BD3400FCA ECB
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: C:\Users\user\AppData\Local\Temp\11111.exe, Author: Joe Security
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....L..-...-...-..4"...-..4"...-.....-..-....-...-...,.....-.....-.....-.....-..Rich.- .....PE..L.....^.....J.....f.....@.....lv.....0..... text...J..... ..`.rdata.....@..@.data.....@....rsrc.....0.....@..@..... ....

C:\Users\user\AppData\Local\Temp\4c91d8e5-f330-473d-bea7-49691b483a08.exe	
Process:	C:\Users\user\Pictures\Adobe Films\kXM34tDnyQtIWwfvEKDMhvoQ.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	586608
Entropy (8bit):	7.9520986935334035
Encrypted:	false
SSDEEP:	12288:wa2VzKsLoUg/F6Vk1RKohU38X75zdt0B8N/SSVs8gZGuM8F2FVrn:WZXo/d6G1Rfhv75xmB8N/h2bG984zn
MD5:	309F89D4E7F28E93B0CB02D7A5806F6C
SHA1:	3BCCC6828FD97840EE7A6AFEB180CD756B4A5124
SHA-256:	4FAE76FD06068B91A9AC1E5164232447481DA7E0B3F16079FB617BE3418F3D55
SHA-512:	7B03E21107476A2A3CBC5600CDDF4D352B47DF92BFCC73FB9501056A49F5FF28839B489BACFB40BFB3147D813FF115412D86E66A9665C59067145BEE74EB456(
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\4c91d8e5-f330-473d-bea7-49691b483a08.exe	
Preview:	MZ.E@.....}..J$....4..d".R.3.r..S.._.....X.....4../..t.....Q..... .....PE..L....f.a.....0.....@..... .....p..H.....K..... ...`.....`.....p.....@....rsrc....K.....H.....@..@.....P.....@.....n....R.....@..... .....+.....G....'..&O.u....L#e

C:\Users\user\AppData\Local\Temp\70bb7193-ad9a-4e0f-ae94-6f57b7571a61.exe	
Process:	C:\Users\user\Pictures\Adobe Films\kXM34tDnyQtIWwfvEKDMhvoQ.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	660208
Entropy (8bit):	7.96008450637029
Encrypted:	false
SSDEEP:	12288:H/H8hZVlnMWq5tizLq1qsWO5+Vgz/v2q2kjUE1WhrZ:H/Yn6CGqsWMt7+jkjUn
MD5:	978137D4F66C79D0EC1B931A7BE4BC63
SHA1:	FA14332A662DA4CB7D50F1E0E8C2B465B9C84798
SHA-256:	94D16DD4C1D5D14E81CF91829A8147871234B7B76925C6D33823F70D23FF27A1
SHA-512:	27AA860CFA401C2E9803CE46EB24701802A113D0B535572E41CDA8986F8D4C825F96A8459DC09BD255AD8C89796BA75982815597925FAF23C52B1BEE6B4116E5
Malicious:	false
Reputation:	unknown
Preview:	MZ.E@.....}..J$..y.....DY..^./.X..W.(...5.<.Ik.~'..>.....Q..... .....PE..L....f.a.....@.....@.....M7..... .....P.....8J..... .....p.....`.....@....rsrc...8J.....vF.....@..@.....N.....@.....P.....@..... .....+.....}.....^.....@....

C:\Users\user\AppData\Local\Temp\7469216e-9689-4de8-a329-fc4dce5fd660.exe	
Process:	C:\Users\user\Pictures\Adobe Films\kXM34tDnyQtIWwfvEKDMhvoQ.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	157184
Entropy (8bit):	4.841913685992838
Encrypted:	false
SSDEEP:	1536:W2fF5Px4juCHpbOejJJJJJxg+cSSSSmKKKKnNfKH4XNp/VK:W295yjuePjJJJJJxg+LU4XPw
MD5:	3CED7D2FF590465056530EF500AD7B2C
SHA1:	D7A7042E3A2DE77B8D24FA64828137AD76F7B2F5
SHA-256:	F10F5995C59A1CEEB696DC758FED2F1778A419AD1BF0FFB468A75D1C6152356F
SHA-512:	F93CB7BBA89DC4B8D689E7151D960F9E5E7063A10EC348807A6725DA0B0C15CA767D3FF99F6284F6E25DC1EF2A1EA09C91605A933BC2301ED3BF27DC0FBABA 2E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....@;.....".....0..|..... ....@.. .....r.. ..@.....\...O.....H.....3.^.=&*^LB... ...D.....@....text....x.....z...H..... ..`.rsr c.....@..@.reloc.....b.....@..B.....d..... ..`..... .....

C:\Users\user\AppData\Local\Temp\78-98edf-b53-e3daf-74e31577faa14\Kenessey.txt	
Process:	C:\Users\user\AppData\Local\Temp\is-MBHBG.tmp_____djskjT76(((.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:KWigXn:KWigXn
MD5:	97384261B8BBF966DF16E5AD509922DB
SHA1:	2FC42D37FEE2C81D767E09FB298B70C748940F86
SHA-256:	9C0D294C05FC1D88D698034609BB81C0C69196327594E4C69D2915C80FD9850C
SHA-512:	B77FE2D86FBC5BD116D6A073EB447E76A74ADD3FA0D0B801F97535963241BE3CDCE1DBCAED603B78F020D0845B2D4BFC892CEB2A7D1C8F1D98ABC4812EF5/ F21
Malicious:	false
Reputation:	unknown
Preview:	installer

C:\Users\user\AppData\Local\Temp\78-98edf-b53-e3daf-74e31577faa14\Ledaparifa.exe	
Process:	C:\Users\user\AppData\Local\Temp\is-MBHBG.tmp_____djskjT76(((.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

C:\Users\user\AppData\Local\Temp\78-98edf-b53-e3daf-74e31577faa14\Ledaparifa.exe	
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	6144:ezn5wRH9Z04nxJyzqDEu5UtNw1U9Tiq01jSCXu/7+QxDiM5snMvB0EmKLZPDvOBU:ezn5wRsi52w1/q0m7hf3bvOBpXEJn1
MD5:	D63BDAFB7AAA3B7C513EB42F1A867157
SHA1:	34B29B47E01756724F9697A975472F6DC23DB7F5
SHA-256:	A1196F944FB9C558F7D43DD3C2FF3563009675184118CF7C76B8C94C5D719DA7
SHA-512:	444312E869015C4161874F8ADA6B4C644540CB5893EDE7D79853BA3C3CB762E8BD3C1BF81763F853E7B1DE9AA4ECC4262CE8583E99AE563E0697477349BC774
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.../!.a..... .....@.. ....@.....@...K..... ....H.....text..... ....`.sdata.....@....rsrc..... .....@..@.reloc.....v.....@..B.....

C:\Users\user\AppData\Local\Temp\7b7bd5d8-d30e-4948-8b49-a7ff0ac8d3a1.exe	
Process:	C:\Users\user\Pictures\Adobe Films\eULKoZpb_80D8HrRwSiJF82y.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	660208
Entropy (8bit):	7.96008450637029
Encrypted:	false
SSDEEP:	12288:H/H8hZVlnMWq5tizLq1qsWO5+Vgz/v2q2kjUE1WhrZ:H/Yn6CGqsWMt7+jkjUn
MD5:	978137D4F66C79D0EC1B931A7BE4BC63
SHA1:	FA14332A662DA4CB7D50F1E0E8C2B465B9C84798
SHA-256:	94D16DD4C1D5D14E81CF91829A8147871234B7B76925C6D33823F70D23FF27A1
SHA-512:	27AA860CFA401C2E9803CE46EB24701802A113D0B535572E41CDA8986F8D4C825F96A8459DC09BD255AD8C89796BA75982815597925FAF23C52B1BEE6B4116E5
Malicious:	false
Reputation:	unknown
Preview:	MZ.E@.....}..J$..y.....DY..^./.X..W.(...5.<.Ik.~'..>.....Q..... .....PE..L....f.a.....@.....@.....M7..... .....P.....8J..... .....p.....`.....@....rsrc...8J.....vF.....@..@.....N.....@.....P.....@..... .....+.....}.....^.....@....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ocdgehdf.x01.psm1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qg3ngdzw.dzt.ps1	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qg3ngdzw.dzt.ps1	
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp\a8155a24-6afe-4a8d-b55c-3e9f9c8f0596.exe	
Process:	C:\Users\user\Pictures\Adobe Films\eULKoZpb_80D8HrRwSiJF82y.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	587792
Entropy (8bit):	7.9520976752586074
Encrypted:	false
SSDEEP:	12288:pUH9E/eyndr1gyfA0XHoboTNEJePb4ULm2WcP6DJdQ7HQ15cwqWy+n:pUH9Edd1A0FNEJqm2WcSDwQ/1
MD5:	87487BB57FA27A114D4569F951F532AC
SHA1:	962D09F29AE25823454C605C7250A70FBA9B32FC
SHA-256:	8D28DFDD872CAEC8C03569128173047703DC16B19B131CD4B375CDD2F655DA1B
SHA-512:	1CFC4EAA5DD28AFE48F763146E52624F2A42E6489B74C906B88C97DDF89F36AEAD9462BB1B7295A858D05F07BF8EC79839FC372C87C03F58FCE9B0518D20188
Malicious:	false
Reputation:	unknown
Preview:	 MZ.E@.....}..J$..U:C]....4h.B.....G.....,$y(jN_C.UT..I.....Q..... .....PE..L....f.a.....@.....@.....'..... .....D.....F..... .....p.....`.....@....rsrc....F.....D.....@..@.....L.....@.....N.....@..... .....+.....|.....:....e

