ID: 534003
Sample Name: 912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe
Cookbook: default.jbs
Time: 23:27:07
Date: 04/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

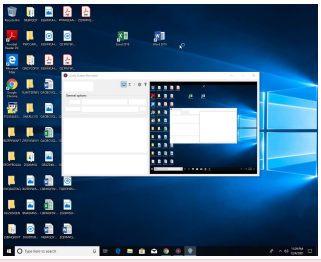
Windows Analysis Report 912534A5380738D96E8DDB7…

Overview

General Information

Sample Name:	912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe
Analysis ID:	534003
MD5:	8b7b82eb83d4a6..
SHA1:	e827272cd42a90..
SHA256:	912534a5380738..
Tags:	exe GCleaner
Infos:	

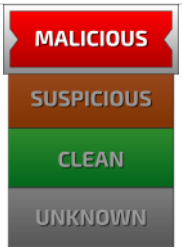
Most interesting Screenshot:



Errors

- Sigma runtime error: Invalid condition: all of selection* Rule: Conti Backup Database
- Sigma runtime error: Invalid condition: all of selection* Rule: Stop Or Remove Antivirus Service
- Sigma runtime error: Invalid condition: all of selection* Rule: Conti Volume Shadow Listing
- Sigma runtime error: Invalid condition: all of selection* Rule: Compress Data and Lock With Password for Exfiltration With 7-ZIP
- Sigma runtime error: Invalid condition: all of selection* Rule: Disable or Delete Windows Eventlog
- Sigma runtime error: Invalid condition: all of selection* Rule: PowerShell Script Copy
- Sigma runtime error: Invalid condition: all of selection* Rule: Compress Data and Lock With Password for Exfiltration With WINZIP

Detection



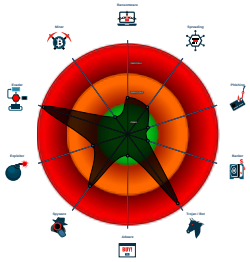
RedLine Socelars Vidar

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

Signatures

- Yara detected RedLine Stealer
- Yara Genericmalware
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for subm…
- Yara detected Vidar stealer
- Yara detected Socelars
- Multi AV Scanner detection for dropp…
- Disable Windows Defender real time…
- Maps a DLL or memory area into an…
- Sigma detected: Suspicious Script E…
- PE file has a writeable .text section
- Tries to detect sandboxes and other…
- Yara detected Costura Assembly Lo…
- Injects a PE file into a foreign proce…
- .NET source code contains very larg…
- Adds a directory exclusion to Windo…
- Checks if the current machine is a v…
- Tries to harvest and steal browser in…
- PE file contains section with special…
- Creates HTML files with .exe extens…
- Checks for kernel code integrity (NtQ…
- Sigma detected: Powershell Defende…
- Obfuscated command line found

Classification



Process Tree

- **System is w10x64**
- 912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe (PID: 5000 cmdline: "C:\Users\user\Desktop\912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe" MD5: 8B7B82EB83D4A6760ECF8E9398FFDA64)
  - setup_install.exe (PID: 5528 cmdline: "C:\Users\user\AppData\Local\Temp\7zS883210E8\setup_install.exe" MD5: 74EFCE83CAF33BD4AA9A18A87B48B584)
    - conhost.exe (PID: 3744 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - cmd.exe (PID: 1952 cmdline: C:\Windows\system32\cmd.exe /c powershell -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Local\Temp" MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - powershell.exe (PID: 6004 cmdline: powershell -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Local\Temp" MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - cmd.exe (PID: 1500 cmdline: C:\Windows\system32\cmd.exe /c Mon06885bbdb13fec3.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - Mon06885bbdb13fec3.exe (PID: 924 cmdline: Mon06885bbdb13fec3.exe MD5: AE0BB0EF615F4606FBE1F050B6F08CA3)
    - cmd.exe (PID: 4008 cmdline: C:\Windows\system32\cmd.exe /c Mon06dc62fb7183b9e.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - Mon06dc62fb7183b9e.exe (PID: 6188 cmdline: Mon06dc62fb7183b9e.exe MD5: F7AD507592D13A7A2243D264906DE671)
    - cmd.exe (PID: 6156 cmdline: C:\Windows\system32\cmd.exe /c Mon06f9c53ffae25af61.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - Mon06f9c53ffae25af61.exe (PID: 6240 cmdline: Mon06f9c53ffae25af61.exe MD5: FC6FCC4C6F1AA7674E7EFB71AE759A42)
        - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - cmd.exe (PID: 6220 cmdline: C:\Windows\system32\cmd.exe /c Mon06d47d8fde50.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - Mon06d47d8fde50.exe (PID: 6264 cmdline: Mon06d47d8fde50.exe MD5: BB4D9EA74D539111AF6B40D6ED4452F8)
        - Mon06d47d8fde50.exe (PID: 7100 cmdline: C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06d47d8fde50.exe MD5: BB4D9EA74D539111AF6B40D6ED4452F8)
    - cmd.exe (PID: 6256 cmdline: C:\Windows\system32\cmd.exe /c Mon0630c6f1115ad5.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - Mon0630c6f1115ad5.exe (PID: 6328 cmdline: Mon0630c6f1115ad5.exe MD5: 8A40BAC445ECB19F7CB8995B5AE9390B)
        - v2lMWzt44zb0lQ28NgmZJByf.exe (PID: 4396 cmdline: "C:\Users\user\Pictures\Adobe Films\v2lMWzt44zb0lQ28NgmZJByf.exe" MD5: 3F22BD82EE1B38F439E6354C60126D6D)
    - cmd.exe (PID: 6304 cmdline: C:\Windows\system32\cmd.exe /c Mon06cebe79e9a244.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - Mon06cebe79e9a244.exe (PID: 6360 cmdline: Mon06cebe79e9a244.exe MD5: 9535F08BD5920F84AC344F8884FE155D)
    - cmd.exe (PID: 6340 cmdline: C:\Windows\system32\cmd.exe /c Mon067df200a8fd43b.exe /mixone MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - Mon067df200a8fd43b.exe (PID: 6380 cmdline: Mon067df200a8fd43b.exe /mixone MD5: AD56ABB0034DE1257634EA56BE9C8CB6)
        - WerFault.exe (PID: 5836 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6380 -s 852 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - cmd.exe (PID: 6368 cmdline: C:\Windows\system32\cmd.exe /c Mon066b4a7578e0123e.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - Mon066b4a7578e0123e.exe (PID: 6472 cmdline: Mon066b4a7578e0123e.exe MD5: E268A668B507C25263CB0B8BB3AEB3BE)
        - WerFault.exe (PID: 6760 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6472 -s 1120 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - cmd.exe (PID: 6452 cmdline: C:\Windows\system32\cmd.exe /c Mon060579dda3b.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - Mon060579dda3b.exe (PID: 6484 cmdline: Mon060579dda3b.exe MD5: D06CD28108181A12FB2167831713A2A2)
        - WerFault.exe (PID: 1980 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6484 -s 2084 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
        - WerFault.exe (PID: 5808 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6484 -s 2084 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - cmd.exe (PID: 6464 cmdline: C:\Windows\system32\cmd.exe /c Mon0699e256d5dc14.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - Mon0699e256d5dc14.exe (PID: 6500 cmdline: Mon0699e256d5dc14.exe MD5: 535AE8DBAA2AB3A37B9AA8B59282A5C0)
    - cmd.exe (PID: 6492 cmdline: C:\Windows\system32\cmd.exe /c Mon06be060a7cb426cf.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - Mon06be060a7cb426cf.exe (PID: 6600 cmdline: Mon06be060a7cb426cf.exe MD5: 9B7319450F0633337955342AE97FA060)
    - cmd.exe (PID: 6524 cmdline: C:\Windows\system32\cmd.exe /c Mon067f2fcee827.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - Mon067f2fcee827.exe (PID: 6624 cmdline: Mon067f2fcee827.exe MD5: 29158D5C6096B12A039400F7AE1EAF0E)
        - Mon067f2fcee827.tmp (PID: 6908 cmdline: "C:\Users\user\AppData\Local\Temp\is-1U6PN.tmp\Mon067f2fcee827.tmp" /SL5="$60038,247014,163328,C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon067f2fcee827.exe" MD5: 206BACA178D6BA6FBAFF62DAD0FBCC75)
    - cmd.exe (PID: 6584 cmdline: C:\Windows\system32\cmd.exe /c Mon06434adde6c2.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - Mon06434adde6c2.exe (PID: 6684 cmdline: Mon06434adde6c2.exe MD5: 1AECD083BBEC326D90698A79F73749D7)
    - WerFault.exe (PID: 6700 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5528 -s 1028 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
    - WerFault.exe (PID: 5920 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5528 -s 1028 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\PL_Client[1].bmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x100aec:$xo1: \xD0\x9D\xF2\x9D\xE7\x9D\xF4\x9D\xF1\x9D\xF1\x9D\xFC\x9D\xB2\x9D\xA8\x9D\xB3\x9D\xAD\x9D • 0x10291c:$xo1: \xD0\xF2\xE7\xF4\xF1\xF1\xFC\xB2\xA8\xB3\xAD
C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06dc62fb7183b9e.exe	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06be060a7cb426cf.exe	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	• 0x30bd:$x1: https://cdn.discordapp.com/attachments/
C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06885bbdb13fec3.exe	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x12ad:$x1: https://cdn.discordapp.com/attachments/
C:\Users\user\Documents\Ei8DrAmaYu9K8ghN89CsjOW1.dll	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x100aec:$xo1: \xD0\x9D\xF2\x9D\xE7\x9D\xF4\x9D\xF1\x9D\xF1\x9D\xFC\x9D\xB2\x9D\xA8\x9D\xB3\x9D\xAD\x9D • 0x10291c:$xo1: \xD0\xF2\xE7\xF4\xF1\xF1\xFC\xB2\xA8\xB3\xAD
Click to see the 8 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000020.00000000.311875939.00007FF7B9D96000.00000002.00020000.sdmp	JoeSecurity_Generic_malware	Yara Generic_malware	Joe Security	
0000002D.00000000.342760171.000000000402000.00000040.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0000001E.00000000.331948601.000000000118E000.00000002.00020000.sdmp	JoeSecurity_Socelars	Yara detected Socelars	Joe Security	
0000001A.00000000.324919353.00000000007DD000.00000040.00000001.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x2449e:$xo1: cATGBBO\x01\x1B\x1E
00000014.00000002.356338732.000000000381000.00000004.00000001.sdmp	SUSP_Double_Base64_Encoded_Executable	Detects an executable that has been encoded with base64 twice	Florian Roth	• 0xd8f60:$: VFZxUUFBT
Click to see the 35 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
22.3.Mon0630c6f1115ad5.exe.3ad1438.86.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	• 0xd58:$x1: https://cdn.discordapp.com/attachments/ • 0x1238:$x1: https://cdn.discordapp.com/attachments/ • 0x1bf8:$x1: https://cdn.discordapp.com/attachments/ • 0x1cc8:$x1: https://cdn.discordapp.com/attachments/ • 0x1d98:$x1: https://cdn.discordapp.com/attachments/
22.3.Mon0630c6f1115ad5.exe.3ad1438.79.raw.unpack	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0xd58:$x1: https://cdn.discordapp.com/attachments/ • 0x1238:$x1: https://cdn.discordapp.com/attachments/ • 0x1bf8:$x1: https://cdn.discordapp.com/attachments/ • 0x1cc8:$x1: https://cdn.discordapp.com/attachments/ • 0x1d98:$x1: https://cdn.discordapp.com/attachments/
22.3.Mon0630c6f1115ad5.exe.3900630.3.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	• 0xf538:$x1: https://cdn.discordapp.com/attachments/ • 0x17990:$x1: https://cdn.discordapp.com/attachments/ • 0x1a840:$x1: https://cdn.discordapp.com/attachments/
0.3.912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe.354fb72.8.unpack	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x12b9:$x1: https://cdn.discordapp.com/attachments/
26.2.Mon067df200a8fd43b.exe.550e50.1.unpack	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x3d3a0:$xo1: cATGBBO\x01\x1B\x1E
Click to see the 41 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Script Execution From Temp Folder

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

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

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Networking:

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

E-Banking Fraud:

Yara Genericmalware

System Summary:

PE file has a writeable .text section

.NET source code contains very large array initializations

PE file contains section with special chars

PE file has nameless sections

Data Obfuscation:

Yara detected Costura Assembly Loader

Obfuscated command line found

Malware Analysis System Evasion:

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:

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

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 Vidar stealer

Yara detected Socelars

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

Remote Access Functionality:

Yara detected RedLine Stealer

Yara Genericmalware

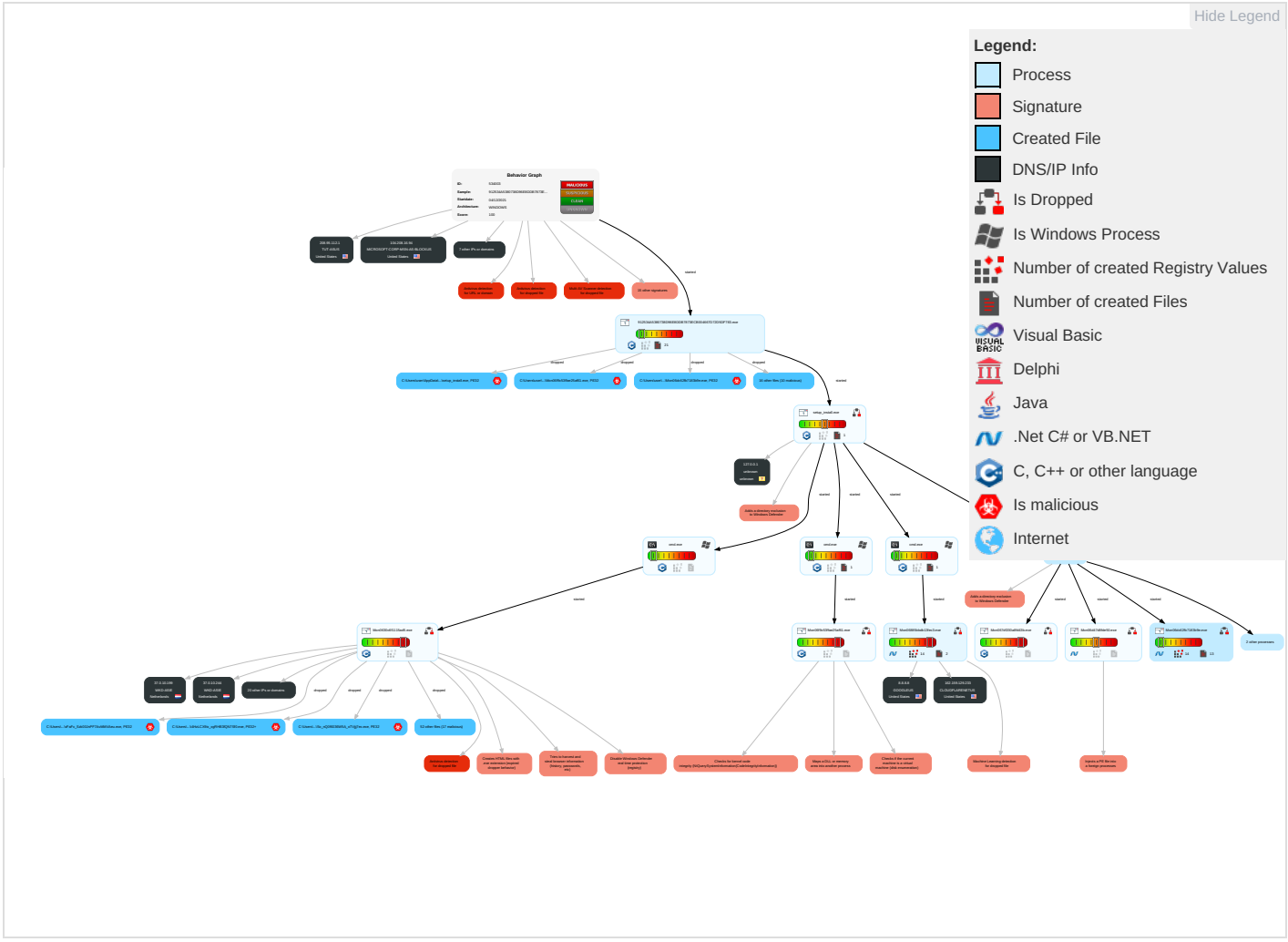
Yara detected Vidar stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Valid Accounts	Native API 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 2 1 1	OS Credential Dumping 1	System Time Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress To Transfer 2
Default Accounts	Command and Scripting Interpreter 1 3	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypted Channel 2
Domain Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Bypass User Access Control 1	Obfuscated Files or Information 4	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration	Steganogr
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 2 1 2	Software Packing 4	NTDS	System Information Discovery 3 6	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersona
Cloud Accounts	Cron	Network Logon Script	Scheduled Task/Job 1	Timestomp 1	LSA Secrets	Security Software Discovery 4 4 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	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Bypass User Access Control 1	DCSync	Virtualization/Sandbox Evasion 1 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 1 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Prot

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 1 3 1	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protc
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 2 1 2	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Trans Protocols

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
912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe	62%	Virustotal		Browse
912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe	75%	ReversingLabs	Win32.Spyware.Socelars	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon067f2fcee827.exe	100%	Avira	HEUR/AGEN.1142105	
C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon067df200a8fd43b.exe	100%	Avira	TR/AD.Chapak.njyhm	
C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06434adde6c2.exe	100%	Avira	TR/Kryptik.jpozl	
C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon066b4a7578e0123e.exe	100%	Avira	TR/Crypt.Agent.wfnia	
C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0699e256d5dc14.exe	100%	Avira	TR/Agent.sdnqs	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Uponrun[1].exe	100%	Avira	HEUR/AGEN.1144479	
C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06be060a7cb426cf.exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon060579dda3b.exe	100%	Avira	HEUR/AGEN.1124060	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\NiceProcessX64[1].bmp	100%	Avira	TR/Agent.dttsn	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\BF1[1].exe	100%	Avira	HEUR/AGEN.1142105	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06885bbdb13fec3.exe	100%	Avira	TR/ATRAPS.Gen	
C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe	100%	Avira	TR/Crypt.XPACK.zbssu	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\install4[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\file1[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon067df200a8fd43b.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Udp[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\xxxx[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon066b4a7578e0123e.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\toolspab2[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\comprehensive1[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Uponrun[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06be060a7cb426cf.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\NiceProcessX64[1].bmp	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Service[1].bmp	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\file3[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06885bbdb13fec3.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\amz[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Setup12[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\ferrari[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\NiceProcessX64[1].bmp	14%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\NiceProcessX64[1].bmp	86%	ReversingLabs	Win64.Packed.Generic	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Uponrun[1].exe	41%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Uponrun[1].exe	89%	ReversingLabs	ByteCode-MSIL.Backdoor.Mokes	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Setup12[1].exe	12%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Setup12[1].exe	59%	ReversingLabs	Win32.Trojan.Fabookie	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\AordVPNWZ3202111221117[1].exe	6%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\AordVPNWZ3202111221117[1].exe	4%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Service[1].bmp	49%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Service[1].bmp	89%	ReversingLabs	Win32.Infostealer.Disbuk	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\askinstall42[1].exe	65%	ReversingLabs	Win32.Adware.ExtInstaller	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\askinstall59[1].exe	47%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\askinstall59[1].exe	96%	ReversingLabs	Win32.Adware.ExtInstaller	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
20.0.Mon06d47d8fde50.exe.3d0000.0.unpack	100%	Avira	HEUR/AGEN.1144480		Download File
22.3.Mon0630c6f1115ad5.exe.8d68420.21.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.3.Mon0630c6f1115ad5.exe.8b08a60.13.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.3.Mon0630c6f1115ad5.exe.8ceee40.82.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.3.Mon0630c6f1115ad5.exe.3a4ade0.25.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.3.Mon0630c6f1115ad5.exe.8d68420.37.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.3.Mon0630c6f1115ad5.exe.8b47e60.28.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.3.Mon0630c6f1115ad5.exe.3a7d280.83.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.3.Mon0630c6f1115ad5.exe.8c6af40.24.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.3.Mon0630c6f1115ad5.exe.8eb3e20.45.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.3.Mon0630c6f1115ad5.exe.3a7d280.59.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.3.Mon0630c6f1115ad5.exe.8ceee40.84.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.3.Mon0630c6f1115ad5.exe.8c5e6a0.7.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.0.Mon06885bbdb13fec3.exe.550000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
22.3.Mon0630c6f1115ad5.exe.8ceee40.68.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.3.Mon0630c6f1115ad5.exe.3ac91c0.19.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.2.Mon06d47d8fde50.exe.3d0000.0.unpack	100%	Avira	HEUR/AGEN.1144480		Download File
22.3.Mon0630c6f1115ad5.exe.8c54f30.63.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.3.Mon0630c6f1115ad5.exe.8c79f60.39.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.3.Mon0630c6f1115ad5.exe.3a7d280.76.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.3.Mon0630c6f1115ad5.exe.8ceee40.67.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.3.Mon0630c6f1115ad5.exe.3a7d280.50.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.3.Mon0630c6f1115ad5.exe.8b47e60.38.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.3.Mon0630c6f1115ad5.exe.34fb610.29.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.3.Mon0630c6f1115ad5.exe.8c5e6a0.9.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
18.0.Mon06f9c53ffae25af61.exe.400000.0.unpack	100%	Avira	TR/Crypt.Agent.dzwmm		Download File

Source	Detection	Scanner	Label	Link	Download
22.3.Mon0630c6f1115ad5.exe.8bdfd00.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
26.2.Mon067df200a8fd43b.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1142240		Download File
14.2.Mon06885bbdb13fec3.exe.550000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
26.0.Mon067df200a8fd43b.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1142240		Download File
22.3.Mon0630c6f1115ad5.exe.8eb3e20.43.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.3.Mon0630c6f1115ad5.exe.8eb3e20.15.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
18.3.Mon06f9c53ffae25af61.exe.560000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.3.Mon0630c6f1115ad5.exe.34fae70.30.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.3.Mon0630c6f1115ad5.exe.8c6af40.40.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.3.Mon0630c6f1115ad5.exe.8c79f60.47.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
22.3.Mon0630c6f1115ad5.exe.8c12760.6.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
26.0.Mon067df200a8fd43b.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1142240		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://software-services.bar	0%	Avira URL Cloud	safe	
http://194.145.227.161/45.227.161/dlc/sharing.php?pub=mixone	0%	Avira URL Cloud	safe	
http://194.145.227.161/dlc/sharing.php?pub=mixonene	0%	Avira URL Cloud	safe	
http://212.193.30.29/WW/file1.exeC:	0%	Avira URL Cloud	safe	
http://212.193.30.29/WW/file3.exe8	0%	Avira URL Cloud	safe	
http://212.193.30.29/WW/file5.exe	0%	Avira URL Cloud	safe	
http://tg8.cllgxx.com/sr21/rtst1047.exe1	0%	Avira URL Cloud	safe	
http://ngdatas.pw/https://www.listincode.com/0.0.0.0%d.%d.%d.%dhttp-1ZIP	0%	URL Reputation	safe	
http://https://software-services.bar/	0%	Avira URL Cloud	safe	
http://https://www.listincode.com/	0%	URL Reputation	safe	
http://https://software-services.bar8	0%	Avira URL Cloud	safe	
http://www.bqmqx.com/askinstall59.exeh	0%	Avira URL Cloud	safe	
http://tg8.cllgxx.com/sr21/rtst1047.exeC:	0%	Avira URL Cloud	safe	
http://amzrouting.com/amz.exe/$	100%	Avira URL Cloud	malware	
http://https://api.ip.sb/geoip%USERPEnvironmentROFILE%	0%	URL Reputation	safe	
http://piratenhits.fm/luna1.exew	0%	Avira URL Cloud	safe	
http://hsiens.xyz/	100%	URL Reputation	malware	
http://hsiens.xyz/addInstallImpression.php?key=125478824515ADNxu2ccbwe&ip=&oid=149	0%	Avira URL Cloud	safe	
http://193.56.146.76/Udp.exev%	0%	Avira URL Cloud	safe	
http://tg8.cllgxx.com/sr21/siww1047.exe	0%	Avira URL Cloud	safe	
http://212.193.30.29/WW/file3.exem	0%	Avira URL Cloud	safe	
http://2.56.59.42/base/api/getData.php	0%	Avira URL Cloud	safe	
http://https://curl.se/V	0%	URL Reputation	safe	
http://194.145.227.161/dlc/sharing.php?pub=mixone	100%	Avira URL Cloud	malware	
http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c0#	0%	URL Reputation	safe	
http://212.193.30.29/WW/file4.exe	0%	Avira URL Cloud	safe	
http://www.bqmqx.com/askhelp59/askinstall59.exeC:	0%	Avira URL Cloud	safe	
http://https://dependstar.bar/?username=p11_5	0%	Avira URL Cloud	safe	
http://https://dependstar.bar/?username=p11_4	0%	Avira URL Cloud	safe	
http://https://dependstar.bar/?username=p11_7	0%	Avira URL Cloud	safe	
http://https://dependstar.bar/?username=p11_6	0%	Avira URL Cloud	safe	
http://amzrouting.com/amz.exew	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt0#	0%	URL Reputation	safe	
http://hsiens.xyz/addInstall.php?key=125478824515ADNxu2ccbwe&ip=&oid=149&oname	100%	Avira URL Cloud	phishing	
http://194.145.227.161/dlc/sharing.php?pub=mixonerogramDataAPPDATA=C:	0%	Avira URL Cloud	safe	
http://212.193.30.29/WW/file4.exet	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/va	0%	URL Reputation	safe	
http://194.145.227.161/dlc/sharing.php?pub=mixoneTIFIER=Intel64	0%	Avira URL Cloud	safe	
http://212.193.30.29/WW/file4.exez	0%	Avira URL Cloud	safe	
http://www.iyiqian.com/	0%	URL Reputation	safe	
http://https://dependstar.bar	0%	Avira URL Cloud	safe	
http://https://c.goatgameh.co/dlc/sharing.php?pub=mixone	0%	Avira URL Cloud	safe	
http://amzrouting.com/amz.exeB	0%	Avira URL Cloud	safe	
http://https://dependstar.bar/?username=p11_1	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.bqmqx.com/askhelp59/askinstall59.exe	100%	Avira URL Cloud	malware	
http://artguide.top/foradvertisingwwb.exeLj	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
193.56.146.76	unknown	unknown		10753	LVLT-10753US	false
52.217.96.20	unknown	United States		16509	AMAZON-02US	false
212.193.30.29	unknown	Russian Federation		57844	SPD-NETTR	false
149.28.253.196	unknown	United States		20473	AS-CHOOPAUS	false
8.8.8.8	unknown	United States		15169	GOOGLEUS	false
104.208.16.94	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
52.95.149.18	unknown	United States		16509	AMAZON-02US	false
65.108.20.195	unknown	United States		11022	ALABANZA-BALTUS	false
104.192.141.1	unknown	United States		16509	AMAZON-02US	false
85.208.48.152	unknown	Germany		61317	ASDETUKhttpwwwheficedcomGB	false
162.159.129.233	unknown	United States		13335	CLOUDFLARENETUS	false
37.0.10.199	unknown	Netherlands		198301	WKD-ASIE	false
104.23.98.190	unknown	United States		13335	CLOUDFLARENETUS	false
2.56.59.42	unknown	Netherlands		395800	GBTCLOUDUS	false
145.131.16.92	unknown	Netherlands		8315	SENTIANL	false
172.67.189.190	unknown	United States		13335	CLOUDFLARENETUS	false
34.117.59.81	unknown	United States		139070	GOOGLE-AS-APGoogleAsiaPacificPteLtdSG	false
107.148.201.36	unknown	United States		18013	ASLINE-AS-APASLINELIMITEDHK	false
74.114.154.18	unknown	Canada		2635	AUTOMATTICUS	false
20.189.173.20	unknown	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	false
162.159.133.233	unknown	United States		13335	CLOUDFLARENETUS	false
163.181.57.228	unknown	United States		24429	TAOBAOZhejiangTaobaoNetworkCoLtdCN	false
208.95.112.1	unknown	United States		53334	TUT-ASUS	false
5.188.38.39	unknown	Russian Federation		199524	GCOREAT	false
103.155.93.165	unknown	unknown		134687	TWIDC-AS-APTWIDCLimitedHK	false
37.0.10.244	unknown	Netherlands		198301	WKD-ASIE	false
185.215.113.208	unknown	Portugal		206894	WHOLESALECONNECTIONSNL	false
52.218.101.152	unknown	United States		16509	AMAZON-02US	false
185.46.11.66	unknown	Russian Federation		43146	AGAVA3RU	false
5.9.162.45	unknown	Germany		24940	HETZNER-ASDE	false
47.251.42.216	unknown	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	false