C:\Users\user\AppData\Local\Temp\c95bc0fc-f0aa-44e0-82a7-7cd172480ab6.exe	
Process:	C:\Users\user\Pictures\Adobe Films\eULKoZpb_80D8HrRwSiJF82y.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	157696
Entropy (8bit):	4.85110399306064
Encrypted:	false
SSDEEP:	1536:kpE4mbmjZLtQyAlf2HszpGvqJMJJJJJxg+cSSSSmKKKKnNfKH4XNp/VK:kpAbmj5tQvlf2KMJJJJJxg+LU4XPw
MD5:	E3FD169B40795DBB7CF48D5FC66B8ED3
SHA1:	1C8BEA5CD4EDF84124E64B34ACE6546D72AD9783
SHA-256:	6A36C03EFDE61A3806DC8E454F7F92F7C743A0882E51F2D439F1D46B6571AAA1
SHA-512:	2EC2F74E6B94C0C6567ACA473A4F9DF1CB0CD1CB8EE4D67C087B3EBAD99FBDFD5251239653F60F5FE4DF158F39786DDD2456051B025D54DD0C38B30BFF01D E7
Malicious:	false
Reputation:	unknown
Preview:	 MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....@;.....".....0..|..... ....@.. .....%.. ..@.....K.....H.....g!ny.KP+hD... ...F.....@....text...8x.....z...J..... ..`.rsr c.....@..@.reloc.....d.....@..B.....f..... ..`..... .....

C:\Users\user\AppData\Local\Temp\dce6bd67-7e1f-466b-94f1-f9f5c2acf9dd.exe	
Process:	C:\Users\user\Pictures\Adobe Films\kXM34tDnyQtIWwfvEKDMhvoQ.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	338944
Entropy (8bit):	7.873711406291665
Encrypted:	false
SSDEEP:	6144:NnjgA74tOje1fdnrg3nRrd7MfgM+pMA2lt07RZc56HrdwIQc:OtOjePnrg3nNWIX2x+Zu6Hrh
MD5:	748DBD76B3D32F174DEBD3BD296A2C4D
SHA1:	E6DD0F6344BEF30209E58C5448E8109C635F2BF2
SHA-256:	5F12A7FFA468931565D2D01827C5E6D12FA69ADA88C0A9383A352AF9F79C8F31
SHA-512:	783D2BACF2B17E659F1D3E51B607D2B77317510963720540E7C6E2E0655A2DAFE168545B1665CE1E4893466BE652A642CE8838219A87B7EC2EB1B0F3CF22F9F7
Malicious:	**true**
Reputation:	unknown
Preview:	 MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....I.a.....V..... ....@.. ....@.....W...`.....H.....8nx9=]N~.L.. ...N.....@....text...`.....R..... ..`.rsr c.....`.....".....@..@.reloc.....(.....@..B.....*..... ..`..... .....

C:\Users\user\AppData\Local\Temp\dd-cf194-64d-5a3ae-892e29c1cf407\Jaxuxyleda.exe	
Process:	C:\Users\user\AppData\Local\Temp\is-MBHBG.tmp_____djskjT76(((.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	6144:HDHBMXu/7+QxDiM5snMvB0EmKLZPDvOBpqgOMcIsI4oF6cuz:TB57hf3bvOBpX4y6
MD5:	7F9B48E1096C162D3D0615E43D935A04
SHA1:	D649B2FC357162741554C9E728E68209CA386BEE
SHA-256:	E845049F572E60F5D8DEBEBF492F06F57AAC4FABD31054D03C4149F8392E019F
SHA-512:	F0701E0FF9BB56080D62AB46B5656C530F212ACF795CC7C36EFE19AC4D97E94DFF00F59B1564103A2457FF208411D33A47705B02B07F992F39BE1C5DDFA7CEE
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...q..a.....$.....~.... .....@.. .....`..... ..@.....0...K.... .....@..... ..... ..H.....text..... ..... ..`.sdata.....@....rsrc..... .....@..@.reloc.....@.....@..B..... ....

C:\Users\user\AppData\Local\Temp\dd-cf194-64d-5a3ae-892e29c1cf407\Jaxuxyleda.exe.config	
Process:	C:\Users\user\AppData\Local\Temp\is-MBHBG.tmp_____djskjT76(((.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	24:2dZmht+SDfy4GOy4TO4q5X4tndGubyB8GRyF:ccdfy4G74TO4qN4hRN
MD5:	98D2687AEC923F98C37F7CDA8DE0EB19
SHA1:	F6DCFCDCFE570340ECDBBD9E2A61F3CB4F281BA7
SHA-256:	8A94163256A722EF8CC140BCD115A5B8F8725C04FE158B129D47BE81CB693465
SHA-512:	95C7290D59749DF8DF495E04789C1793265E0F34E0D091DF5C0D4AEFE1AF4C8AC1F5460F1F198FC28C4C8C900827B8F22E2851957BBAEA5914EA962B3A1D059
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8" ?>..<configuration>.. <startup useLegacyV2RuntimeActivationPolicy="true">.. <system.xml.serialization>.. <xmlSerializer useLegacySerializerGeneration="true"/>.. </system.xml.serialization>.. <supportedRuntime version="v2.0.50727"/>.. <supportedRuntime version="v4.0" sku =".NETFramework,Version=v4.0,Profile=Client" />.. <supportedRuntime version="v4.0" sku =".NETFramework,Version=v4.0" />.. <supportedRuntime version="v4.0" sku =".NETFramework,Version=v4.0.1,Profile=Client" />.. <supportedRuntime version="v4.0" sku =".NETFramework,Version=v4.0.1" />.. <supportedRuntime version="v4.0" sku =".NETFramework,Version=v4.0.2,Profile=Client" />.. <supportedRuntime version="v4.0" sku =".NETFramework,Version=v4.0.2" />.. <supportedRuntime version="v4.0" sku =".NETFramework,Version=v4.0.3,Profile=Client" />.. <supportedRuntime version="v4.0" sku =".NETFramework,Version=v4.0.3" />.. <supportedRuntime version="v4.0" sku =".NETFramework,Version=v

C:\Users\user\AppData\Local\Temp\fl.exe	
Process:	C:\Users\user\Pictures\Adobe Films\C1aYSYmMy9tQLrifaCN41EQ8.exe
File Type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	4305408
Entropy (8bit):	**7.9911404738712575**
Encrypted:	**true**
SSDEEP:	49152:ytvLJ8aVdjB0WyEnmG3KLeEE85uuglA1M/VCPSPMcoH6Tg3LIpumuH9Raa9hFVwT:opVZBhMLesuJl3+SrozI4muTagmab
MD5:	148A71FE5BFA1675691EE37FD79DEBCE
SHA1:	5AE6D8CFF109371043F6E220BCAAC44CBA28A0F1
SHA-256:	77F247FC20E89E3EA48DE49AC691A5ABB02112D28BAF639463EC7A0B086F493B
SHA-512:	75E26DCF73D7E3CD7128037F933CC5A9F2F4564EA057175A7FEE49F7DBB83CEFD266E4F2E59D393FEC3DB218C981C41D73E191787F4DC8CDC0A5A71146AEEI D3
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....a....."....."..... .....@..... .....@...@.....@..... .....`.....o..H.....text....j... ..... ..`.vmp0...z. .....`.. `.vmp1.....A...?...A.....`..`.rsrc.....`.....A.....@..@..... .....reloc. .....

C:\Users\user\AppData\Local\Temp\is-FNG8T.tmp\P65Nqt8GfRApLpFwJ9bOb7YH.tmp	
Process:	C:\Users\user\Pictures\Adobe Films\P65Nqt8GfRApLpFwJ9bOb7YH.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped

C:\Users\user\AppData\Local\Temp\is-FNG8T.tmp\P65Nqt8GfRApLpFwJ9bOb7YH.tmp	
Size (bytes):	883200
Entropy (8bit):	6.427161951853137
Encrypted:	false
SSDEEP:	24576:iQYh1yLmSKrPD37zzH2A6QD/IpqggE2CfNaftvyyx9dy:a02rPD37zzH2A6SBIfNaftvX6
MD5:	7FC94D54F886839996FB02FBBE1B42C8
SHA1:	E14184155C18A79382266569252FA754FC69C169
SHA-256:	9E0606D367E9F0504449C11C155B483A10C3FC3CB438B81467E6966ECF1CA6FE
SHA-512:	B7B89D112AF83CAD362A6D6834787FD5B6CE59C6129F8CF09D28F2D215E632E9EDACCC64431D5118D332707926F8BAB0B9FDFEC7CFA1FE7500F0BE18A10630D
Malicious:	**true**
Reputation:	unknown
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....@.....p.....@.....@.....&.....0..... .....CODE....$..... ..`DATA.... .....@...BSS.....idata...&.....(.....@....tls.....rdata..... ... .@..P.reloc.....0.....@..P.rsrc.....@..P.....f.....@..P..... .....