Private

IP
192.168.2.1

IP
127.0.0.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	534003
Start date:	04.12.2021
Start time:	23:27:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 17m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	912534A5380738D96E8DDB7873ECB004667D72D5DF783.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:	56
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@80/115@0/34
EGA Information:	Failed
HDC Information:	• Successful, ratio: 27.8% (good quality ratio 20.6%) • Quality average: 67.7% • Quality standard deviation: 42.8%
HCA Information:	• Successful, ratio: 62% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All
Errors:	• Sigma runtime error: Invalid condition: all of selection* Rule: Conti Backup Database • Sigma runtime error: Invalid condition: all of selection* Rule: Stop Or Remove Antivirus Service • Sigma runtime error: Invalid condition: all of selection* Rule: Conti Volume Shadow Listing • Sigma runtime error: Invalid condition: all of selection* Rule: Compress Data and Lock With Password for Exfiltration With 7-ZIP • Sigma runtime error: Invalid condition: all of selection* Rule: Disable or Delete Windows Eventlog • Sigma runtime error: Invalid condition: all of selection* Rule: PowerShell SAM Copy • Sigma runtime error: Invalid condition: all of selection* Rule: Compress Data and Lock With Password for Exfiltration With WINZIP

Simulations

Behavior and APIs

Time	Type	Description
23:28:08	API Interceptor	22x Sleep call for process: powershell.exe modified
23:28:16	API Interceptor	58x Sleep call for process: Mon0699e256d5dc14.exe modified
23:28:20	API Interceptor	593x Sleep call for process: Mon06434adde6c2.exe modified
23:28:45	API Interceptor	3x Sleep call for process: WerFault.exe modified
23:29:41	API Interceptor	2x Sleep call for process: Mon067df200a8fd43b.exe modified
23:29:49	Task Scheduler	Run new task: PowerControl HR path: C:\Program s>Files (x86)\PowerControl\PowerControl_Svc.exe
23:29:50	Task Scheduler	Run new task: PowerControl LG path: C:\Program s>Files (x86)\PowerControl\PowerControl_Svc.exe

Time	Type	Description
23:30:13	Autostart	Run: HKLM64\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce system recover "C:\Program Files (x86)\autoit3\Cemelupozhe.exe"
23:30:57	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run WinHost C:\Users\user\AppData\Roaming\WinHost\WinHoster.exe
23:31:32	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run WinHost C:\Users\user\AppData\Roaming\WinHost\WinHoster.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:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Mon06d47d8fde50.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06d47d8fde50.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	700
Entropy (8bit):	5.346524082657112
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhat/DLI4M/DLI4M0kvoDLIw:ML9E4Ks2wKDE4KhK3VZ9pKhgLE4qE4jv
MD5:	65CF801545098D915A06D8318D296A01
SHA1:	456149D5142C75C4CF74D4A11FF400F68315EBD0
SHA-256:	32E502D76DBE4F89AEE586A740F8D1CBC112AA4A14D43B9914C785550CCA130F
SHA-512:	4D1FF469B62EB5C917053418745CCE4280052BAEF9371CAFA5DA13140A16A7DE949DD1581395FF838A790FFEBF85C6FC969A93CC5FF2EEAB8C6C4A9B4F1D55D
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.CSharp, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Dynamic, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1234_0402[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	data
Category:	dropped
Size (bytes):	1584996
Entropy (8bit):	6.6707364134457325
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1234_0402[1].bmp	
SSDEEP:	24576:AL0m485/dyq4FTqBok7wHDv2+wfBHYSaSs7GaD:ALZh5/dyNTAUHDYHY57GaD
MD5:	AED481A4F86FAD194F708239628BED73
SHA1:	44B91743C6D323CB58183E80D82269A0C282C353
SHA-256:	7D2942DCD4C245456EAA2F90AF4D36635938197A33A5EF51FB728C41E9900A59
SHA-512:	D4A6E96CF6151D95EABF1D3FBC5B78C241832016C85670E631166F6898887D686A6B0756252DF5094655D0401222D2FB0ED14068142D095E0849502BAB073B96
Malicious:	false
Reputation:	unknown
Preview:	...]....uq.1.>...-...Y.....A(.|.u%3.....o.....D....KX...0.....L..... .....FG.....}.....!.....}.....s.....A..... .....].....=.....}..... .....q.L.Z..+&.+..(..2w-....d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\1234_0402[2].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	data
Category:	dropped
Size (bytes):	1584996
Entropy (8bit):	6.6707364134457325
Encrypted:	false
SSDEEP:	24576:AL0m485/dyq4FTqBok7wHDv2+wfBHYSaSs7GaD:ALZh5/dyNTAUHDYHY57GaD
MD5:	AED481A4F86FAD194F708239628BED73
SHA1:	44B91743C6D323CB58183E80D82269A0C282C353
SHA-256:	7D2942DCD4C245456EAA2F90AF4D36635938197A33A5EF51FB728C41E9900A59
SHA-512:	D4A6E96CF6151D95EABF1D3FBC5B78C241832016C85670E631166F6898887D686A6B0756252DF5094655D0401222D2FB0ED14068142D095E0849502BAB073B96
Malicious:	false
Reputation:	unknown
Preview:	...]....uq.1.>...-...Y.....A(.|.u%3.....o.....D....KX...0.....L..... .....FG.....}.....!.....}.....s.....A..... .....].....=.....}..... .....q.L.Z..+&.+..(..2w-....d

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\7e248_0401[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	data
Category:	dropped
Size (bytes):	675844
Entropy (8bit):	7.606679429916527
Encrypted:	false
SSDEEP:	12288:BRx2n3cWH2QEVD5VdtXyd/yeYstcD5LDlkdY4T2iLrP9Z:jxC/H21lY/yPZk+IrP/
MD5:	CDBAD69C1BF8FE6D59D0D230301571A4
SHA1:	2F4243F545ACA03385F9B79E494C47E6432423EB
SHA-256:	CA1813B564264304DC658E72798305B0EB35ED658E17B5E5E392E2324CEE8DAA
SHA-512:	A1C102BE3E13180813FBD664B866B327535D22DDA26BCE0BE92104ABD0A15D651B465A2CEF2B6E80203EBD3F94F342862217D1FBBC5B53606ED644646CD968D A
Malicious:	false
Reputation:	unknown
Preview:	...]...........bb..%.....}....'..).P.%..P.....;.....r...r...r.a..e.r.a....r.a.....r.X0..x.r...s...r.a...~.r.a..~.r.a..~.r.....r.....}..... .....U.....].....!.....=.....]..... .....Ax...-...9.....].....=..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\HwL0301[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	data
Category:	dropped
Size (bytes):	858524
Entropy (8bit):	5.987742169958862
Encrypted:	false
SSDEEP:	12288:jSosO9Y3XUhXjyRYNfc+1JaYB+l1rE2BoDd+3JDc:j/xYHoGRYdc+nbB+l+U7Dc
MD5:	0D147EDA7A4CB444D881EDA1BECCB7F9
SHA1:	178DB6612DE895DFA5D22F51823EF6ED35820B49
SHA-256:	6A9BE3032914BA38DA23886219E4E27B0D8ADA683243CE4E05CCB1B981715565
SHA-512:	F81B5D9D070CE4475638B42D1032A96E72A9E8FBB9CC47798DDA43074F828667EF5E9B0D805DD39AC2D3B2CCE4ECDBDBB7AD38BDDA4E4D32F29F9D2A8701E D81
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\HwL0301[1].bmp	
Reputation:	unknown
Preview:	...]...........bb..%.....'..).P.%..P.....tK.=.....}.....q.....#..... .....G.....k.....Yw.....q.....G.....s.....i.....=..... I.....Q...Q...>.....c.....c.....c.....\.....c.....c.....c.....c.....c.. .....^.....c.....V.....c.....c.....<.....'.....M.....?...>.....c.....c...9...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\NiceProcessX64[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.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: 86%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....I4.!.U.r.U.r.U.r.>.s.U.r.>.s.U.r.>.s.U.r.:.s.U.r.:.s.U.r.:.s$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\0W10PBUV\SoftPInstaller0401[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	data
Category:	dropped
Size (bytes):	134148
Entropy (8bit):	7.605563463974317
Encrypted:	false
SSDEEP:	3072:SMbEv8J6CXKrfQtfNjq7pp/trmndI9+9kMZ7PG:SMxXcYTjqlVt6FkMhPG
MD5:	39538DF1A3981A0CF4B72F56A871EA51
SHA1:	1B9748845DE5928964106582531E016BBC8529DF
SHA-256:	F68C853BEE40E686199308926D3EE0CCA2709F2DFF6C9AA613D81E25166374BC
SHA-512:	D57FA725033CE2A17C076DD7D67A115E1126DC88767789FC8758D507CF8D8948E09B5E4A2A276FDE42F1C532CACE36E6572392D67DA59CE2AD4B3478A52A06
Malicious:	false
Reputation:	unknown
Preview:	...]...........bb..%.....'..).P.%..P.....6.....}.....=..... .....}.....5.....m..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Topov0401[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	data
Category:	dropped
Size (bytes):	1594420
Entropy (8bit):	6.725900726106779
Encrypted:	false
SSDEEP:	24576:sL0m485/dyq4FTqjMlFZw83WDys3Ei3FZ:sLZh5/dyNT46ZwJDycEiVZ
MD5:	BAE26E384178E4D8F976A528C11A0567
SHA1:	03D77A6B2D923EF452F66830C28831BA64D46077
SHA-256:	37D185ED5A2ACA00D4FBE5A1A8DB36D47D227663C89E3CDB1DC9513E213CB67C
SHA-512:	1725A957078E8EE07AC856222EFF3B9CC61D5E3BEFE9368EBDDCC91691C4BAE1E322FA75368E9CE6CBD48DF151BA0ADD601C96B4D71EA2DF07D98C0BA536A 191
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Topov0401[1].bmp	
Preview:	...]....uq.1.>...-...Y.....A(.|.u%3....o.....D....KX...0.....L..... .....Hz.....}.....!.....-.....}.....Q.....q..... .....]....q....q.....=...-..~.....}..... .....OD//ZW/..[4\..EU.X..D

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Uponrun[1].exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1353728
Entropy (8bit):	7.627858865969598
Encrypted:	false
SSDEEP:	24576:hMxBw0ghWHYkSi3fgmFxcvv/RCVZEryaXDykVwDS+soqwSGI8:zWHlSi3fg+kBwDS+1qw1
MD5:	DF7CF1092B66BAD6905E0F4C66D314ED
SHA1:	232CCED627B8263DEE9328C850E2C099F06F8B95
SHA-256:	5AAC592F8CF0F53A57E7B44D891442C5C002E47D993890B58BD4812D8309EE4D
SHA-512:	CB02FA9EAE6B91BE6AB8F0650520F66D84C2C830A86E330EBBA533A6860B43365AF88BF8E816A3BA01CC0E4AAFEFAABED2F55866B84FBA5FC5B8FA5D9CE53174
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 41%, Browse • Antivirus: ReversingLabs, Detection: 89%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....G.a..... .....@.. ....@.....O..... ....H.....text...4.... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....)...|.....0..._.....~....,.(.....(....~....,.(.....(....~....,.(.....(....~....,.(.....(....~....,~.... ....Z(....~....,r...pr.. .p.(....&..8....~.....o.....~.....o.....~.....o.....~.....o.....(.....~....,...(.....~....r...p(.....,(....r...po.....(.....+)~....r1..p(....,...(....r...po....(.....(....(.....(.....(.....X..~....o....?....~... .&*..0../.....s.....s.....s.....o......,

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\app0301[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	data
Category:	dropped
Size (bytes):	4300332
Entropy (8bit):	7.94763660679426
Encrypted:	false
SSDEEP:	98304:5rLSI3kFtchw7egdngaEcMTnE5r9khwn7iU4eHo:hLSI3kF76gF3EciE5rywn7R4eI
MD5:	9F8D3D9EB15C7C32864B0B6489A4DA2B
SHA1:	F9922EB35AC972C36CEB08B968717DA32CB4E828
SHA-256:	5714B7270EE1FBB3565A5C2FA0DF6789DA50822A1A47F4BB83F21E7CB510B37E
SHA-512:	3602922339407F36B913215FC8D058259B6743C79A116D9A96495EA0D59B912B62E30A0F7439A5EE746A557BD5E208F57F376A06A3FB099E730600381E7453CF
Malicious:	false
Reputation:	unknown
Preview:	...]..... bb..%.....m.....'..).P.%..P.....X..Q9..Q9..Q9...w..P9..>O4..9..>O..O9..>O5..9..XA..R9..Q9...9..>O0.P9..>O. .P9..>O..P9.....Q9.....C.....}.....=.....q..... .....V.....A.....].....k.....=..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\filinnn0301[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	data
Category:	dropped
Size (bytes):	1623260
Entropy (8bit):	**7.993473863398102**
Encrypted:	**true**
SSDEEP:	49152:bgdwxKk5fKTYlCpY6H3GS3DyS6jKfz1AeH2e:lw1KklaXGYOSVx5
MD5:	240B2CC8DA75B0A537BCE76D694A9371
SHA1:	42460FA7690763915AA6154CF572CA880938688C
SHA-256:	1934940FA8810241CD8478F584DDC20BC3F0F0BD03E3F9565019616870C46263
SHA-512:	9E647D5B1A593013D44C96ADE84A45C09A78424E3179B67D85CA4792083A81E367FD1ED111CD13ECEFDA5653DAC7508817240AB7B3114F1F748116204217619A
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\filinnn0301[1].bmp	
Preview:	...]..........bb..%.....'..).P.%..P.....7.....}.....E..... .....}.....}.....=.....}.....]..... .....}.....}.....}.....=.....}.....]..... .....}.....}.....}.....=.....}.....]..... .....}.....}.....}.....=.....}.....]..... .....5.....}.....!.....}.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\help0301[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	data
Category:	dropped
Size (bytes):	419844
Entropy (8bit):	6.639403968592733
Encrypted:	false
SSDEEP:	6144:2b4BAoVvQTYuIB22YglAVvQ1IO7qMLReJTZapWE4gWfptYmvmEuJOddw5VCH16Hb:0YAEQTcgsWQx7j6WClwx
MD5:	5111F55E85097CD50870A56A284E88EC
SHA1:	39C4B8AA2A0464A4882319621C985B8AA2BF2FE9
SHA-256:	8A098703049A4DED68CB14265D7AE74A2756F0BDDB1195293722319 33C76283A
SHA-512:	CEF658C146BE9C705D2C950B15F5300B214C74FF05A5FEC9F49D4D966E3398AB14ACBA9F1B46B7082E75B1455F7055CAC908666B0C97BE5AEBF1C932D8B2551F
Malicious:	false
Reputation:	unknown
Preview:	...]..........bb..%.....e.....'..).P.%..P.....n>..*_._*_._*_._..0_+_._E)._._._E)6_4_._E)._._._#';_)_._*_._._._E)._+_._E)2 _+_._E)5_+_._...*_._.....>.....}.....''.....m..].....i..-..... .....%.....&.....E.....]....|....}.....w.....]....]....m.....s.....K..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\install_new0402[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	data
Category:	dropped
Size (bytes):	421380
Entropy (8bit):	7.111497578124489
Encrypted:	false
SSDEEP:	6144:kwk8S+5TIZQzvM9e5rK7qT+cObexh2PtvMipCaysiO87DTyfge0aH7k1:/k8ZNU7qTx1r2X3yrOWT20P
MD5:	B8443CD3F7B81935D842B655545D87A7
SHA1:	057644AD46022D8034F36992417340E1D5D6C143
SHA-256:	D53B22505420709029C14600ABEA65FE7DF194FEF28D6271B49C327988B5FF67
SHA-512:	00710319B2408C597DC72416F70410BCF5AAA4C9DB1D9885C185FB156093351EDECE8B31AA88130322083B6F2EF3C3D9FAF4E9BBC0B180A216E0855CFBA5CAD
Malicious:	false
Reputation:	unknown
Preview:	...]..........bb..%.....}.....'..).P.%..P.....T..5...5...5...g...5...g..45...g...5.....5...5..<5...g...5...g...5...g...5.....5.....~... .....}.....}.....N..... .....]..... .....6.....U..... .....x...M...9../.....].....].....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\lance[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	data
Category:	dropped
Size (bytes):	1616628
Entropy (8bit):	6.596892624142386
Encrypted:	false
SSDEEP:	24576:rDhWpG3R4J4+GbChXIBEdsJiHEA8J0MXJhyXwaF82x7i8sKbn+g2EcbmOGxxeJxL:rFGeZ+pEEHE7ZGp82xVb+gxleJN
MD5:	E4577659FADA268079F65C51A8DB2EAB
SHA1:	662DF43BB5CD7AC0350D9656CC8E87A0101670D3
SHA-256:	9B9CF563B86A9B4E4EDC848BE856135CC86806691947906C294EFB4FDB03FEF4
SHA-512:	D2A120CD93B2BAAC9C975D156F32ABD240F1DF9A073C819481A5E10749650D9CD4DC5A22D0D6FAA38261AC2B84D4913D0E49A8D11B99B9FE589830AA27B2274
Malicious:	false
Reputation:	unknown
Preview:	...].....uq.1.>...-...X.a"`.Ar>o.....Eq....6..K...(....<._.....L..... .....T.....}.....!...s.....}.....r.....I.....N..... .....].....N.....N.....G.....}..... .....f...M...b...e.E..Y.~.9c...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\mill[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	data
Category:	dropped
Size (bytes):	1584164
Entropy (8bit):	6.717838503058161
Encrypted:	false
SSDEEP:	24576:hL0m485/dyq4FTqkWkkZSTq6VuuBg+40UgGI8ye1qT1:hLZh5/dyNT4RSe6VQx+e1q5
MD5:	54241D5F1D4927BF47A0158FE9A29063
SHA1:	250C97DE402F1A1CD47DF7F8BD6BD4C2437FE03A
SHA-256:	BB8667AF0B5FF8013F8A18FF4D80BBFEC45209A3BDD8C60C1DCFC5316931865E
SHA-512:	E36ACAA2F668B44D1108D4C8F000C5FBED113E8FDE679073CA67843B170583F57A1334B54A423BA364F09B96B7C9776C9AB0D36CE5A60A835B561B33BF3F6AB C
Malicious:	false
Reputation:	unknown
Preview:	...]....uq.1.>...-...Y.....A(.|.u%3.....o.....D....KX...0.....L..... .....&.|.....}.....!.....}.....I..... .....].....=.....}..... .....1-9.....Q>..9....U.J.[$tw