C:\Users\user\AppData\Local\Temp\is-MBHBG.tmp_____djskjT76(((.exe	
Process:	C:\Users\user\AppData\Local\Temp\is-FNG8T.tmp\P65Nqt8GfRApLpFwJ9bOb7YH.tmp
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	867840
Entropy (8bit):	5.623588278659965
Encrypted:	false
SSDEEP:	6144:rSTibEKFBZ2UoI0YXu/7+QxDiM5snMvB0EmKLZPDvOBpqgOMLmTgVZk:uKju7hf3bvOBpXLy
MD5:	16B30C7902FC1B0A34744C95A64E332B
SHA1:	B0C6E9CCBDC992EC40951D7D03EEB3190F24042E
SHA-256:	B4DE777B819328EF831CA297F8240F21D200B184B0FE89745C62935C7DFDA2DE
SHA-512:	7FFE4D05BE6928C40AF78B054472077A6FA890A869FDB0BE29A54F140C675BE30EE39E152496055FEDC0DC4EFE75E97EFF52B2F40157CC59001F0AC59FA38A4F
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...&.....z.....~.... .....@.. ....@.....0...K..... ....H.....text....y... ...z..... ..`.sdata.....~.....@....rsrc..... .....@..@.reloc.....<.....@..B..... .....

C:\Users\user\AppData\Local\Temp\is-MBHBG.tmp_isetup_setup64.tmp	
Process:	C:\Users\user\AppData\Local\Temp\is-FNG8T.tmp\P65Nqt8GfRApLpFwJ9bOb7YH.tmp
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	6144
Entropy (8bit):	4.720366600008286
Encrypted:	false
SSDEEP:	96:sfkcXegaJ/ZAYNzcld1xaX12p+gt1sONA0:sfJEVYlvxaX12C6A0
MD5:	E4211D6D009757C078A9FAC7FF4F03D4
SHA1:	019CD56BA687D39D12D4B13991C9A42EA6BA03DA
SHA-256:	388A796580234EFC95F3B1C70AD4CB44BFDDC7BA0F9203BF4902B9929B136F95
SHA-512:	17257F15D843E88BB78ADCFB48184B8CE22109CC2C99E709432728A392AFAE7B808ED32289BA397207172DE990A354F15C2459B6797317DA8EA18B040C85787E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....^.....I.....=\.....=\.....=\.....Rich.....PE.. d.....R.....#.....@.....`.....<!.....P..H....@..0..... .....text..... ..`.rdata..|.... .....@..@.data...,....0.....@....pdata..0....@.....@..@.rsrc...H....P.....@..@..... .....

C:\Users\user\AppData\Local\Temp\is-MBHBG.tmp_isetup_shfoldr.dll	
Process:	C:\Users\user\AppData\Local\Temp\is-FNG8T.tmp\P65Nqt8GfRApLpFwJ9bOb7YH.tmp
File Type:	PE32 executable (DLL) (GUI) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	23312
Entropy (8bit):	4.596242908851566
Encrypted:	false
SSDEEP:	384:+Vm08QoKkiWZ76UJuP71W55iWHHoSHigH2euwsHTGHVb+VHHmnH+aHjHqLHxmoq1:2m08QotiCjJuPGw4

C:\Users\user\AppData\Local\Temp\is-MBHBG.tmp_isetup_shfoldr.dll	
MD5:	92DC6EF532FBB4A5C3201469A5B5EB63
SHA1:	3E89FF837147C16B4E41C30D6C796374E0B8E62C
SHA-256:	9884E9D1B4F8A873CCBD81F8AD0AE257776D2348D027D811A56475E028360D87
SHA-512:	9908E573921D5DBC3454A1C0A6C969AB8A81CC2E8B5385391D46B1A738FB06A76AA3282E0E58D0D2FFA6F27C85668CD5178E1500B8A39B1BBAE04366AE6A86D3
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....IzJ^..$...$...$...%.".$.T87...$.[."...$...$...$.Rich..$.....PE..L.....\;.....#..... ...4.....'.....0.....q.....k...l)..<....@.../.....p..T.....text...{..... ....`.data...\....0.....&.....@....rsrc..../...@...0...(.....@..@.reloc.....p.....X.....@..B..... ....

C:\Users\user\AppData\Local\Temp\is-MBHBG.tmp\idp.dll	
Process:	C:\Users\user\AppData\Local\Temp\is-FNG8T.tmp\P65Nqt8GfRApLpFwJ9bOb7YH.tmp
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	221184
Entropy (8bit):	6.422522500850037
Encrypted:	false
SSDEEP:	3072:6XHWOJd5D0ocxYF0+CT4zNHNpwZNjlhBKL/kg/0r4YLuztNJaFlCx:6G6tae7wZNOpiWP
MD5:	8F995688085BCED38BA7795F60A5E1D3
SHA1:	5B1AD67A149C05C50D6E388527AF5C8A0AF4343A
SHA-256:	203D7B61EAC96DE865AB3B586160E72C78D93AB5532B13D50EF27174126FD006
SHA-512:	043D41947AB69FC9297DCB5AD238ACC2C35250D1172869945ED1A56894C10F93855F0210CBCA41CEEE9EFB55FD56A35A4EC03C77E252409EDC64BFB5FB821C5
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;..;..;....B.....B.....B.....2...;.....B..7....B..:....B..:....B..:....Rich;.....PE..L...)".T.....!....._.....DB.....P.....d....@.....P.....`.....@.....text....{..... ..`.rdata...l.....p.....@..@.data...`9..... .....@....rsrc.....@..... .....@..@.reloc...+...P...0...0.....@..B..... ....

C:\Users\user\AppData\Local\Temp\pidHTSIGEi8DrAmaYu9K8ghN89.dll	
Process:	C:\Users\user\Pictures\Adobe Films\NNNBSubeVPxRXeeZnGu7gQkK.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	171520
Entropy (8bit):	6.254386787351419
Encrypted:	false
SSDEEP:	3072:tw96uifZtOVSgpyt2RGe2SOrC4WOcfV+UmLosIwW:GE2Sgct82tCOcfX
MD5:	F07AC9ECB112C1DD62AC600B76426BD3
SHA1:	8EE61D9296B28F20AD8E2DCA8332EE60735F3398
SHA-256:	28859FA0E72A262E2479B3023E17EE46E914001D7F97C0673280A1473B07A8C0
SHA-512:	777139FD57082B928438B42F070B3D5E22C341657C5450158809F5A1E3DB4ABDED2B566D0333457A6DF012A4BBE3296B31F1CAA05FF6F8BD48BFD705B0D30524
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....vM..vM..vM.rL..vM.uL..vM.sLG.vM.rL..vM.uL..vM.sL..vM.wL..vM..wM..vM...L..vM...M..vM..tL..vMRich..vM.....PE..d.....<a....." .....TZ.....`.....z..(..... .....X..8.....X..0.....text..... ..`.rdata..`.....@..@.data.....n.....@....pdata.....z..... .....@..@_RDATA.....@..@.rsrc.....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\Temp\sport.exe	
Process:	C:\Users\user\Pictures\Adobe Films\0y_alCQBJv4J1LDnCOe55cop.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	2017040
Entropy (8bit):	7.919713794877077
Encrypted:	false
SSDEEP:	49152:GACD+K95aLs7kBlURd7zxCLt2RUlWxAcCbRaELb:GACD+K95aY71y8WUxnC9zb
MD5:	F9F4221AE3F35A92683CAC17358B831D
SHA1:	E1299E13DD44CDF129D8B498B60BFF7CF6F7D563
SHA-256:	003B3FFA5A79CA2045DF425EB6A699038B8C08C3F2B54042B2AD023694D0BCAA

C:\Users\user\AppData\Local\Temp\sport.exe	
SHA-512:	5A723731206AA1E6F0C8ED2A3AF4CCF0F29D630E883CFFE15F0E344AAF8CE9D1F7E94FCCC39E5286621C86C3BA454766319F1D0E6F03DAE50646D5A0E5E13FB
Malicious:	false
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(3...32.....f.....C'B{b.........+..R...d:.....Q..... ....PE..L...b.fa.....P?.....0....@.....@.....;.....@.....02.\....@2..... ...rdata... 2.....`.itext.....02.....@....rsrc.....@2..m.....@..@.CRT.....P?..x...t.....@..... .....}m..V.\..|W.3c.=..... @..p.4.