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\ruzki[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	data
Category:	dropped
Size (bytes):	1655580
Entropy (8bit):	6.671398706503429
Encrypted:	false
SSDEEP:	24576:7L0m485/dyq4FTq9UrX+F+Thq1Y3ARIQDSpgbQ:7LZh5/dyNT+UrXtThq1SwIQmibQ
MD5:	618879FBEDF8FBADA8C24466E0F45D4B
SHA1:	121E11E73D3202AA8BB58B67B512AED332DBC8FF
SHA-256:	B1686D5FB387C5330393DB5F66775955786A435F1CB91002A0052FFF808F81A4
SHA-512:	931E80FDC1D55286C8B38EAC014FFCDE1DB6F528DB221E4ED7CA2172E554192832C2E16D269D845F6CB8F674E1E6E33DFC00E14D18F13B51CD8EE2F67FF3E5 C
Malicious:	false
Reputation:	unknown
Preview:	...]....uq.1.>...-...Y.....A(.|.u%3.....o.....D....KX...0.....L..... .....@cdG.....}.....#.....-.....}.....G.....A.....I..... .....].....I.....I.....=...-..8.....}..... .....M8...ax..aPM..N....\.E}.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sfx_123_310[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	data
Category:	dropped
Size (bytes):	1271304
Entropy (8bit):	7.876403861670934
Encrypted:	false
SSDEEP:	24576:I5rCCDttjFaXq1f2VhZm9VdPatyRW4E6IL9O9NSvtGJ:IRCCDHFaXq9M+VdPr3EK9NSvS
MD5:	58CF10BAD2ADF96413FCADCE17904D10
SHA1:	E38BC7EAC5E475639F3885628E4A9060BE2FA7F1
SHA-256:	30F63DE1D0DAE84127A2E7A5CAD88310FD57BD6D86D5520C2B27520AC888DE6A
SHA-512:	2C841403760F36563714A8A1EC339036BB2FDB0284C9593E36430BCD0B442E75F120A5D9DED13A0F099315AB92FF3788FAA92FE752724DD8CA14F291C6B01516
Malicious:	false
Reputation:	unknown
Preview:	...]..........bb..%.....'..).P.%..P.....N.c.....n.....n.....n.....R....1.....1.....1...#.....U....., ...~.!.....}.....e.....].....\.....].....i.....MB.....e.....?.....9..... .....].....].....MB.....}.....e..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\under0401[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	data
Category:	dropped
Size (bytes):	1712132
Entropy (8bit):	**7.994487067070858**
Encrypted:	**true**

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\under0401[1].bmp	
SSDEEP:	24576:xZ5hqVmfj5aPMJYighpf5lG00Kjiqe55q6B2H+aLpKkPhJxzpoyJeD2Molok:xjsdRZGOi7Lq6oFpJ1poAeGKk
MD5:	CAA8D3E04C1BB42606701ABA546C9224
SHA1:	38328E4281520227ACA75CEF2CFC13215C05A967
SHA-256:	B071596FB0A807D2228C90A4E0FC8FF348AA0011CD163CE354F70C02F4A9D2C0
SHA-512:	C5124457C97003A8BB23D69F61D4746D3597B5496F40EB3AA6C62E9FCDB6F21BF2F48D0C25CB4D2D07C78BB6A0833856CF3CF995910A2891421FAF0B8D55AC3
Malicious:	false
Reputation:	unknown
Preview:	...]..........bb..%.....'..).P.%..P.....$ .....}.....]..... =.....H..... Q..E.....=.....}.....]..... }.....}.....}..... .....}.....}.....=.....}.....O...;.....}.....]...]...5.....}.....}..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Setup12[1].exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3050456
Entropy (8bit):	7.983654030728459
Encrypted:	false
SSDEEP:	49152:pAI+1INT6MOHNYU+DLrIJFpAFiZxrB7dsPQDpvjQYTwhEzGM0ekmOCulFP6ihRf7:pAI+m6MSNYKFQi7rp249vcYECBPihl
MD5:	9DF053279BDD9B34A92EB605DE4FD8B3
SHA1:	A98225283A4FD39284A2AA53AA38173FCA38AC06
SHA-256:	4C43CDE240F407A02C557A37A17DC3252F9C3873B06A46D6185D2F7F6AFE1E8C
SHA-512:	4F968A307AD664FD0AE60034E165B8F71FD003790CB7B8A3BA9A49713A340D92CABC03CE69D1D55F3F6F68C3C2E9DD92DBF547492EC671AC7F5457D137C146 2
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 12%, Browse • Antivirus: ReversingLabs, Detection: 59%
Reputation:	unknown
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....F...|.....hT.....`....@.....0.....w.....@..... .....CODE.....D.....F..... ..`DATA.....(...`...*...J.....@...BSS.....t.....idata.....t.....@....tls.....rdata..... .....@..P.reloc.....@..P.rsrc.....@..P..... .....@..P..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\design0401[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	data
Category:	dropped
Size (bytes):	1578228
Entropy (8bit):	**7.992837829614341**
Encrypted:	**true**
SSDEEP:	49152:1a403bBL1dvZBMQ8OlYiSCVH2AePf20fQ++mN:YzLBM+lYiSWH2e0fQ++mN
MD5:	BC969C492DAD8AE207BB26BD9CD26BD3
SHA1:	D54E5A59A3BC388DCFA978140CB45FD436BFB087
SHA-256:	EED384E45727661E5E0CB210ADC2FC74F268681D9F447863E57305B315AEA04D
SHA-512:	8B42A97C10FD6E3C501B3C8B97737E031508E4C10CC80F4920B85BE3CE8393D2773692A1980E11D6064A970F93CA479A60FC273565E791102DE66D2924E54261
Malicious:	false
Reputation:	unknown
Preview:	...]..........bb..%.....'..).P.%..P.....2.h.....}.....]..... .1..E.....=.....}.....]..... }.....}.....}..... .....}.....}.....=.....}.....!...5.....}.....]...=...5.....}.....}..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\real0403[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	data
Category:	dropped
Size (bytes):	754180
Entropy (8bit):	7.626807189452252
Encrypted:	false
SSDEEP:	12288:Lm4zjJKet4CC4IJfp4Iot2sA5CeOou9MgpBYWT8obr/ClcEPsm1UQOuCGq+m5U2z:q4zjxt4CC4o4IHlEj/Y884jCemqQgkEz
MD5:	1722428380A8B66B0984FC0A1DAD7777
SHA1:	21DC5572E7406DF01F8DAF8422CF2B91D5549D8C

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\real0403[1].bmp	
SHA-256:	833506165347562 19CD5FF77895349101AEAE9B350FED103578ECE192E509AF9
SHA-512:	789F8E9B52E30740B786F2638857FC4D384DC9EA780233251F42F014AF01AC5ED5A9CB1DBF4EF4011B4CEF5D101B8EFF9818CFE8998055533CF3E909D47C659
Malicious:	false
Reputation:	unknown
Preview:	...]...........bb..%.....}....'..).P.%..P.....T..5...5...5...g...5...g..45...g...5....5...5..<5...g...5...g...5...g...5.....5.....e... .....}.....].....P.....M.....&..... .....x...}...9...[.....].....z...M..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\AordVPNWZ3202111221117[1].exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	29676504
Entropy (8bit):	**7.99622998723258**
Encrypted:	**true**
SSDEEP:	786432:kPLBBBAarluFO0Y2LiZsBlQ04FN4Tn4EGK:uXAjAvwiZsBlPTnhT
MD5:	BF7E997F53E2FC3BD8D0E6E5E8782FA2
SHA1:	7497EBAA4D19912B838372430DE65D671054F5E5
SHA-256:	C2B27A37E47861DE9994783D85F661162C9E9B4EAA450348748639BF1E7DC99F
SHA-512:	DD65F41420D3DBB7F0F460DA35B235E950D750C8FDD76DD63BD21E16257D3EE7FBEB0B9EBF28BD1F4E466C749A88C3AB71348CAA9F7BA92B64B43518F1033 BF
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 6%, Browse • Antivirus: ReversingLabs, Detection: 4%
Reputation:	unknown
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...I.m^.....`.....n.....@.....0.....50....@.....@.....P.....0..... ....*.....p..... ...2..@....@.....text...HF.....H..... ..`.itext..h....`.....L..... ..`.data....7.....8...d.....@....bss....xg.....idata.....0..... @....didata.....@.....@....edata.....P.....@..@.tls.....`.....rdata..]....p.....@..@.rsrc.....@..@..... .....@..@.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\PL_Client[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	data
Category:	dropped
Size (bytes):	1341956
Entropy (8bit):	6.710274489426762
Encrypted:	false
SSDEEP:	12288:CBxvo3SsGknj0YGPQ/fL/rcPt8B7O3FAhlhPZF2vhPZPgu4WKbIgF/QhPQhPZPgA:Cr8Ss10YjnLDcVg4aDtpw2OFNl1vi3
MD5:	5326331C85F3F09526D88E387A7D92E5
SHA1:	BB06C6A2F1C76FDF010BC0728FBCDBB9C1238FA1
SHA-256:	AFADAEE973ECF0272BE793A321C6A065390BF3FDD362D2E2E6D95E4A6B9256B2
SHA-512:	A7653990F06A764F6217C3645969458CC58B4C448D5A2ADF5212882B91DA18D21E4CB4D0F3822175795C3688860EC7C66E0BDBA5B6743DF8234071EB5D5C1D3
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\PSUEOSZZ\PL_Client[1].bmp, Author: Florian Roth
Reputation:	unknown
Preview:	...]...........bb..%.....'..).P.%..P.....<...R...R...R...QT..R...WT/.R...VT..R.....R...WT..R...VT..R...QT..R...ST..R...S.7 .R.V.ZT.R.V....R.....R.V.PT..R.....R.....5:.....}.....]...A.....M.....M.....V.....j..... .....M..).....#.....].....M.....Y.....}.....W.....].....j.....e..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Service[1].bmp	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.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\PSUEOSZZ\Service[1].bmp	
Antivirus:	• 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\PSUEOSZZ\Udp[1].exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	421376
Entropy (8bit):	7.113053483334034
Encrypted:	false
SSDEEP:	6144:BqztsmVs7Z1tyFvD1EFBEmHvKzjVQAARnB8cmP6UlFwK+eBvfxg4S1:BqB5sZSD1EF2WvKQR8cc6gFwAJg4S
MD5:	6F9E546026262180D94EB594EAB11705
SHA1:	34C797AFD80531BD114C86759078AAC8073E8562
SHA-256:	1A88073C331184DF09635FA1A9A73A67C064EE49F57D896F304347D6357A14C4
SHA-512:	B60BBB8474A99EE98E388501D4BEAABEC407AFF4EBFCD305E38F9583CE63D51995D089B22ED8DF2E3A39082528FACBD76F4DA0A94742DB232FCB40516848A5F8
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e.hD!...!...!...?...;...?.....?.....n}.&...!.....?... ...?... ...?... ...Rich!.....PE..L.....`_.....d...Z.....=7.....@.....P.....@.....@.....text....b.....d..... ..`.rdata..\l.....J...h.....@..@.data.....@....rsrc...@.....V.....@..@.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\askinstall42[1].exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1515520
Entropy (8bit):	6.6504077407296345
Encrypted:	false
SSDEEP:	24576:qEpfLmZkUtN/Wy+jtYkQkbF7vZjHYdG/9QDkMhJgXgaFJAIQiFX:bpylrKY2m4+7/gXgaFJT9FX
MD5:	F41CF108FA69603EAC9C6876E15DF7F4
SHA1:	1769AD4196D67936025E7CA2EBD73EB5475ED559
SHA-256:	0BE56CF2F98C19535B17E425094EBC300AB4FD020DDC82A7B955126ACFC59D4A
SHA-512:	A1FF7A27334F8FBE00324E52CBDAD702264494E1BECEB12587708A65740391B97AE5E56FE44A2915A76050D062C464C81AC970A9111388E3F19391CF32F6D68F
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Socelars, Description: Yara detected Socelars, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\askinstall42[1].exe, Author: Joe Security
Antivirus:	• Antivirus: ReversingLabs, Detection: 65%
Reputation:	unknown
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....@.....-.....+.w.....+.....*.....-.....&.....*.....(...../...../.7....*.....+.....,.....Rich.....PE..L.....a.....z.....S].....@.....@.....\|4.....6..... ..`.....8.....@.....H...@.....text..... ..... ..`.yukiess.X...0...Z...$..... ..`.rdata..:.....~.....@..@.data....w...P.....6.....@....yukiessP.....d.....@....rsrc....6.....8...f.....@..@.reloc..`.... .....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\askinstall59[1].exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1515520
Entropy (8bit):	6.650399929218108
Encrypted:	false
SSDEEP:	24576:jEpfLmZkUtN/Wy+jtYkQkbF7vZjHYdG/9QDkMhJgXgaBJAIQiFX:QpylrKY2m4+7/gXgaBJD9FX
MD5:	007D615236090B4DCF1C1C979C124A0C
SHA1:	BDDA130320670DD4D92CC5AA4463ECE6D90C558C
SHA-256:	50D4C7CBC4AE809095AA8173B3668420A15277D3C18166FA0D2E043638BF3111