C:\Users\user\AppData\Local\Temp\tmp121E.tmp	
Process:	C:\Users\user\AppData\Local\Temp\01913ed7-c54a-4682-ba7f-2339dfb12dae.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	361224
Entropy (8bit):	6.050962807966151
Encrypted:	false
SSDEEP:	6144:xgbV/njhcI8II6ROG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxin4:xgxnuzII7GNPUZ+w7wJHyEtAW5
MD5:	13AC615812A78AE2750546F4B80788BC
SHA1:	AE717A912A0462EB6339EFBA43288C56AF6AFB49
SHA-256:	69D5ECDBDD0F12C6996F77A49157631F2FE449A877507C2B6F042FF9E0DE807D
SHA-512:	072CE962C1B2B15C118F993F64646112470CA48802693B1F4A95492AF39FBD4145A1894432D345441A2973D2698E0E734C29BDF70FB928144D3E8DD137728051
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601479294004414e+12,"network":1.601454638e+12,"ticks":615959194.0,"uncertainty":4316795.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\tmp1310.tmp	
Process:	C:\Users\user\AppData\Local\Temp\dce6bd67-7e1f-466b-94f1-f9f5c2acf9dd.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp1AE1.tmp	
Process:	C:\Users\user\AppData\Local\Temp\dce6bd67-7e1f-466b-94f1-f9f5c2acf9dd.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	361224
Entropy (8bit):	6.050962807966151
Encrypted:	false
SSDEEP:	6144:xgbV/njhcI8II6ROG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxin4:xgxnuzII7GNPUZ+w7wJHyEtAW5
MD5:	13AC615812A78AE2750546F4B80788BC
SHA1:	AE717A912A0462EB6339EFBA43288C56AF6AFB49
SHA-256:	69D5ECDBDD0F12C6996F77A49157631F2FE449A877507C2B6F042FF9E0DE807D
SHA-512:	072CE962C1B2B15C118F993F64646112470CA48802693B1F4A95492AF39FBD4145A1894432D345441A2973D2698E0E734C29BDF70FB928144D3E8DD137728051
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\tmp1AE1.tmp	
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601479294004414e+12,"network":1.601454638e+12,"ticks":615959194.0,"uncertainty":4316795.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\tmp3259.tmp	
Process:	C:\Users\user\AppData\Local\Temp\01913ed7-c54a-4682-ba7f-2339dfb12dae.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp4D4C.tmp	
Process:	C:\Users\user\AppData\Local\Temp\dce6bd67-7e1f-466b-94f1-f9f5c2acf9dd.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp52B3.tmp	
Process:	C:\Users\user\AppData\Local\Temp\dce6bd67-7e1f-466b-94f1-f9f5c2acf9dd.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	361224
Entropy (8bit):	6.050962807966151
Encrypted:	false
SSDEEP:	6144:xgbV/njhcI8II6ROG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxin4:xgxnuzII7GNPUZ+w7wJHyEtAW5
MD5:	13AC615812A78AE2750546F4B80788BC
SHA1:	AE717A912A0462EB6339EFBA43288C56AF6AFB49
SHA-256:	69D5ECDBDD0F12C6996F77A49157631F2FE449A877507C2B6F042FF9E0DE807D
SHA-512:	072CE962C1B2B15C118F993F64646112470CA48802693B1F4A95492AF39FBD4145A1894432D345441A2973D2698E0E734C29BDF70FB928144D3E8DD137728051
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601479294004414e+12,"network":1.601454638e+12,"ticks":615959194.0,"uncertainty":4316795.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\tmp52B3.tmp

C:\Users\user\AppData\Local\Temp\tmp61F6.tmp	
Process:	C:\Users\user\AppData\Local\Temp\01913ed7-c54a-4682-ba7f-2339dfb12dae.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	361224
Entropy (8bit):	6.050962807966151
Encrypted:	false
SSDEEP:	6144:xgbV/njhcI8II6ROG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxin4:xgxnuzII7GNPUZ+w7wJHyEtAW5
MD5:	13AC615812A78AE2750546F4B80788BC
SHA1:	AE717A912A0462EB6339EFBA43288C56AF6AFB49
SHA-256:	69D5ECDBDD0F12C6996F77A49157631F2FE449A877507C2B6F042FF9E0DE807D
SHA-512:	072CE962C1B2B15C118F993F64646112470CA48802693B1F4A95492AF39FBD4145A1894432D345441A2973D2698E0E734C29BDF70FB928144D3E8DD137728051
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601479294004414e+12,"network":1.601454638e+12,"ticks":615959194.0,"uncertainty":4316795.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\tmp6A99.tmp	
Process:	C:\Users\user\AppData\Local\Temp\dce6bd67-7e1f-466b-94f1-f9f5c2acf9dd.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	361224
Entropy (8bit):	6.050962807966151
Encrypted:	false
SSDEEP:	6144:xgbV/njhcI8II6ROG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxin4:xgxnuzII7GNPUZ+w7wJHyEtAW5
MD5:	13AC615812A78AE2750546F4B80788BC
SHA1:	AE717A912A0462EB6339EFBA43288C56AF6AFB49
SHA-256:	69D5ECDBDD0F12C6996F77A49157631F2FE449A877507C2B6F042FF9E0DE807D
SHA-512:	072CE962C1B2B15C118F993F64646112470CA48802693B1F4A95492AF39FBD4145A1894432D345441A2973D2698E0E734C29BDF70FB928144D3E8DD137728051
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601479294004414e+12,"network":1.601454638e+12,"ticks":615959194.0,"uncertainty":4316795.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0lyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\tmp787C.tmp	
Process:	C:\Users\user\AppData\Local\Temp\01913ed7-c54a-4682-ba7f-2339dfb12dae.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\tmp787C.tmp	
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmp78E8.tmp	
Process:	C:\Users\user\AppData\Local\Temp\01913ed7-c54a-4682-ba7f-2339dfb12dae.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	691
Entropy (8bit):	5.163559264201053
Encrypted:	false
SSDEEP:	12:57DtSA6NW8ibv3fBbBB5ouVux2DOzzn1T/UWoHPw6jewGxMKjX4CIymgSs2uKJXF:BxSAN17vBVL/ux2DOX1YWuHjeTKKjX4L
MD5:	CF2260463527DCFDA0774B4F8EA0461A
SHA1:	0375633752D237AE1A88BC9E45BD08FB8CC42F39
SHA-256:	5F3205FF686CA4CE77312BA060D973EF4C0C0D5F3F7D025CD25FCF66AB56D0B3
SHA-512:	885F63FF5A3287A9B40E95541A282E4F9AE38CBB4B691270198730CB03F7C0C06559A760AFDDD5FE4E580E0B40AC3888427AD18287A6594968CA337FA956BA04
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220114153251..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 301389 (Microsoft Windows NT 10.0.17134.0)..Host Application: PowerShell Get-MpComputerStatus..Process ID: 3832..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220114153251..**********..PS>Get-MpComputerStatus..

C:\Users\user\AppData\Local\Temp\tmp898E.tmp	
Process:	C:\Users\user\AppData\Local\Temp\dce6bd67-7e1f-466b-94f1-f9f5c2acf9dd.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\tmpBA38.tmp	
Process:	C:\Users\user\AppData\Local\Temp\01913ed7-c54a-4682-ba7f-2339dfb12dae.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	361224
Entropy (8bit):	6.050962807966151
Encrypted:	false
SSDEEP:	6144:xgbV/njhcl8II6ROG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxin4:xgxnuzII7GNPUZ+w7wJHyEtAW5
MD5:	13AC615812A78AE2750546F4B80788BC
SHA1:	AE717A912A0462EB6339EFBA43288C56AF6AFB49
SHA-256:	69D5ECDBDD0F12C6996F77A49157631F2FE449A877507C2B6F042FF9E0DE807D
SHA-512:	072CE962C1B2B15C118F993F64646112470CA48802693B1F4A95492AF39FBD4145A1894432D345441A2973D2698E0E734C29BDF70FB928144D3E8DD137728051
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601479294004414e+12,"network":1.601454638e+12,"ticks":615959194.0,"uncertainty":4316795.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTlhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\tmpC4C0.tmp	
Process:	C:\Users\user\AppData\Local\Temp\dce6bd67-7e1f-466b-94f1-f9f5c2acf9dd.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	361224
Entropy (8bit):	6.050962807966151
Encrypted:	false
SSDEEP:	6144:xgbV/njhcl8II6ROG0OP1eVxR+v+F7EFpfY4XB3iE7ZPXYGzLxin4:xgxnuzII7GNPUZ+w7wJHyEtAW5
MD5:	13AC615812A78AE2750546F4B80788BC
SHA1:	AE717A912A0462EB6339EFBA43288C56AF6AFB49
SHA-256:	69D5ECDBDD0F12C6996F77A49157631F2FE449A877507C2B6F042FF9E0DE807D
SHA-512:	072CE962C1B2B15C118F993F64646112470CA48802693B1F4A95492AF39FBD4145A1894432D345441A2973D2698E0E734C29BDF70FB928144D3E8DD137728051
Malicious:	false
Reputation:	unknown
Preview:	{"browser":{"last_redirect_origin":"","shortcut_migration_version":"85.0.4183.121"},"data_use_measurement":{"data_used":{"services":{"background":{},"foreground":{}},"user":{"background":{},"foreground":{}}}},"hardware_acceleration_mode_previous":true,"intl":{"app_locale":"en"},"legacy":{"profile":{"name":{"migrated":true}}},"network_time":{"network_time_mapping":{"local":1.601479294004414e+12,"network":1.601454638e+12,"ticks":615959194.0,"uncertainty":4316795.0}},"os_crypt":{"encrypted_key":"RFBBUEkBAAAA0Iyd3wEV0RGMegDAT8KX6wEAAACMBYze0bKMTIhZGR/AW4M5AAAAAAIAAAAAABBmAAAAAQAAIAAAACoSPhbyumSaNjLuAHEna2OUDn+rpXOk+H/ONjHe5ZwbAAAAA6AAAAAAgAAIAAAADezR1ii2QiPYGPz0Jd0ZQiE5jKOKMttbbwwADHJYDpEMAAAACuIP4EJtfud3aEFZzvijkFSTP1RNwcy8fFg19xXfiV1Q9wriZb5iS+jYbOXKVX44kAAAAByJv8rXU2wt9ZoSemiGl7Rv1MeHwgrJRvbYcUfMpjLAz2bh77nWHOppVpZzR2K2uw89vs6aWrPXuiWeIEQQvEM"},"password_manager":{"os_password_blank":true,"os_password_last_changed":"13245952488007586"},"plugins":{"metadata":{"adobe-flash-player":{"disp

C:\Users\user\AppData\Local\Temp\tmpF0E9.tmp	
Process:	C:\Users\user\AppData\Local\Temp\01913ed7-c54a-4682-ba7f-2339dfb12dae.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Roaming\5BBD.tmp.exe	
Process:	C:\Users\user\Pictures\Adobe Films\fyqi7uQSxz8XM3xkvrctriED.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	143872
Entropy (8bit):	6.074860303790983
Encrypted:	false
SSDEEP:	1536:+Rjag85YZeVUa7jLxJ6ErQN/0xttmbgSTuVLXylEYpxYlhwNLSNsWJd09dlt+mGM:+pgUabx5rTTtmcuuVLXq1wMf+mkQ
MD5:	5D88433ACCC7194A4B00EBF5ED3B89E9
SHA1:	D4F1FBB70BF3E1D456CB8F0A0E0E54A6F3B8122B
SHA-256:	A4CB0942DC11A1BB4BA19B67D25EF048A6CBCD08F46BC966D57C4CB5E0ACA42E
SHA-512:	AED23DA0D6F8CFFAB600C1A51F0984444C953A6BADC67E268DB2CA083D0158F2E418AF1407A935363F71FD88F8EDFE70D0D666B726C9FA230A75B923D598D2B
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....M.....L.....{.....{.....{... ....Rich.....PE..d.....a.....".....F.....x.....@.....`.....L.....p.....@.....d.....8..... ...8..... ...`..H.....text...pE.....F..... ..`.rdata.....`.....J.....@..@.data..... .....@....pdata.....@.....@..@_RDATA.....`.....&.... .....@..@.rsrc.....p.....(.....@..@.reloc..d.....*.....@..B..... .....

C:\Users\user\AppData\Roaming\D9C.tmp.exe	
Process:	C:\Users\user\Pictures\Adobe Films\fyqi7uQSxz8XM3xkvrctriED.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	350720

C:\Users\user\AppData\Roaming\D9C.tmp.exe	
Entropy (8bit):	5.837263630193013
Encrypted:	false
SSDEEP:	6144:z0d0y3YN3kF+VkgVDZqWCinN4roRkv6KcEih31c2Kigl3y29:C0I03u2HvNUoyvmhZmC29
MD5:	8C0449C168C009C9DC860902E0F1CA66
SHA1:	5CF505891182ABCAFA951F13095446AF7C76080F
SHA-256:	E77A7FC7620DEF141DD138FE6192B9C34E800EBDC0A34B35D72B3289BACF6544
SHA-512:	B6929C8D093A323FF4505419963D5DB6228AAEE467266D085F903BBA018A8A95742180C4935169172A4FF93AAD46CAABBBA549BC97C09D1FF09971CA38FBEFB
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....2.....Rich..... .....PE..L.....a.....x.....@.....@.....d.....p..p.....@.....<..... .....text...rw.....x..... ..`.rdata..._.....`...|.....@..@.data...dw.....n.....@....reloc..p....p.....J.....@..B..... ....

C:\Users\user\AppData\Roaming\F4E.tmp.exe	
Process:	C:\Users\user\Pictures\Adobe Films\fyqi7uQSxz8XM3xkvrctriED.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	272384
Entropy (8bit):	4.939288121191688
Encrypted:	false
SSDEEP:	3072:TRgSGODomPPSmzU1U3LXkhvrQJcST/aDWrxpzbgqru:T2tmPPS51YohvrZST/guzbgwu
MD5:	C2EC5A75462D14AF2C509F3E61C0CA68
SHA1:	2A97AA969650C7C75E15F960C47EDF54BA36E78A
SHA-256:	DDAA51B7F3C2B6DD0E8BCCB4785B1C6D86A6D7E39FFB6C5A9B6F5F989B9838A3
SHA-512:	4526B6292559F542CE96E21B5E3211797895B0A9CF11DAC0BF5FBCA8AC90C7B0384B3DD6C7DB27AF89B16BFC6B22B7562F92A1F81388B2EF194FD1CD156822AE
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W..O6..O6..O6..QdR.S6..QdD..6..QdC.a6..h..L6..O6...6..QdM.N6..QdS.N6..QdV.N6..RichO6.....PE..L...b,._..... .....00.....0....@.....A.....f..(.....(.....1..... ....Y..@.....0.....text...C..... ....`.rdata...?...0...@...$.....@..@.data....V...p.....d.....@....rsrc...(.....Z.....@..@..... ....

C:\Users\user\Documents\20220114\PowerShell_transcript.301389.VVOMqrLu.20220114153242.txt	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	691
Entropy (8bit):	5.163559264201053
Encrypted:	false
SSDEEP:	12:57DtSA6NW8ibv3fBbBB5ouVux2DOzzn1T/UWoHPw6jewGxMKjX4CIymgSs2uKJXF:BxSAN17vBVL/ux2DOX1YWuHjeTKKjX4L
MD5:	CF2260463527DCFDA0774B4F8EA0461A
SHA1:	0375633752D237AE1A88BC9E45BD08FB8CC42F39
SHA-256:	5F3205FF686CA4CE77312BA060D973EF4C0C0D5F3F7D025CD25FCF66AB56D0B3
SHA-512:	885F63FF5A3287A9B40E95541A282E4F9AE38CBB4B691270198730CB03F7C0C06559A760AFDDD5FE4E580E0B40AC3888427AD18287A6594968CA337FA956BA04
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220114153251..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 301389 (Microsoft Windows NT 10.0.17134.0)..Host Application: PowerShell Get-MpComputerStatus..Process ID: 3832..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220114153251..**********..PS>Get-MpComputerStatus..

C:\Users\user\Documents\3bt5DsNiQBL2dnO8YKYIjDPi.exe	
Process:	C:\Users\user\Pictures\Adobe Films\sCI8qb6amvGp4AhJGUUX5nQx.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	130048
Entropy (8bit):	6.425220045896409
Encrypted:	false
SSDEEP:	3072:Ix3W04qaxUUI4Y+TM4UzqlwGCD+IgQn0uG4PkWZNRgaWrSJSDhixGW2pldwuMmzA:IchAXD+UFkWDiwwixv+0uMmzv34
MD5:	4EDBAE4F41DBFFF3675A867FE06EA0DB
SHA1:	F6E91D1E642B7E9762B0ECC2E36B6FC489DA4A13

C:\Users\user\Documents\3bt5DsNiQBL2dnO8YKYIjDPi.exe	
SHA-256:	0F61C7D939EA77FFF7EB409522338347B140BEB1C5977BD0FC84FF301DD31605
SHA-512:	7C65FB74664C142B3FB9BEE0BEB1F01B36D2EBAE592C864481B2D07C706DA9312F030BADE9721353CA298B985A24BAC8FC1F87A6BB39A10273A4A4E66AC835C8
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B>cG._..._..._...4..._...4..._...4..._...0..._...0..._...0..*_...4..._.. ._..X_...0..._...0..._..._..._...0..._..Rich._.....PE..L...c..a.....L.....@.....@.....@.....4...<.....(..... ..T. ...a.....a..@.....0.....polik..... ..`.data...D.....@....idata.....@..@.rsrc...(.....@. .@.reloc..T.... .....@..B..... .....