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\askinstall59[1].exe	
SHA-512:	F30AE210A6EAF22CA922F68EC1486FBCFA4C428A107EB4785BB55A9EEF599DD1475807556ABCF8C351497D1F9858D013FF1B4B44D40AE3A88103E706D48CE24 6
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Socelars, Description: Yara detected Socelars, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\askinstall59[1].exe, Author: Joe Security
Antivirus:	• Antivirus: Metadefender, Detection: 47%, Browse • Antivirus: ReversingLabs, Detection: 96%
Reputation:	unknown
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....@.....-.....+.w.....+.....*.....-.....&.....*.....(...../...../.7.... .*.....+.....,.....Rich.....PE..L.....a.....z.....S].....@.....@.....\|4.....6..... ..`.....8..... ...@.....H...@.....text..... ..... ..`.yukiess.X...0...Z...$..... ..`.rdata..:.....~.....@..@.data....w...P.....6.....@.... yukiessP.....d.....@....rsrc....6.....8...f.....@..@.reloc..`.... .....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\ferrari[1].exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	420864
Entropy (8bit):	7.108935296953452
Encrypted:	false
SSDEEP:	6144:+oztsDVs7Z1tyFvDDQCysshSzXOMlS6JmLcA2LE9B+0hOKzZo4A1:+oBAsZSDDQCyssQX+6QL3T9B+rK24A
MD5:	E59FE8EBCC566952658B3D0AFC3AFCB1
SHA1:	66A2A99F16B66F67492FF8AD3C9895B283988F76
SHA-256:	79B245557B3B30E1D7DF10D212F6BC8EAA7134FB99BE5B1C7E93B9A61D080AD8
SHA-512:	34173D80AE89EE825E25D7CB326E3131CA07749C9324865740949BD235484D4A49C45A8B8E72A1E20ACAF1076F38854F0B1A7CE0936807ACFA3CBA477E203E25
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e.hD!...!...!...?...;...?.....?.....n}.&...!.....?... ...?... ...?... ...Rich!..... .....PE..L...0uG`.....b...Z.....=7.....@.....O.....P.....@.....@..... .....text....`.....b..... ..`.rdata..\l.....J...f.....@..@.data.....@....rsrc...@.....T.....@..@.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\file1[1].exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1791712
Entropy (8bit):	**7.994286100518312**
Encrypted:	**true**
SSDEEP:	49152:ud3+YjGSkgxjmxnCe06IUkfLkoNauU6NV4+:uUYjGWcCeUZowpK+
MD5:	5525DB91A602F578DE98EB9AF0B767D2
SHA1:	0F5EF84853E2EDC7F1399852051D04855AF1ADD0
SHA-256:	D7AE0785ECBECB35BC33FD7B50687037F439AAFC2EAA436C220A14EDC41D8F12
SHA-512:	5B4218D8A9B88A4EDA6841C1A3FFAB5A13D000CC6741F6C41E1C2D411CE04CD330FD8B12713BAA9490B42D30C4920A2974AD684E794130C550AA666B88A43F8 B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...ig.....0..... ... .@.. .....?.. ....9. .....|.:.....`.....@..... .....@..... ..... .....@.....@.....@..... ..@.....@....rsrc... ...`.....@.....@8.....@....rz7RpXi.....:.....@....adata... .... ?.....N.....@.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\hiddis_setup_add[1].htm	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	4323
Entropy (8bit):	4.966457667673525
Encrypted:	false
SSDEEP:	96:1j9jwljYjyDK/DZD8jH+k16cvJADh/pRs5sXszbGD:1j9jhjYjWK/lyH+k6cRADh/pm5sXsfGD
MD5:	1F04720AF4B12E3300187B4031260214

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\hiddis_setup_add[1].htm	
SHA1:	1B54FC1A51CD128580EB0E0D7EB3DABA5EBA4832
SHA-256:	FA55E173B327E08882519D28EE60482B7C81EE6FDB1F5A9E358629D69C0E80E3
SHA-512:	86FF0B926A1F5DD2C767459FEDCBF086B9C4D594B4AB66A64E873EEA111C01F773F92E7DC09EC4B4C13ADA0F376734BC74D5CABFF4C43CCC7E01CBA3A62C D19
Malicious:	false
Reputation:	unknown
Preview:	<!DOCTYPE html>. [if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->. [if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->. [if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->. [if gt IE 8]> > <html class="no-js" lang="en-US"> <![endif]-->.<head>.<title>Suspected phishing site | Cloudfl are</title>.<meta charset="UTF-8" />.<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />.<meta http-equiv="X-UA-Compatible" content="IE=Edge,c hrome=1" />.<meta name="robots" content="noindex, nofollow" />.<meta name="viewport" content="width=device-width,initial-scale=1" />.<link rel="stylesheet" id=" cf_styles-css" href="/cdn-cgi/styles/cf.errors.css" type="text/css" media="screen,projection" />. [if lt IE 9]><link rel="stylesheet" id='cf_styles-ie-css' href="/cdn-cgi/styles/c f.errors.ie.css" type="text/css" media="screen,projection" /><![endif]-->.<style type="text/css">body{margin:0;padding:0}</style>...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\setup_525403[1].exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	7587427
Entropy (8bit):	**7.996946142563**
Encrypted:	**true**
SSDEEP:	196608:91OstTOblOrPMNTQAmTUDWSRDixgNnDvX7d0ti/WthsmHiFzuNI3Q:3O4OkrmTQAm8WSVGmL7dKuWth/CkNI3Q
MD5:	A164D8B53BFCA9859BF45DE3765785EE
SHA1:	B4B12F8C87159E1F3EB8E6F6731D493DE72FD54F
SHA-256:	20CB22AEF742946E90AECE10451BECF27E43BB9CAFCB0A136B3B6869EBC2A4B8
SHA-512:	3CC667FC67125ADEEAB23097F1E397B8C195E81EB4D45BDDDC124662FDBED2A105B488E39E45C7B37433F27452CBEB796AD3F64CFC20BBE54536A03A377AF3 F1
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\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\siww1047[1].exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1407488
Entropy (8bit):	6.463710025379365
Encrypted:	false
SSDEEP:	24576:QH+9mwfaxNwTnfWKZrAZ/LD47RHQ9WFqc804cYq4IVJt:QH+9mBLwbfWirA5LsQ9W402YVJ
MD5:	90E040AD0BC66EF17D109D03218040D6
SHA1:	D70ECC79996CE88FDB1DEA83A012C586F2E8BC9A
SHA-256:	EF1A6DE96A75C8541E856D1811CD41E19EC65FF98D7ECA00DAF73615AE6C790C
SHA-512:	C0FB44FE1B4771599FB641DD3F11EFE776C2C2B767A14E5943B964FF594DE619B242EC3DEA63B4CF9597491ECCDCBCBCDA6D4117DE6BEE5344B3FE8685608 E4
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Generic_malware, Description: Yara Generic_malware, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\siww1047[1].exe, Author: Joe Security
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0...^...^...^...Z...^...]...^...[.Q.^.Q.[...^.Q.]...^..Z...^.]...^..[..^..._... ^..._.'.^.\.W...^.\....^.\.\...^.Rich..^.....PE..d.....a....."....@...6.....4".....@.....`.....x.....8..... ...J..p.....L..(...0K..8.....P..0.....text....?.....@..... ..`.rdata..`....P.....D.....@..@.data...d.....@....pdata..... ....@..@_RDATA.....R.....@..@.rsrc...8.....T.....@..@.reloc... ....."...X.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\BF1[1].exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	766721
Entropy (8bit):	6.100484546820966
Encrypted:	false
SSDEEP:	6144:d/QiQXCi5m+ksmpk3U9j0ltjuwsoxvjFEOTb9WmZX/8shzdsY4CpHPhn+UBE:VQi3ic6m6UR0lt6wp1hf39Wkv8xwJ3E
MD5:	BCB9F3E57C6CA459DD8408A7D7EF6C9E
SHA1:	6ADCDD9DFE71929F266C87D4713138AE3A8224DC

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\BF1[1].exe	
SHA-256:	9E987CF65077DE7825606813039AF92F72B685950CC2A055C5FD8EC676FF1EEB
SHA-512:	C61BED55533DA8766EC532D6AF10766C4460780F6E0E63A0E34BF1E9BF401793068F067B8E168AEF3261AC6029D7C3441149800997802265 1CB29B724DF91155
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\WJ8I2OL4\amz[1].exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	278528
Entropy (8bit):	6.35166785962771
Encrypted:	false
SSDEEP:	3072:7yTB8F8fejmNpVsYWJZYIDx9pJi8dKgMXUaFv1gnwaj03AHYegQMwu56Tv6X:21JfBVMsIVN67v17a4D4MaTSX
MD5:	F118C5D35478B3F97A4EA01DE61E4C85
SHA1:	7D31DFDE5DCECD20396EC1FD0D061BC63ECCD23C
SHA-256:	78BCB8651339AB0460A3C5D5DC8CC726B68B382A0F8D7DF60215C99BDF102C49
SHA-512:	0CC102D31C12491C52D74FC63CD3CA52DEF262DC5A3CE6BBEE46E3EC4525AAE7996D16B70792ACDAC9E20A2126813B3BBDA40AC57D3C9B222E4556624DB9 B2C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e.hD!...!..!...?...;...?.....?.....n}.&...!.....?... ...?... ...?... ...Rich!..... .....PE..L...n._.....6...X.....=7.....P....@.....uo.....P.....@.....P..... .....text...]5.....6..... ..`.rdata..\l...P...J...:.....@..@.data.....@....rsrc...@.....(.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\comprehensive1[1].exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1896234
Entropy (8bit):	7.921840655641192
Encrypted:	false
SSDEEP:	49152:7847rx6xgJW+GUy10f8rx3Su0H+fVLFZAKVS7eF1Hm6:7NAyJW+ny10f8rx3SupfVLFZdsQf
MD5:	C02926A3207BC28691D4FD6CED55D036
SHA1:	ABD050B7474651627E2FFF413E0DB8DCD1F27943
SHA-256:	239CA58590920FEF69005486D9B95FB7C556EA080EA2E349A360A869D8ADDB3F
SHA-512:	266DBDC406805E4773C34CE81412868E92832B1C9B8073F4226D2650154E377C068A385B64F501DCF3A51B329A8347AD75C4A681E7BC1D080D3006D11B5A6E72
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b`..&...&...&.....h.+.....j.....k.>.....^.$....._..0...._..5...._...../y..../y ..#...&...+...._....._..'...._f.'...._..'...Rich&.....PE..L....).`.....0....@.....@.....@.....@.....0...4...d...<....0..p.....|".....T..... .....U..@.....0..`..... .....text..... ..`.rdata.."....0.....@..@.data...(7.....@....didat..... .....@....rsrc..... ..0.....@..@.reloc..|".....$.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\file3[1].exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1650160
Entropy (8bit):	6.835466888014812
Encrypted:	false
SSDEEP:	24576:o9m1ERwuDhMrhn7WiDogqoPrZNUDI2A3rHik117wmZS4:o9m6RwwhMrhn7WiDogqozp3rHik11zV
MD5:	294C381E6D73739319D5162013F72162
SHA1:	06A8C8EC3C016BC9C381CF5F3B2FF4F1F048EE02
SHA-256:	45BD65B7EC522C1E8AEC332D7C29DF30036709FF7EB3D69E013D97DAD7C6C3DE

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\file3[1].exe

SHA-512:	9B06C050E1B6988F2DA0234E42F92B5B9EBFD5614D5E49ADC07E9EDA7E0E5A8D0CCE40914B1441AD31A8738AC977DCEDF03550385F638C2FEEDD60B19312FF10
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(..LY(.`...x.;.^U....,6A...5K/.#..DS.....Q..... .PE..L.....h..... .....@..... .....<#....@..... .....0..<M..... .....`..... .....@....rsrc...<M...0..<M.....@..@.....T.....@..... .....O\..d.@.bOS...I.....L.eR.C.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\install4[1].exe

Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	396800
Entropy (8bit):	7.027534750128602
Encrypted:	false
SSDEEP:	6144:xmTNLmVs7XZj0vjGgc+MtFEQ5R6h6qBFLiwJCuqV:xmBLmMXZSjrcVtHqBYq
MD5:	C2995AAAE4BBFFC3E883D36E10AC3C16
SHA1:	43E97FA4520E62133000174D9DF74B4C728A3C29
SHA-256:	725AD6618F1043A925591A5F93ED2F78C51CD7440007E80BFDC3F9072285392D
SHA-512:	7EF96772F79CA068F6486A803C426D8C1371A5C3C760F4A2126F41254B4F35A162E52A07915775E22232BDE8B897967C538B9319640BCEE1AC2DC1B94039A802
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e.hD!...!..!...?...;...?.....?.....n}.&...!.....?... ...?... ...?... ...Rich!..... .....PE..L....X._.....Z.....=7..... ....@.....M.....]..P....`..@.....K..@..... ..... .....text..... ..`.rdata..\l... ...J.....@..@.data.....p.....R.....@....rsrc...@....`.....@..@..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\toolspab2[1].exe

Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	279552
Entropy (8bit):	6.35917638560849
Encrypted:	false
SSDEEP:	3072:Q5Tu8F8fejyNpVsYWJZYIDx9pJi8dKgMXUaFv1ggMYuWVSLUFIQM3u56T:K6JftVMslVN67v1TgpLAHMZT
MD5:	C78C953BE09381236D245964E5E380FA
SHA1:	E76342EF91E0E1F2710CD97C9D9CFBE52C6F8872
SHA-256:	41A71A7A0DE2ADCB3476472F34C1D32EFCB54516F187E58D598CED5723100C31
SHA-512:	EEFBD9BBBD7C0110C27DCF5C9E88949E64C770E8D36E40499948C91AAFA96313C68910BE4DBC74691DC1B9F11F93AD06B604D17D4E9A6F59C76A07D60EF3FB98
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e.hD!...!..!...?...;...?.....?.....n}.&...!.....?... ...?... ...?... ...Rich!..... .....PE..L.....^.....:...X.....=7.....P....@.....)..... .....P.....@.....{..@.....P..... .....text...-9.....:..... ..`.rdata..\l...P...J...>.....@..@.data.....@....rsrc...@.....,.....@..@..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\xxxx[1].exe

Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	1480560
Entropy (8bit):	7.38643087410028
Encrypted:	false
SSDEEP:	24576:6io3nJlgcKBLzFbNj1EQHLiizd8V2bMYbCFbTj1tXQnfV4b6zN/Z7ut:6iQ7a9NjqQHLfziCkTjPQZN/Z7u
MD5:	AAD2435A3663422F7C49A1E0AC3500B8
SHA1:	62CE189E78B1A23EC74509516661863127C2966A
SHA-256:	3FB9AFB2B0957204767D11C03647EF5255BC4BFAEB0A3DC20F9C0773FE08FE95
SHA-512:	0D7176EBE813B5A55AB50F82E223A2DFAE6BDFEB3EAA056B6CC1088FED9E387FD9E1109ED6FFB4EE2320FE0C5BE71DD0B18E860C1D0F7D1E0D9110E7EFEEF2D2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\xxxx[1].exe	
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(.W...1....&ci!..N...T..5...l....qd.....b.....Q..... .....PE..L...O/.....0... .....@.....L,....@..... .....0..... .....`..... .....@....rsrc.....0.....@..@.....0...x.....@..... .....b.*.l..-.i.-.....~.....o_.F4

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22228
Entropy (8bit):	5.609223978238586
Encrypted:	false
SSDEEP:	384:/ztCDZCnMrnxZZxtjafu9S0nxjoklTItJ9gsS43QSTlGMZXZlbxV7l4WDlzZBDIs:4jx9tjhTxNlTuIsvXl5lfbZXVz
MD5:	B968ACE2EC2223FEBFE7CBA6C92BC8F4
SHA1:	0940CB7C093158D433A857FE9FB650467A63087F
SHA-256:	32CE4DE4921D0E779B63CFDFE157EA9EE6F8A0F4225DFE6FD02582FB980ECDC4
SHA-512:	7341ADED68A2C71D22A49ACB33C2638B32CA9B3E9604990C80FDD560072EB6C04AD480655D3AE810E416E39FF732527A7EBF6DD53B79BA8A4841E0E031B7F1D 0
Malicious:	false
Reputation:	unknown
Preview:	@...e.....l.....h.j.....F.....@.....H.....<@.^.L."My...:/..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automati on4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microso ft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....Syste m.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Trans actions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....Sy stem.Configuration.Ins

C:\Users\user\AppData\Local\Module_Art\Mon06dc62fb7183b9e.exe_Url_plmwxjco1mh2rarhkmu4d43wt11ojz2e\1.2.1.0\fb0nnnxr.newcfg	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06dc62fb7183b9e.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	964
Entropy (8bit):	4.8503380686722455
Encrypted:	false
SSDEEP:	12:TMHdGGqt1s26K9BQvDLI4MWiO691AiYfs26K9YG6DLI4MWivBRVcXHhuGnOLAiYV:2dqIK07E449KEK6E4Ev+X7QGnvo0vFr
MD5:	8E18625CD36F0075DA4BF0CE8FAC8204
SHA1:	0DF80AD1C5EA9BDDCB5CFCF2C60C6FB3DB903216
SHA-256:	35799F5570B76AA51478E74EA9D1C42B39BE157C3953A2B44047DD3ED2E629B1
SHA-512:	74D8BE6CDDFC1C13ACB30C18752D93EF8D57348B8B29220914ECB126AE8459318DD150B2F51299870119BDB6483F35417BAA988C688F0F621512C5A47E227C2(
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<configuration>.. <configSections>.. <sectionGroup name="userSettings" type="System.Configuration.UserSettingsGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >.. <section name="quick_screen_recorder.Properties.Settings" type="System.Co nfiguration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUser" requirePer mission="false" />.. </sectionGroup>.. </configSections>.. <userSettings>.. <quick_screen_recorder.Properties.Settings>.. <setting name="Preview" serializeAs="String">.. <value>True</value>.. </setting>.. <setting name="QualityIndex" serializeAs="String">.. <value>2</value>.. </setting>.. </quick_screen_recorder.Properties.Settings>.. </userSettings>..</configuration>

C:\Users\user\AppData\Local\Module_Art\Mon06dc62fb7183b9e.exe_Url_plmwxjco1mh2rarhkmu4d43wt11ojz2e\1.2.1.0\myvnba1h.newcfg	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06dc62fb7183b9e.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1101
Entropy (8bit):	4.825270421776283
Encrypted:	false
SSDEEP:	24:2dqIK07E449KEK6E4Ev+X7QGnvo0vLYvFr:crr7HKKE7Hq2QGng0DY9r
MD5:	0DFDBEE2FD28C743C8F14714B341E88C
SHA1:	35CC98517FFA98E5879DB0D3FB3A9C1FF99A0F27
SHA-256:	1AB59E3B2A99C37EE18614F27FA0D2308409810D2E2C3B9701F8242E0E26CA0C
SHA-512:	96EF620CB1BEC93AF3CE1CD16A4E9412048317164AF44F1DD3E6EE451557B6EC658F1CECFC61F556713528ABC572DD2F756E312A7C8F420FC9D98AB241C584 D
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Module_Art\Mon06dc62fb7183b9e.exe_Url_plmwxjco1mh2rarhkmu4d43wt11ojz2e\1.2.1.0\myvnba1h.newcfg	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<configuration>.. <configSections>.. <sectionGroup name="userSettings" type="System.Configuration.UserSettingsGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >.. <section name="quick_screen_recorder.Properties.Settings" type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUser" requirePermission="false" />.. </sectionGroup>.. </configSections>.. <userSettings>.. <quick_screen_recorder.Properties.Settings>.. <setting name="Preview" serializeAs="String">.. <value>True</value>.. </setting>.. <setting name="QualityIndex" serializeAs="String">.. <value>2</value>.. </setting>.. <setting name="Folder" serializeAs="String">.. <value>C:\Users\user\Desktop</value>.. </

C:\Users\user\AppData\Local\Module_Art\Mon06dc62fb7183b9e.exe_Url_plmwxjco1mh2rarhkmu4d43wt11ojz2e\1.2.1.0\oqzi3r40.newcfg	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06dc62fb7183b9e.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	842
Entropy (8bit):	4.901340076587983
Encrypted:	false
SSDEEP:	12:TMHdGGqt1s26K9BQvDLI4MWiO691AiYfs26K9YG6DLI4MWivBRVcXHhuGnOLAiYn:2dqIK07E449KEK6E4Ev+X7QGnvFr
MD5:	1B02B89AB3872D00C6A46CB4A7048DC9
SHA1:	0840AEFBBE40A00D7290D32CE8243DE3CF98339E
SHA-256:	AC8517EFBED88850A40943FBD667D9A06F6A156F0031109F59B4CA821AA22FD4
SHA-512:	0EEEE6C2CF1EAA11D561BA17ED65CAF97E069B5CCBF7420C3AE4BF88859F1273034A600DA91620411B12CD3241DCFABDC8D4DDD58218F2781254AC6CCF1FA19
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<configuration>.. <configSections>.. <sectionGroup name="userSettings" type="System.Configuration.UserSettingsGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >.. <section name="quick_screen_recorder.Properties.Settings" type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUser" requirePermission="false" />.. </sectionGroup>.. </configSections>.. <userSettings>.. <quick_screen_recorder.Properties.Settings>.. <setting name="Preview" serializeAs="String">.. <value>True</value>.. </setting>.. </quick_screen_recorder.Properties.Settings>.. </userSettings>..</configuration>

C:\Users\user\AppData\Local\Module_Art\Mon06dc62fb7183b9e.exe_Url_plmwxjco1mh2rarhkmu4d43wt11ojz2e\1.2.1.0\user.config (copy)	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06dc62fb7183b9e.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1101
Entropy (8bit):	4.825270421776283
Encrypted:	false
SSDEEP:	24:2dqIK07E449KEK6E4Ev+X7QGnvo0vLYvFr:crr7HKKE7Hq2QGng0DY9r
MD5:	0DFDBEE2FD28C743C8F14714B341E88C
SHA1:	35CC98517FFA98E5879DB0D3FB3A9C1FF99A0F27
SHA-256:	1AB59E3B2A99C37EE18614F27FA0D2308409810D2E2C3B9701F8242E0E26CA0C
SHA-512:	96EF620CB1BEC93AF3CE1CD16A4E9412048317164AF44F1DD3E6EE451557B6EC658F1CECFC61F556713528ABC572DD2F756E312A7C8F420FC9D98AB241C584D
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="utf-8"?>..<configuration>.. <configSections>.. <sectionGroup name="userSettings" type="System.Configuration.UserSettingsGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >.. <section name="quick_screen_recorder.Properties.Settings" type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUser" requirePermission="false" />.. </sectionGroup>.. </configSections>.. <userSettings>.. <quick_screen_recorder.Properties.Settings>.. <setting name="Preview" serializeAs="String">.. <value>True</value>.. </setting>.. <setting name="QualityIndex" serializeAs="String">.. <value>2</value>.. </setting>.. <setting name="Folder" serializeAs="String">.. <value>C:\Users\user\Desktop</value>.. </

C:\Users\user\AppData\Local\Module_Art\Mon06dc62fb7183b9e.exe_Url_plmwxjco1mh2rarhkmu4d43wt11ojz2e\1.2.1.0\user.configs_ (copy)	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06dc62fb7183b9e.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	842
Entropy (8bit):	4.901340076587983
Encrypted:	false
SSDEEP:	12:TMHdGGqt1s26K9BQvDLI4MWiO691AiYfs26K9YG6DLI4MWivBRVcXHhuGnOLAiYn:2dqIK07E449KEK6E4Ev+X7QGnvFr
MD5:	1B02B89AB3872D00C6A46CB4A7048DC9
SHA1:	0840AEFBBE40A00D7290D32CE8243DE3CF98339E
SHA-256:	AC8517EFBED88850A40943FBD667D9A06F6A156F0031109F59B4CA821AA22FD4
SHA-512:	0EEEE6C2CF1EAA11D561BA17ED65CAF97E069B5CCBF7420C3AE4BF88859F1273034A600DA91620411B12CD3241DCFABDC8D4DDD58218F2781254AC6CCF1FA19
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Module_Art\Mon06dc62fb7183b9e.exe_Url_plmwxjco1mh2rarhkmu4d43wt11ojz2e\1.2.1.0\user.configs_ (copy)	
Preview:	<?xml version="1.0" encoding="utf-8"?>..<configuration>.. <configSections>.. <sectionGroup name="userSettings" type="System.Configuration.UserSettingsGroup, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" >.. <section name="quick_screen_recorder.Properties.Settings" type="System.Configuration.ClientSettingsSection, System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089" allowExeDefinition="MachineToLocalUser" requirePermission="false" />.. </sectionGroup>.. </configSections>.. <userSettings>.. <quick_screen_recorder.Properties.Settings>.. <setting name="Preview" serializeAs="String">.. <value>True</value>.. </setting>.. </quick_screen_recorder.Properties.Settings>.. </userSettings>..</configuration>

C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon060579dda3b.exe	
Process:	C:\Users\user\Desktop\912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1448448
Entropy (8bit):	6.704983858178146
Encrypted:	false
SSDEEP:	24576:JIVFA1pqtg/TnMbX0lwyh0FVmEByU1fwFYyOs6bQCH6S8q4AQqYfqv:8FA1pvTMbOwa0TmYpMYEQNH6S8cQqYCv
MD5:	D06CD28108181A12FB2167831713A2A2
SHA1:	3C8FE09E692F814730CD8EFB37FC34446BD226BD
SHA-256:	2B337408770B08F1A5853778C35C4FE4AEC5DBFA353E50DD6FD7979C37EA9BBB
SHA-512:	E46DA49814DDFA3D6ACB8292B6CC5AA46ED4EEBEEE70E5ABB658CD2D58E9B377F770B70B31D660166F29A1EE6EA2BFC31F70F4E793DAB88D4442DC03C77A109D
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Socelars, Description: Yara detected Socelars, Source: C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon060579dda3b.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....4..g..g..g..f..g..fz..g...f...g...f.g...f..gi..f..g..f..g..f..g..f..g..g5..gi..f..gi..f..gi.Rg..g.:g..gi..f..gRich..g.....PE..L...p.Ea.....u.....@.....@.....D.....`.....@..$...`C..p.....pD.....C..@.....text...q/.....0..... ..`.ghhergf.....@.....6..... ..`.ghhergf.$...P...&...F..... ..`.ghhergf.....l..... ..`.ghhergfV.....p..... ..`.ghhergf.....t..... ..`.ghhergf..... ..`.ghhergf..... ..`.rdata.....@..@.data....w.....,.....@....ghhergfP....P.....@....rsrc.....`.....

C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe	
Process:	C:\Users\user\Desktop\912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	542208
Entropy (8bit):	6.547140461142
Encrypted:	false
SSDEEP:	12288:Vf10mGcWBCu+mijhqb7/J2xnwIjmTbpa:Vf10Ytqb7CwDs
MD5:	8A40BAC445ECB19F7CB8995B5AE9390B
SHA1:	2A8A36C14A0206ACF54150331CC178AF1AF06D9C
SHA-256:	5DA618D0D54F9251A1735057B27F9A5188E2DDD44F53CE35CE69CAAF678F26A8
SHA-512:	60678907BD654FF44036ABCB4491056A1A2279B21E6AC933D2423362DC59AB1232C67CD93DDB80BFE80DECC288EB874E333A8B630BF96A0E723BC654C4E35D6
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....w...3f..3f..3f..'.|.9f..'.z.f..'.{.!f..8.{."f..8.|.$f..8.z..f..'.~.0f..3f~.Rf....v.0f.....2f..3f..2f....}.2f..Rich3f.....PE..L...*CCa.....@.....@.....>..(....p.....p..D....3.....x4.....3..@.....<.....text...?..... ..`.rdata...e.....f.....@..@.data.....P.....@....rsrc.....p.....8.....@..@.reloc..D....p.....0.....@..B.....