C:\Users\user\Documents\Ei8DrAmaYu9K8ghN89CsjOW1.dll	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	data
Category:	dropped
Size (bytes):	1759748
Entropy (8bit):	6.609401987377134
Encrypted:	false
SSDEEP:	24576:RAoCuQN3sS4wWmp/wbJU3MaWtNA/8nk5quGviobr:RAqQN3sS4wWmpsqWtGguGvtP
MD5:	57F492DB3101CA040176C4CEACCC8C5E
SHA1:	4FB9A8FB0F97605FA31086D77E9D096F2C20FFD9
SHA-256:	9BFB00DFDF0BB2AD99D138F721260F2B3FB1BD7CDDEC20EC92291CF57EA63C4B
SHA-512:	A5A8CFF754D2024210C6AEE910661D6FF39210B392AD0C6331BC896E48A69F73E2DA1472BE8B5DADFA6CC3EDB3A6817F7EC05504CCB1B0B3837D7DDC8004F0A
Malicious:	false
Yara Hits:	• Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: C:\Users\user\Documents\Ei8DrAmaYu9K8ghN89CsjOW1.dll, Author: Florian Roth
Reputation:	unknown
Preview:	...]..... .bb..%.....'..).P.%..P.....Q...Q...Q...P...Q...P/..Q...P...Q...Q...Q...P...Q...P...Q...P...Q...P...Q...P...Q...Q:..QV..P..QV.-Q...Q..EQ...QV..P...Q.....Q.....|.....}.....s.....[.....-...j.....-.....>.....9..... >.....].....].....j...-...e.....-..... .....

C:\Users\user\Pictures\Adobe Films\0y_aICQBJv4J1LDnCOe55cop.exe	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	560752
Entropy (8bit):	7.587785097600988
Encrypted:	false
SSDEEP:	12288:b/D0l7bieAtJl4gcl4LxzuB5lK+hJEacXVeN19xPkNj:b/xAZclKxYIINFefPGj
MD5:	3ECFD5D9F991294510E111DCF96357FD
SHA1:	7B208DA6822F3B04E27F0B1DCE0E48B11D3E7DA7
SHA-256:	9F7FDE5DC8DD5812E5F58AAB39268D6FFB15FD7A1CCD77686FA970EF55693F85
SHA-512:	36DD26FB198A46E7B453BF13D781BB4F3F970368869BBCBC0F5D8472BAC22B42ABCD41705EB0A0F3085079C8CF37E18513BB695F3EA7210C8D622C630C5039C
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(3...32.....f.....C'B{b.....+..R...d:.....Q..... ....PE..L.....0.....H..... ...@....@.....@.....@.....`.....p..pG..... ...gfids...P.....`BSS.....`.....@....rsrc...pG...p.....@..@BSS.....y...$.....@..... .....on..D.}[A.y[[C%.x..t.k..i...

C:\Users\user\Pictures\Adobe Films\56IWdY4eqRTdJgfAC3WHYY1z.exe	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	412160
Entropy (8bit):	7.124266199340482
Encrypted:	false
SSDEEP:	6144:flSQc2qhAGg2AV5c+dznE1rA8r6nDDrBC14SrxCbsxg7GMjH5oRWSe:f4Qc2BG0cunERAtBC1Pd8sxSbZoRW
MD5:	D08898F15B9373D16001E84A320628E5
SHA1:	9350EC1E0FCA1C3E78A56025596D4A230832BBBE
SHA-256:	018AE123C7095FA1CF54A2FED5F54A4E953A556BB1B180D80E9D955351A93DB8
SHA-512:	A66929317B32590312BF81CF64EC2F89524159C28AB86E40095EBEA41267E78C61C716BA73183DB82991C5C55D6C4002E845C24DAE92EFFF2BD0D2FE3BECE00
Malicious:	false
Reputation:	unknown

C:\Users\user\Pictures\Adobe Films\56IWdY4eqRTdJgfAC3WHYY1z.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....I..U(...(...(...6.).1...6.?.W....I..+...(.....6.8.....6.(.)...6.-.)...Rich(..... .....PE..L....fe_.....X...v.....6.....p....@.....Q.....S..(....@...{.....X.....@.....8..... .....text...HW.....X..... ..`.data.....p.....\.....@....mepav.....t.....@....butoji..... .....v.....@....xuteru.....0.....x.....@....rsrc.... {...@...|.....@..@.reloc...F.....H.....@..B..... .....

C:\Users\user\Pictures\Adobe Films\5Pl0uv0ZiLthX_vA39iBZgFo.exe	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	1321600
Entropy (8bit):	7.6348046060767425
Encrypted:	false
SSDEEP:	24576:E8f39B+OecSnrJYG4oPSiANTfUrnmXb9mL8VkFq5aXq5Uzr0W:porJYGPyTenmZ64+3zr9
MD5:	BF577170C86E15B04BA705FD3F07151F
SHA1:	2647B6F5968B8521FC3A024E3600554D8746A4D8
SHA-256:	901CA296CF9AAA112CA787FAE18AB87AE5E8DAF1ECB037F0A2BEA44F9125E8DA
SHA-512:	CD04DC5243444953F08BA159800315DE9636C08BEE1814D53E711440799E6EAF277337EE0021C7076AA47084C4203B7196CADEC38FA75C35EE01F20875138EF0
Malicious:	false
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(3...32.....f.....C'B{b.....+..R...d:.....Q..... ....PE..L....j.....0..<..... ...`....@..... .....@.....@..... ..didata..p.....`.pdata.....@....rsrc...@.....@.....@..@.text.....Ax.....@..... .....G..sI.0.gmY.=.'....mL.{.

C:\Users\user\Pictures\Adobe Films\5q_HfaMaCiUp12tkPrR6eSka.exe	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	7652141
Entropy (8bit):	**7.996937403105424**
Encrypted:	**true**
SSDEEP:	196608:91OLi0Xz1oNNxRqT8kMmyur5ums3v2DF2r:3Oe0D2Txw8Hmd5uxvF
MD5:	F7A84C588542DBD6AAB35892B9D88DCD
SHA1:	531ED1D8622968E1979D2561D5F98ADBAEC40B31
SHA-256:	DBF97E84632CCD62E28F0A7CC717A5C5C67D9FF99638D8D12084DC6796761E04
SHA-512:	7C2EED1DA4E18605D8B3B85A71079B2084586F2C0F013283F9CFF3A0B0D94595550C8BE0DA2DB6D6B38A6E56498895842FE14F8E6F78B809C9591FB27073E1D6
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W..s...s...s...}...s...y..s...,...s...r.!.s.....s...x..s.....s.....s.^.u. ..s.Rich..s.....PE..L....S.L.....K.....@.....d....p..`..... .....text..... ..`.rdata...D.....F.....@..@.data...HZ.....2.....@....sxdata.....`.....@....rsrc...`....p.....@..@..... ....

C:\Users\user\Pictures\Adobe Films\8fPwMu8Y3u0_P21OCUSRcOu9.exe	
Process:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	580
Entropy (8bit):	4.807409249660683
Encrypted:	false
SSDEEP:	12:TjeRHdHiHZdtkll5r4NGlTF5TF5TF5TF5TF5TFK:neRH988aTPTPTPTPTPTc
MD5:	9E47D3A502A7B2BCEC1F1375430CA0EB
SHA1:	E3845E5E982AE0580FA31ABF301C803D89ADAB52
SHA-256:	CBF1FDFDB7257DAF8B0905D94BD04E2829C502C9C01B1D96BB979069E2EBC895
SHA-512:	8239210B404E0B19E841D7832D73452617A17C39A29F7CB6E8CCE8F1474B7C17D6ACBA630EFB6510CB3F0315C3147B7BB62C0B0BEECEF8EF29764B8B906E8EF 3
Malicious:	false
Reputation:	unknown
Preview:	<html>..<head><title>404 Not Found</title></head>..<body bgcolor="white">.. 404 Not Found ..<hr> nginx/1.14.0 (Ubuntu) .. </body>..</html>.. a padding to disable MSIE and Chrome friendly error page -->.. a padding to disable MSIE and Chrome friendly error page -->.. a padding to disable MSIE and Chrome friendly error page -->.. a padding to disable MSIE and Chrome friendly error page -->.. a padding to disable MSIE and Chrome friendly error page -->.. a padding to disable MSIE and Chrome friendly error page -->..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.314785279304417
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	kGl1qp3Ox8.exe
File size:	1049088
MD5:	7ebf41b7e0d24473f2ad0b25e354f615
SHA1:	6e9c110ed531f7239ff849a6b7c998d1c958f2d8
SHA256:	15cea3c23e9d0f1ec3a748746bd425d642ae25b042b1b36c8364f721235f0f0d
SHA512:	83dc1c23462f6f647d049214d9dba23874f3a1ba75815476107a0ffba769521d085a0e831132c09e02fe596290d1ec2ba954d26ec4d51cf7ee8636c2c5d2a24d
SSDEEP:	12288:W71ZEyufdBGp4MAuVEVRtyncxQRhJJzhoqgH5sB4dxHGA4:o1ZoGp/4RhQRh9B4dZ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\4.w2g.w2g.w2g..1f.w2g..7fPw2g..6f.w2g..6f.w2g..1f.w2g..7f.w2g..3f.w2g.w3g.w2g..;f.w2g...g.w2g.w.g.w2g..0f.w2gRich.w2g.....

File Icon

Icon Hash:	e0d8b06171f0c0f0

Static PE Info

General

Entrypoint:	0x413fce
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x612F2FD4 [Wed Sep 1 07:46:28 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	93fd4ae8d78e56fe707a53a5a49cf9e3

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x284af	0x28600	False	0.534999032508	data	6.56081725367	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x2a000	0x7854	0x7a00	False	0.445216444672	data	5.05039221406	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x32000	0x15ec	0xc00	False	0.159505208333	data	2.18639249804	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x34000	0xcd768	0xcd800	False	0.34014075806	data	6.07334010967	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x102000	0x18c4	0x1a00	False	0.755558894231	data	6.47158058379	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: kGl1qp3Ox8.exe PID: 6940 Parent PID: 2940

General

Start time:	15:31:17
Start date:	14/01/2022
Path:	C:\Users\user\Desktop\kGl1qp3Ox8.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\kGl1qp3Ox8.exe"
Imagebase:	0x11f0000
File size:	1049088 bytes
MD5 hash:	7EBF41B7E0D24473F2AD0B25E354F615
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Generic_malware, Description: Yara Generic_malware, Source: 00000001.00000003.492052786.0000000005280000.00000004.00000010.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: NNNBSubeVPxRXeeZnGu7gQkK.exe PID: 2468 Parent PID: 6940

General

Start time:	15:32:09
Start date:	14/01/2022
Path:	C:\Users\user\Pictures\Adobe Films\NNNBSubeVPxRXeeZnGu7gQkK.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Pictures\Adobe Films\NNNBSubeVPxRXeeZnGu7gQkK.exe"
Imagebase:	0x7ff62bf00000
File size:	326144 bytes
MD5 hash:	3F22BD82EE1B38F439E6354C60126D6D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

Analysis Process: kXM34tDnyQtIWwfvEKDMhvoQ.exe PID: 5892 Parent PID: 6940

General

Start time:	15:32:25
Start date:	14/01/2022
Path:	C:\Users\user\Pictures\Adobe Films\kXM34tDnyQtIWwfvEKDMhvoQ.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Pictures\Adobe Films\kXM34tDnyQtIWwfvEKDMhvoQ.exe"
Imagebase:	0x8d0000
File size:	166912 bytes
MD5 hash:	0C70224F09C65619BC9D6AFC456294C9
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Registry Activities Show Windows behavior

Analysis Process: DFhRro1WrdTF3ZDuGSOCgEWZ.exe PID: 5124 Parent PID: 6940

General

Start time:	15:32:25
Start date:	14/01/2022
Path:	C:\Users\user\Pictures\Adobe Films\DFhRro1WrdTF3ZDuGSOCgEWZ.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Pictures\Adobe Films\DFhRro1WrdTF3ZDuGSOCgEWZ.exe"
Imagebase:	0x400000
File size:	433152 bytes
MD5 hash:	DDFE3C0D174EC565750DCACEF9A52363
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000007.00000003.509157725.0000000000621000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: eULKoZpb_80D8HrRwSiJF82y.exe PID: 5184 Parent PID: 6940

General

Start time:	15:32:25
Start date:	14/01/2022
Path:	C:\Users\user\Pictures\Adobe Films\eULKoZpb_80D8HrRwSiJF82y.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Pictures\Adobe Films\eULKoZpb_80D8HrRwSiJF82y.exe"
Imagebase:	0xdb0000
File size:	166912 bytes
MD5 hash:	A9DED7D6470F741B9F4509863665F74C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Registry Activities — Show Windows behavior

Analysis Process: gw2BglocGXw_yTn_uJ3zXLrN.exe PID: 5480 Parent PID: 6940

General

Start time:	15:32:25
Start date:	14/01/2022
Path:	C:\Users\user\Pictures\Adobe Films\gw2BglocGXw_yTn_uJ3zXLrN.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Pictures\Adobe Films\gw2BglocGXw_yTn_uJ3zXLrN.exe"
Imagebase:	0x400000
File size:	373248 bytes
MD5 hash:	0162C08D87055722BC49265BD5468D16
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_onlyLogger, Description: Yara detected onlyLogger, Source: 00000009.00000003.518327651.00000000020E0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities — Show Windows behavior

Registry Activities — Show Windows behavior

Key Created

Key Value Created

Analysis Process: VxkVtHpwGFsrs3Al2PFI1pOG.exe PID: 5524 Parent PID: 6940

General

Start time:	15:32:25
Start date:	14/01/2022
Path:	C:\Users\user\Pictures\Adobe Films\VxkVtHpwGFsrs3Al2PFI1pOG.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Pictures\Adobe Films\VxkVtHpwGFsrs3Al2PFI1pOG.exe"
Imagebase:	0x400000
File size:	320512 bytes
MD5 hash:	61931A7DE1769BC844394F161F1DE150
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000A.00000003.516403023.00000000009D0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: XzPWSUxlao64h10K0Z7pfPtI.exe PID: 4760 Parent PID: 6940

General

Start time:	15:32:25
Start date:	14/01/2022
Path:	C:\Users\user\Pictures\Adobe Films\XzPWSUxlao64h10K0Z7pfPtI.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Pictures\Adobe Films\XzPWSUxlao64h10K0Z7pfPtI.exe"
Imagebase:	0x6d0000
File size:	984576 bytes
MD5 hash:	6D87BD5B6C8585B0FECB45BAD7F3D92B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: P65Nqt8GfRApLpFwJ9bOb7YH.exe PID: 4928 Parent PID: 6940

General

Start time:	15:32:33
Start date:	14/01/2022
Path:	C:\Users\user\Pictures\Adobe Films\P65Nqt8GfRApLpFwJ9bOb7YH.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Pictures\Adobe Films\P65Nqt8GfRApLpFwJ9bOb7YH.exe"
Imagebase:	0x400000
File size:	636743 bytes
MD5 hash:	3A9664DAD384F41DCDC1272ED31171E0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: fyqi7uQSxz8XM3xkvrctriED.exe PID: 6000 Parent PID: 6940

General

Start time:	15:32:34
Start date:	14/01/2022
Path:	C:\Users\user\Pictures\Adobe Films\fyqi7uQSxz8XM3xkvrctriED.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Pictures\Adobe Films\fyqi7uQSxz8XM3xkvrctriED.exe"
Imagebase:	0xe80000
File size:	127488 bytes
MD5 hash:	7A14B5FC36A23C9FF0BAF718FAB093CB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: e5SEitbuPomqfmRpQ1nXQBM2.exe PID: 5968 Parent PID: 6940

General

Start time:	15:32:34
Start date:	14/01/2022
Path:	C:\Users\user\Pictures\Adobe Films\e5SEitbuPomqfmRpQ1nXQBM2.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Pictures\Adobe Films\e5SEitbuPomqfmRpQ1nXQBM2.exe"

Imagebase:	0xb30000
File size:	560752 bytes
MD5 hash:	3ECFD5D9F991294510E111DCF96357FD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: _Phvk0uQfXOn269qFdHTiuOG.exe PID: 6596 Parent PID: 6940

General

Start time:	15:32:34
Start date:	14/01/2022
Path:	C:\Users\user\Pictures\Adobe Films_Phvk0uQfXOn269qFdHTiuOG.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Pictures\Adobe Films_Phvk0uQfXOn269qFdHTiuOG.exe"
Imagebase:	0x810000
File size:	1685504 bytes
MD5 hash:	DECA67F083AE99A6BB5E9F8E8F31550C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: JiryxVDn0P_ka7w2xP8PdulD.exe PID: 6640 Parent PID: 6940

General

Start time:	15:32:34
Start date:	14/01/2022
Path:	C:\Users\user\Pictures\Adobe Films\JiryxVDn0P_ka7w2xP8PdulD.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Pictures\Adobe Films\JiryxVDn0P_ka7w2xP8PdulD.exe"
Imagebase:	0x400000
File size:	766464 bytes
MD5 hash:	5348327DE92D40720D25952A88613986
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000010.00000003.537769681.0000000000860000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000010.00000003.537769681.0000000000860000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: Ne0JuwDw1Qp0B7KETuyFd5jI.exe PID: 5192 Parent PID: 6940