C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06434adde6c2.exe	
Process:	C:\Users\user\Desktop\912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	5.766022293896966
Encrypted:	false
SSDEEP:	384:iGfNhz85TJAGMwDqHYVdGqviXikCw0lS3JwgLTu3fquwKKyFpjWmouPrM7Gl:nQTGpikCw0WZfMfqunWmouDYGl
MD5:	1AECD083BBEC326D90698A79F73749D7
SHA1:	1EA884D725CAEC27AAC2B3C0BACCFD0C380A414E
SHA-256:	D5CCEBEA40A76EC2C82CAC45CC208A778269E743F1A825EF881533B85D6C1D31
SHA-512:	C1044945B17C8F2063A9B95367DB93AD6D0F6E316AD9C3B32D2A2259459098B72F85F5569B5A33F7DAE68194697C448617E37B6F24558A7AD9CB53B0F382B064
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%

C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06434adde6c2.exe	
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.....p.....Vf.....p.....p.....p.....Vv.....p.....p.....r..... p.....Rich.....PE..L...LsEa.....(...,.....'.....@....@.....@.....L.....x...pE..8.....E..@.....@ ..`.....text...'.....(..... ..`.rdata.....@.....,.....@..@.data...|....`.....B.....@....gfids..p....p.....D.....@..@.rsrc.....F.....@..@ .reloc..x.....L.....@..B.....

C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon066b4a7578e0123e.exe	
Process:	C:\Users\user\Desktop\912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	683520
Entropy (8bit):	7.7483060172666205
Encrypted:	false
SSDEEP:	12288:V3l31go0C7nc6OGiacJH8Gq0Dg89PFbDGmIviXWHkZlSFrbIVPsjGVTlH:Fl3G6OxBljFXGPiXWLr0dPJ
MD5:	E268A668B507C25263CB0B8BB3AEB3BE
SHA1:	E116499E5B99F81580601B780F6018FE5C0A7F65
SHA-256:	82C816980FE9B0DE916FC1954A2E1DB51011770F794F8FD15A2E84656962E6B7
SHA-512:	543654E296D299FEBBBF2DD43E565CF4199B3C7CFFC8DB5FFD490B51C4753D38B080FE72B73E79BBCDB3853227F9198BF6C88A6D230E68A6017D1FBC03C461 4
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....$.....E..w+X.w+X.w+X.%.X.w+X.%.X.w+X.%.X.w+X..PX.w+X.w*X .w+X.%.X.w+X.%.X.w+X.%.X.w+XRich.w+X.....PE..L....j_.....~.....p.....@.....p.....6.....xL..<.....(.....0.....0..... ..... C..@.....text...p..... ..`.rdata..r.....@..@.data.....`.....J.....@....rsrc....(.....*.....@.. @.reloc...:...0...<...2.....@..B.....

C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon067df200a8fd43b.exe	
Process:	C:\Users\user\Desktop\912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	350720
Entropy (8bit):	7.256311123481712
Encrypted:	false
SSDEEP:	6144:rLZQ5cRLLhQ010eWbF/7iGFQYz4odfSC7tc8fDrWyic+E0Ol2WXE8:XZFLLhQ010T57i49MohSCnrtipE0uF0
MD5:	AD56ABB0034DE1257634EA56BE9C8CB6
SHA1:	662AB69A9C24D7037C06889D203A308152B3FEF8
SHA-256:	5540F68B07BB827E21BA5CA68F18033FB9D159381FDAB69D7B8C1970C3981434
SHA-512:	1BA8F2EBD057FC058643C66B6EEAE32EBE100E775ADFBF047F8B21252BD3E969C86703C103F8C372492EDFFDED35084AF9D667C85DA7B2226B88048838E9DB 3
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....$.....l.u(..&(..&(..&6.~&9..&6.h&F..&6.o&...&.o.&-..&(..&...&6.a&).. &6..&)..&6.z&)..&Rich(..&.....PE..L....(._.....h.....@.....`.....pO..<.....8..... .....@.....0F... ....E..@.....text...P..... ..`.rdata.....@..@.data....f...`.....P.....@....tls.....@....rsrc....8.....:..... .....@..@.reloc...7... ...8...".....

C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon067f2fcee827.exe	
Process:	C:\Users\user\Desktop\912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	515512
Entropy (8bit):	7.493026999948429
Encrypted:	false
SSDEEP:	12288:ZQi3giy16m6URA3PhFWKd+J3xNm+CSBJTYKSa8kcWOqsMpg:ZQi1y4hhld+J371xLSXPgg
MD5:	29158D5C6096B12A039400F7AE1EAF0E
SHA1:	940043FA68CC971B0AA74D4E0833130DAD1ABC16
SHA-256:	36CC42294D2CAC9E45FA389F9A7A1DF18CB5AF6F68ED2D5E9563BD522F48BC4A
SHA-512:	366F6F7BC8FF07995A273DC28F77F5D43515C9A079D3E64308228E4EBA12F32BB7945FC898E8EF9AC02A0F58FDC6ED90F82142D43EEC94FE2CF7DA80D7B1AD 8

C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon067f2fcee827.exe

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\Temp\7zS883210E8\Mon06885bbdb13fec3.exe

Process:	C:\Users\user\Desktop\912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	4.679766885087222
Encrypted:	false
SSDEEP:	96:OJOElmu1B9ilJJMOfEkdEKozt1Ex3CfkcqkTzNt:yLkJwGE3ERCL1
MD5:	AE0BB0EF615F4606FBE1F050B6F08CA3
SHA1:	F69B6D6496D8941EF53BCA7C3578AD616CF5A4B1
SHA-256:	03D079303A3164960677E57A587E86C3A5E7736FBDE0AB7B9E60C4B8B2E50745
SHA-512:	EC9AC14AC2EF705867C6C1611671C8185F3D3FE671A787840132A337D4BDF1AD3B808AA3CA24EEE58BDA78BEF19E7A2A9EA5299B224BB370622E5072AA790AD
Malicious:	**true**
Yara Hits:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06885bbdb13fec3.exe, Author: Florian Roth
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...%.Ga.....4... ...@....@.. ....@.....4..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....4.....H.....L$..@.....0.....~.....,(.....,(....~.....,(.....,(....~.....,(.....,(....~.....,(.....,(....~.....,~.... ... .Z(...~....,r...pr...p.(....&r...p(.....(....r...p(.....(.....(...~....&*...0..q..... ....(.....(....t.....r...po.....o....t.....o.....s.....o.....o.....o.....o.....,.o....& ....(.....*.....:.W.....aa. .....0.....(....o....r...p(.....(.....(...-.(!...o".....(

C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0699e256d5dc14.exe

Process:	C:\Users\user\Desktop\912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1421312
Entropy (8bit):	6.45719070398168
Encrypted:	false
SSDEEP:	24576:MmPTV4IoRBi+PzaW9N+whuPPQSDX1kEMjuOkhL42:MCS3Rg+raW9ofQUXmj6K2
MD5:	535AE8DBAA2AB3A37B9AA8B59282A5C0
SHA1:	CB375C45E0F725A8EE85F8CB37826B93D0A3EF94
SHA-256:	D838CFAF7B197D6C3379E2C5DAF269CC422A09DF556DE6CA08FE174B4906B3B6
SHA-512:	6BE6A3D8FA5D1FB17F85BDACF873280A3A074739FB68037DE1A50C63D2D24E5B6B3FFABB838C3097FF9840ED27391A3FB812C802010CA3DB860414C34123867
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Generic_malware, Description: Yara Generic_malware, Source: C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0699e256d5dc14.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....$..`...`...`...t..u...t..m...t.....G.....a.....p.....j.....t..m...`.....h.....y. a.....a...Rich`.....PE..d...>.Fa.....".....L...`.....2.....@.....0.....`.....x.....<.... ..(.....$.....p..... ...@...(.....0.....`..(.....text...,K.....L..... ..`.rdata..n...`.....P.....@..@.data...$.... .....@....pdata..(.... .....@..@_ RDATA.....@..@.rsrc...<.....@..@.reloc...$.....&.....@..B..... .....

C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06be060a7cb426cf.exe

Process:	C:\Users\user\Desktop\912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	16896
Entropy (8bit):	6.186063061179731
Encrypted:	false
SSDEEP:	384:GadRY1nSjkFhH1vHTZj3S6qpA/MrfDWZKTufg9:GkR1AFhH1vTrqpwmfSZfg
MD5:	9B7319450F0633337955342AE97FA060

C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06be060a7cb426cf.exe	
SHA1:	4CC5B5DFC5A4CF357158AEDCAB93CE4CC5BFF350
SHA-256:	C3926CCEF4C9BCE26BD1217EA25E108D92707847E04DDB4E1EADFFF1A913D085
SHA-512:	E75D5E032374EAD6836E37AD8A4E2D59DA7E641AEA178551EE187980455067D90C076AC8E49330B55E1F13591A14305401F3E59520B63ED628A83213220B7FFB
Malicious:	**true**
Yara Hits:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06be060a7cb426cf.exe, Author: Florian Roth
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.....o.....".P..6.....U... ...`....@.. ..... ..@.....T..O....`.....@..... ....H.....text...$5... ...6..... ..`.rsrc.....`.....8.....@..@.rel oc.....@.....@..B.....U.....H.....)...+.....).....*. ....%(....%(....%(....%(....%(....(....*r....%(....%(....%(....(....*..(....*&..(.....*.s..... ....s.....s.....s.....*&.....*&..(%....*".....*Vs....(*...t.....*..(+...*>..r9..p.o.....*R..(%.....s1...}"...*6.(....o?....*..(%...*..0.....~....o.....+..*.0.....~....o.....+..*.0..... ...~....o.....+..*.0.....~....o.....+..*.0.....(....(....+.+.....*...0..

C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06cebe79e9a244.exe	
Process:	C:\Users\user\Desktop\912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	51712
Entropy (8bit):	6.834090443732188
Encrypted:	false
SSDEEP:	768:FSjJeR0GQ8+cIFQpiMitcxZmWqwN5lVucTk4tayPxZrF9ajgE5eZpEEm+:FSjJeK8+cIFQQMitcxh1ERW9+
MD5:	9535F08BD5920F84AC344F8884FE155D
SHA1:	05ACF56D12840558EBC17A138D4390DAD7A96D5A
SHA-256:	BBE7D6E50B7B2229D023AA7170B52D2FA3E63646C6232C25102FA121D1A4534E
SHA-512:	2DAC84FA85149C3C287B70FBD53A1B1AEC2DE5D44099972A988C3F65822CF659E0CE0C758DF009CD39B420EF4B2DB027E8BF3E8966CDC3C18C459421C9E873F
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....o.....".0..t...R..... ...`... ....@.. .....@..... ..@.....,g..O..... .....`..H.....!.B.c}.7... ...8.....@....text....q...`...r...<..... ..`.rsrc..... .....@..@.reloc.....@..B..... ....`.....

C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06d47d8fde50.exe	
Process:	C:\Users\user\Desktop\912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	455168
Entropy (8bit):	3.7291750310747456
Encrypted:	false
SSDEEP:	12288:4klT97iJI2k2Pjho/njNGInARGGy4Tz6f8C2t3hC5Vu4oVIF+/5P1I:fijhq
MD5:	BB4D9EA74D539111AF6B40D6ED4452F8
SHA1:	0E0B2F1AE4655DCD33FB320E84B604859618E1F2
SHA-256:	9156E9DEF914E7EABD23D6EA797D553ADCC3AE0416C9990542CB5D56D6A53E94
SHA-512:	BF8695B227553890ADA8BB65DB9BDF46DE44AF953BAB7A95710272E203AB782DBD263FDBA91074597AB74ECFD882B5F167A94DA794C699F9359A416A5FD3E631
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....\.....0..... ... .@.. .....`..... ..@.....K.... .....@..... ..... ..H.....text..... ..... ..`.rsrc..... .....@..@.rel oc.....@.....@..B.....H.....P6.....0.....~....u....s....z&.....*.....2(.... ....j*....r...p(....*.s....%.}.....s....o... .9....s....z*....(.....*2.s....(....*...v.(.....r]..p~....o....(....*....{....*.0..s.....:...~.....(.....~....:$.....(.....(....(....(.....~....{....~.....o....~....o....(....o....}....*..0.....(.....(.....o.. ..*.6..(....(....*...0..8.....s.....8.....i].a(..

C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06dc62fb7183b9e.exe	
Process:	C:\Users\user\Desktop\912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1575424
Entropy (8bit):	6.29682801876485
Encrypted:	false
SSDEEP:	12288:WldRStsZZzk8/dRStsZZzkldRStsZZzkbgoPYj3YnSn93kEcnVAcx6lQr1Mjg9WL:lCdktCdkiCdkbkjInJmcIlQGjZCmClk
MD5:	F7AD507592D13A7A2243D264906DE671
SHA1:	13E5BFA6CDD1C96B6C9E2170F090E3B260AE95E5

C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06dc62fb7183b9e.exe	
SHA-256:	D5959E437E58709C5E5E7A923EFE7351B28BEDEF15CB00CD9FDB4E5E955B2A13
SHA-512:	3579DB6E38A6F2FF2045FFE4C67399722823F75697A08DD3F7F2F1562BF5D16C733579AAB9970A97E066DDA0BD0F8227CA5F293BC1FBC40311A3870C01D4CDF
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06dc62fb7183b9e.exe, Author: Joe Security
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0.....F.....>.... .....@.. ..... .`.....K.....C.....`..... ....H.....text...D.... ....`.rsrc....C.....D.....@..@.reloc.....`. .....@..B..... .....H.....f...z.....X.....(....*2r7..p(-...&*2rs..p(-...&*2r...p(-...&*N.(....t....&.(/...*F.o0.....3..(/...*2rM..p(-...&*z.,..{....,. {....o1.....(2...*R.....si...(j...&*b.ok....(l...(m....(n...*Z.{....o}...(~...(x...*..(....u.....(....o.....(....u.....(....o/...*>..}.....}....*z,..{....,..{....o1.....(2...*..{4...*"..}4...*..(....*J.{W....(....o....*J. {X....(....o....*..(4...*j.{6....,..{6....o'...oj...*..{A...o.....3..{<..