General

Start time:	15:32:34
Start date:	14/01/2022
Path:	C:\Users\user\Pictures\Adobe Films\Ne0JuwDw1Qp0B7KETuyFd5jI.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Pictures\Adobe Films\Ne0JuwDw1Qp0B7KETuyFd5jI.exe"
Imagebase:	0x160000
File size:	2059890 bytes

MD5 hash:	3A6EBD3377AFDB9EFC2195E7B6A00A69
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 56IWdY4eqRTdJgfAC3WHYY1z.exe PID: 5860 Parent PID: 6940

General

Start time:	15:32:34
Start date:	14/01/2022
Path:	C:\Users\user\Pictures\Adobe Films\56IWdY4eqRTdJgfAC3WHYY1z.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Pictures\Adobe Films\56IWdY4eqRTdJgfAC3WHYY1z.exe"
Imagebase:	0x400000
File size:	412160 bytes
MD5 hash:	D08898F15B9373D16001E84A320628E5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 00000012.00000000.573252466.0000000000670000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_onlyLogger, Description: Yara detected onlyLogger, Source: 00000012.00000000.573252466.0000000000670000.00000040.00000001.sdmp, Author: Joe Security • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 00000012.00000000.565856471.0000000000781000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 00000012.00000000.571146850.0000000000400000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_onlyLogger, Description: Yara detected onlyLogger, Source: 00000012.00000000.571146850.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 00000012.00000000.563078389.0000000000670000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_onlyLogger, Description: Yara detected onlyLogger, Source: 00000012.00000000.563078389.0000000000670000.00000040.00000001.sdmp, Author: Joe Security • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 00000012.00000000.574219405.0000000000781000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 00000012.00000000.560601681.0000000000400000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_onlyLogger, Description: Yara detected onlyLogger, Source: 00000012.00000000.560601681.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 00000012.00000003.541639341.00000000006C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_onlyLogger, Description: Yara detected onlyLogger, Source: 00000012.00000003.541639341.00000000006C0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: sCI8qb6amvGp4AhJGUUX5nQx.exe PID: 6096 Parent PID: 6940

General

Start time:	15:32:34
Start date:	14/01/2022

Path:	C:\Users\user\Pictures\Adobe Films\sCI8qb6amvGp4AhJGUUX5nQx.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Pictures\Adobe Films\sCI8qb6amvGp4AhJGUUX5nQx.exe"
Imagebase:	0xda0000
File size:	394752 bytes
MD5 hash:	503A913A1C1F9EE1FD30251823BEAF13
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: dce6bd67-7e1f-466b-94f1-f9f5c2acf9dd.exe PID: 4148 Parent PID: 5892

General

Start time:	15:32:38
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\dce6bd67-7e1f-466b-94f1-f9f5c2acf9dd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\dce6bd67-7e1f-466b-94f1-f9f5c2acf9dd.exe"
Imagebase:	0xd40000
File size:	338944 bytes
MD5 hash:	748DBD76B3D32F174DEBD3BD296A2C4D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: svchost.exe PID: 1040 Parent PID: 560

General

Start time:	15:32:38
Start date:	14/01/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6b7590000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: P65Nqt8GfRApLpFwJ9bOb7YH.tmp PID: 580 Parent PID: 4928

General

Start time:	15:32:39
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\is-FNG8T.tmp\P65Nqt8GfRApLpFwJ9bOb7YH.tmp
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\is-FNG8T.tmp\P65Nqt8GfRApLpFwJ9bOb7YH.tmp" /SL5="$C03EA,312591,228864,C:\Users\user\Pictures\Adobe Films\P65Nqt8GfRApLpFwJ9bOb7YH.exe"
Imagebase:	0x400000

File size:	883200 bytes
MD5 hash:	7FC94D54F886839996FB02FBBE1B42C8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: powershell.exe PID: 3832 Parent PID: 6596

General

Start time:	15:32:39
Start date:	14/01/2022
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	PowerShell Get-MpComputerStatus
Imagebase:	0x7ff743d60000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: 4868 Parent PID: 3832

General

Start time:	15:32:40
Start date:	14/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 3440 Parent PID: 5524

General

Start time:	15:32:42
Start date:	14/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: 4c91d8e5-f330-473d-bea7-49691b483a08.exe PID: 6828 Parent PID: 5892

General

Start time:	15:32:42
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\4c91d8e5-f330-473d-bea7-49691b483a08.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\4c91d8e5-f330-473d-bea7-49691b483a08.exe"
Imagebase:	0x400000
File size:	586608 bytes
MD5 hash:	309F89D4E7F28E93B0CB02D7A5806F6C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: 01913ed7-c54a-4682-ba7f-2339dfb12dae.exe PID: 644 Parent PID: 5184

General

Start time:	15:32:45
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\01913ed7-c54a-4682-ba7f-2339dfb12dae.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\01913ed7-c54a-4682-ba7f-2339dfb12dae.exe"
Imagebase:	0xb80000
File size:	340480 bytes
MD5 hash:	9734ED168A74A29DC30C2273FE7AEDDC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: SiJXWwfMYK4L8VTC7HncQkab.exe PID: 3640 Parent PID: 6940

General

Start time:	15:32:45
Start date:	14/01/2022
Path:	C:\Users\user\Pictures\Adobe Films\SiJXWwfMYK4L8VTC7HncQkab.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Pictures\Adobe Films\SiJXWwfMYK4L8VTC7HncQkab.exe"
Imagebase:	0x7ff65a320000
File size:	2139648 bytes
MD5 hash:	DD3C57E2520A47D634E5FAAC52782FDA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Generic_malware, Description: Yara Generic_malware, Source: 0000001D.00000000.569672179.00007FF65A410000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Generic_malware, Description: Yara Generic_malware, Source: 0000001D.00000000.547428729.00007FF65A410000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001D.00000000.547517237.00007FF65A450000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001D.00000000.569965966.00007FF65A450000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Generic_malware, Description: Yara Generic_malware, Source: 0000001D.00000000.563735555.00007FF65A410000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001D.00000000.564589303.00007FF65A450000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Generic_malware, Description: Yara Generic_malware, Source: C:\Users\user\Pictures\Adobe Films\SiJXWwfMYK4L8VTC7HncQkab.exe, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: C:\Users\user\Pictures\Adobe Films\SiJXWwfMYK4L8VTC7HncQkab.exe, Author: Joe Security

Analysis Process: 0y_alCQBJv4J1LDnCOe55cop.exe PID: 5100 Parent PID: 6940

General

Start time:	15:32:45
Start date:	14/01/2022
Path:	C:\Users\user\Pictures\Adobe Films\0y_alCQBJv4J1LDnCOe55cop.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Pictures\Adobe Films\0y_alCQBJv4J1LDnCOe55cop.exe"
Imagebase:	0x140000
File size:	560752 bytes
MD5 hash:	3ECFD5D9F991294510E111DCF96357FD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: C1aYSYmMy9tQLrifaCN41EQ8.exe PID: 3556 Parent PID: 6940

General

Start time:	15:32:45
Start date:	14/01/2022
Path:	C:\Users\user\Pictures\Adobe Films\C1aYSYmMy9tQLrifaCN41EQ8.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Pictures\Adobe Films\C1aYSYmMy9tQLrifaCN41EQ8.exe"
Imagebase:	0xcd0000
File size:	1314720 bytes
MD5 hash:	2DBF77866712D9EBD57EC65E7C1598A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: NhzjvwxrwXd3QBEl8Ly0lN5e.exe PID: 1316 Parent PID: 6940

General

Start time:	15:32:45

Start date:	14/01/2022
Path:	C:\Users\user\Pictures\Adobe Films\NhzjvwxrwXd3QBEl8Ly0lN5e.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Pictures\Adobe Films\NhzjvwxrwXd3QBEl8Ly0lN5e.exe"
Imagebase:	0x400000
File size:	781824 bytes
MD5 hash:	67848A34646ADF30BCC92518C0AE1BD1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: nnaUz9XFoo0RBkjZ4wuMqrTl.exe PID: 6632 Parent PID: 6940

General

Start time:	15:32:50
Start date:	14/01/2022
Path:	C:\Users\user\Pictures\Adobe Films\nnaUz9XFoo0RBkjZ4wuMqrTl.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Pictures\Adobe Films\nnaUz9XFoo0RBkjZ4wuMqrTl.exe"
Imagebase:	0x400000
File size:	1846416 bytes
MD5 hash:	FAB86F0D2562E6CD30D8CBC915A05ECC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: _____djskjT76(((.exe PID: 4460 Parent PID: 580

General

Start time:	15:32:50
Start date:	14/01/2022
Path:	C:\Users\user\AppData\Local\Temp\is-MBHBG.tmp_____djskjT76(((.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\is-MBHBG.tmp_____djskjT76(((.exe" /S /UID=2710
Imagebase:	0x560000
File size:	867840 bytes
MD5 hash:	16B30C7902FC1B0A34744C95A64E332B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Disassembly

Code Analysis