C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06f9c53ffae25af61.exe	
Process:	C:\Users\user\Desktop\912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	250368
Entropy (8bit):	6.807800081325135
Encrypted:	false
SSDEEP:	6144:ffZQ9MVHPsHqbLeWB9QFCkHk6YzqhH4tcddCI6OJ8:nZLPsHqbLT1kHJEMHs3MJ
MD5:	FC6FCC4C6F1AA7674E7EFB71AE759A42
SHA1:	99D6B80958C6260B06E94413BA229364829BD30B
SHA-256:	CE08913A5BAB71C72527B4AE3C2F83FFA6BEC9A620AECA29BBB7862999E8A84C
SHA-512:	69DEB999E28E24F0B415911EEA4E52B3EB8810F4EC2272CCB4EFB81210BD875F5242590CC2D5BEACC4245853CC64FFBDF9A52F48736E7F88D748299D3C9FB8 5
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l.u(..&(..&(..&6.~&9..&6.h&F..&6.o&...&.o.&-..&(..&...&6.a&).. &6..&)..&6.z&)..&Rich(..&.....PE..L...+..^.....@.....:.....pO..<....P...8.....@..... ....E..@.....text...P..... ..`.rdata.....@..@.data.....`.....P.....@....rsrc....8...P...:..`.....@..@.reloc...6.....8. .....@..B..... .....

C:\Users\user\AppData\Local\Temp\7zS883210E8\libcurl.dll	
Process:	C:\Users\user\Desktop\912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	223232
Entropy (8bit):	7.91725038805347
Encrypted:	false
SSDEEP:	6144:Kk3jgivfCVSRrLV7yAVzKZIjCbanUKWw+ba//PXHUo:30iH0iVPVzKOOunLWf2//0
MD5:	D09BE1F47FD6B827C81A4812B4F7296F
SHA1:	028AE3596C0790E6D7F9F2F3C8E9591527D267F7
SHA-256:	0DE53E7BE51789ADAEC5294346220B20F793E7F8D153A3C110A92D658760697E
SHA-512:	857F44A1383C29208509B8F1164B6438D750D5BB4419ADD7626986333433E67A0D1211EC240CE9472F30A1F32B16C8097ACEBA4B2255641B3D8928F94237F595
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...J4e`....Y.....!.....Dk..... ..... .....-... ...<.....text.....t.....`.P..data.... .....z.....@.`..rdata..... ...F.....@.`./4.....4.....@.0..bss....h.....`..edata.....@.0..idata... .....@.0..CRT.....@.0..tls .....@.0..rsrc.....@.0..reloc...@.....&.....@.0./14.....P.....8.....@.@./29..... ...`.....:.....@.../41.....J..... ..@.../55.....L.....@.../67.....N..

C:\Users\user\AppData\Local\Temp\7zS883210E8\libcurlpp.dll	
Process:	C:\Users\user\Desktop\912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	55808
Entropy (8bit):	6.9891040161841085
Encrypted:	false
SSDEEP:	768:W//WT2mbP+7x4Mx5KzVAn/QqvtdZs8LlR67diTNh4joK7qmQhyOl4UuGoxX9j3D:WHIK1R2VA/Qqvtzz67dbn1QhyOl4UuD
MD5:	E6E578373C2E416289A8DA55F1DC5E8E
SHA1:	B601A229B66EC3D19C2369B36216C6F6EB1C063E
SHA-256:	43E86D650A68F1F91FA2F4375AFF2720E934AA78FA3D33E06363122BF5A9535F
SHA-512:	9DF6A8C418113A77051F6CB02745AD48C521C13CDADB85E0E37F79E29041464C8C7D7BA8C558FDD877035EB8475B6F93E7FC62B38504DDFE696A61480CABAC 9

C:\Users\user\AppData\Local\Temp\7zS883210E8\libcurlpp.dll	
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Gf`....B.....!.....T.....0.....(k.....`.....x..... ....0F.. @..$.....DA.....?.....text.....4.....`.P..data.....:.....@.0..rdata.....<.....@.`./4.....@.....B.....@.0..bss.....`..edata...P... ...H...R.....@.0..idata... ...p.....@.0..CRT.....@.0..tls.....@.0..reloc.....@.0./14.....@.@./29..... .....@.../41.....@.../55.....@.../67.....@.0./80..... .....

C:\Users\user\AppData\Local\Temp\7zS883210E8\libgcc_s_dw2-1.dll	
Process:	C:\Users\user\Desktop\912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	116238
Entropy (8bit):	6.249236557413483
Encrypted:	false
SSDEEP:	3072:nti6N0WeF35Ro7hAWP6cagLSuf6LG3qSbKE4M:ti6N2F33wGJVuHuE
MD5:	9AEC524B616618B0D3D00B27B6F51DA1
SHA1:	64264300801A353DB324D11738FFED876550E1D3
SHA-256:	59A466F77584438FC3ABC0F43EDC0FC99D41851726827A008841F05CFE12DA7E
SHA-512:	0648A26940E8F4AAD73B05AD53E43316DD688E5D55E293CCE88267B2B8744412BE2E0D507DADAD830776BF715BCD819F00F5D1F7AC1C5F1C4F682FB7457A20D0
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....#....^.....p.....n.....0..... .....u..... ..$.....D.....text....\.....^.....`.P`.data....,....p.....b.....@.0..rdata..T..... .....d.....@.`@/4.....4.....4...r.....@.0@.bss.....`..edata..u.....@.0@.idata.....@.0..CRT....,..... ..@.0..tls.....@.0..reloc..$.... .....@.0B.....

C:\Users\user\AppData\Local\Temp\7zS883210E8\libstdc++-6.dll	
Process:	C:\Users\user\Desktop\912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	662528
Entropy (8bit):	7.222450867745387
Encrypted:	false
SSDEEP:	12288:ZGRoW1chMjnv+gvJhb6bmpPSmCnh4o0v4Mc2jTrKoDSwq/3PmkfT4CmwcMcP1uE:uowcmBhKmlC4o0v4k1
MD5:	5E279950775BAAE5FEA04D2CC4526BCC
SHA1:	8AEF1E10031C3629512C43DD8B0B5D9060878453
SHA-256:	97DE47068327BB822B33C7106F9CBB489480901A6749513EF5C31D229DCACA87
SHA-512:	666325E9ED71DA4955058AEA31B91E2E848BE43211E511865F393B7F537C208C6B31C182F7D728C2704E9FC87E7D1BE3F98F5FEE4D34F11C56764E1C599AFD02
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....#.....H.....0.....`.....o.....`..... .....w.. @..$.....DA.....?.....text....P.....B.....`.P..data.... ...`.....F.....@.`..rdata.....  ..>...H.....@.`./4.....`.....@.0..bss.....`..edata.....x...6.....@.0..idata... ...p.....@.0..CRT.....@.0..tls. .....@.0..reloc.....P.....@.0..aspack.. ...0.....`....adata.....P.....@..... .....

C:\Users\user\AppData\Local\Temp\7zS883210E8\libwinpthread-1.dll	
Process:	C:\Users\user\Desktop\912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	70656
Entropy (8bit):	6.292322392729986
Encrypted:	false
SSDEEP:	1536:xPCESXKWzkxTz8uLfdkWr2sUX8YNKykl1wwwwUXrMZE4cYdz:x6baWwxH8EzSHYZE4cYdz
MD5:	1E0D62C34FF2E649EBC5C372065732EE
SHA1:	FCFAA36BA456159B26140A43E80FBD7E9D9AF2DE
SHA-256:	509CB1D1443B623A02562AC760BCED540E327C65157FFA938A22F75E38155723
SHA-512:	3653F8ED8AD3476632F731A3E76C6AAE97898E4BF14F70007C93E53BC443906835BE29F861C4A123DB5B11E0F3DD5013B2B3833469A062060825DF9EE708DC61
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\7zS883210E8\libwinpthread-1.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....,Q.....#.....@.....d..... ..... .,....@.,....p..P.....(.....`.....A..d.....text.....`.P`.data.....@.0..rdata..... .....@.`@.bss.....`..edata..,.... .....@.0@.idata..,....@.....@.0..CRT....0....P.....@.0..tls.... ....`..... .@.0..rsrc...P....p.....@.0..reloc..(.....@.0B..... .....

C:\Users\user\AppData\Local\Temp\7zS883210E8\setup_install.exe	
Process:	C:\Users\user\Desktop\912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2250181
Entropy (8bit):	6.015862062939131
Encrypted:	false
SSDEEP:	24576:iAf0p2YBYPmrXzxhckiv6EI0cCftWrmal3juQ55313N:iA8XRFCf0zl3F
MD5:	74EFCE83CAF33BD4AA9A18A87B48B584
SHA1:	6528A3FA57755871AFD63214446E632CA132E254
SHA-256:	8E5B5A6EEAEE3CED88179EA7775490FDA73B7E21523884653DFBEC2E1DEDF3B8
SHA-512:	B0396ADB80E4C73C180C2AF43559684E82BA3510D19B4B8571359D1DAF969058B920E0E772CA05ED5C0C3E66ACFA1540B4BEF05DAFEF5AFD948476A6F9E7494 5
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....)Ha....aY.....X.....@.....].". ....(.....XY..... .....text...$.....`.P`.data.....@.`..rdata..... .....@.`@/4.....@.0@.bss.....p.....`..idata..(.....H.....@.0..CRT....4.....X.....@.0..tls.....Z.....@.0./14. .....\.....@.@B/29.....^.....@..B/41.....P.....@..B/55.....U...p...V.....@..B/67.....8.....^.....@.0B/80.....`..... ..@..B/91.....8.....d.....@..B/102.....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0mu53gul.jvr.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_yp1iwvjd.lzv.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\Documents\20211204\PowerShell_transcript.494126.SvgNFG3o.20211204232806.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped

C:\Users\user\Documents\20211204\PowerShell_transcript.494126.SvgNFG3o.20211204232806.txt	
Size (bytes):	4791
Entropy (8bit):	5.3955683973547215
Encrypted:	false
SSDEEP:	96:BZRh6N3LyqDo1ZdZvh6N3LyqDo1ZdFl3GZuh6N3LyqDo1ZQo9tZ9:J
MD5:	AFE80CD94D05E73373521EAA61E1D11D
SHA1:	B9FE196636EC187C248D726A5E51321363CB2D57
SHA-256:	DB840B0A68B23C85D18808CC4EF2ADD51F00B18304C3C433E545B584277EFFC2
SHA-512:	484AB58AF0F2E5B627164A9BAA525AA2F96308F56F433EAD2872B448B224E8ECF89725F9C97132EE74772737176D03DE17CF66D34E7FBD5C971D70AD73F22BA
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211204232808..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 494126 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath C:\Users\user\AppData\Local\Temp..Process ID: 6004..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: 20211204232808..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Local\Temp..**********..Windows PowerShell transcript start..Start time: 20211204233108..Username: computer\user..RunAs User: computer\user..Config

C:\Users\user\Documents\Ei8DrAmaYu9K8ghN89CsjOW1.dll	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	data
Category:	dropped
Size (bytes):	1341956
Entropy (8bit):	6.710274489426762
Encrypted:	false
SSDEEP:	12288:CBxvo3SsGknj0YGPQ/fL/rcPt8B7O3FAhlhPZF2vhPZPgu4WKbIgF/QhPQhPZPgA:Cr8Ss10YjnLDcVg4aDtpw2OFNl1vi3
MD5:	5326331C85F3F09526D88E387A7D92E5
SHA1:	BB06C6A2F1C76FDF010BC0728FBCDBB9C1238FA1
SHA-256:	AFADAEE973ECF0272BE793A321C6A065390BF3FDD362D2E2E6D95E4A6B9256B2
SHA-512:	A7653990F06A764F6217C3645969458CC58B4C448D5A2ADF5212882B91DA18D21E4CB4D0F3822175795C3688860EC7C66E0BDBA5B6743DF8234071EB5D5C1D36
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.....<...R...R...R...QT..R...WT/.R...VT..R.....R...WT..R...VT..R...QT..R...ST..R...S.7 .R.V.ZT.R.V....R.....R.V.PT..R.....R.....5:.....}.....]...A.....M.....M.....V.....j..... .....M..).....#.....]..... M.....Y.....}.....W.....].....j.....e..... .....

C:\Users\user\Pictures\Adobe Films\70gT3_jLhoTN69YJz2eMYaZ8.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4300328
Entropy (8bit):	7.947636555384773
Encrypted:	false
SSDEEP:	98304:eoWrbIl3Sui9ZJe7HymaOzunrnjlBolTT14B:1WrWRi9ZJeUOzu9BoR14B
MD5:	ED63206B525F9D1611C20F10B2C4B108
SHA1:	289177CF9CA4AC14B151224E4C56F351BFB42121
SHA-256:	112A712D856CE19F322213A9AC9E6CC8C5A14CE7935C03D5A896C01D9DA45298
SHA-512:	091D180B4F309E0E53A15C4337100BDBFC7517E7794BE8C52FE49A26EBD456762BD183779B3E935C43CC86B7C51591C7F198792B19BD6FE9FF9BE0EB8887A65
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....lb..1..1..1_.1..1..1..1..1..1..1M..1..1..1..1...1..1..1..1..1..1Ric h..1.....PE..L....i.^.....@..`.....P.>.....0@...@.....RAB.....@.(....I.`?.....A.(....@.....>.@..... .....@.....text.....@.....@..... ..`.data...`....0@.....@.....@....rsrc...`?=...I..@....@.....@..@.reloc..._...@...`...6A.....@..B..... ....

C:\Users\user\Pictures\Adobe Films\7ciFxtIpptvH3EmimVuzKQBx.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	275
Entropy (8bit):	5.24627283865109
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3G0CezoIR+kn7gLcXaoD:J0+oxBeRmR9etdzRxGezH0q7gLma+

C:\Users\user\Pictures\Adobe Films\7ciFxtIpptvH3EmimVuzKQBx.exe	
MD5:	978489E2DDB94E1A8F3C4842596BED8B
SHA1:	CCDAA1B6E674D7D7F6E2FE7233239ADD9D62CC75
SHA-256:	222FF59C7DCD2FFE6BBFAA15DDA759C48F5F205DF0B82BCF969FAF845C1F12E2
SHA-512:	A99B30607BF0FD80458374DE3688C7E1AE5FF2CEDE946DA308B13BA5639B0500E69A09E2B8A94BEDB0D59B4B5B031149AFEE6E98C2556254EFFC1A6D8EECE837
Malicious:	false
Reputation:	unknown
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL was not found on this server. .<hr>.<address>Apache/2.4.41 (Ubuntu) Server at 212.193.30.29 Port 80</address>.</body></html>.

C:\Users\user\Pictures\Adobe Films\8L6ugJuHG9eDlcL37667vJc9.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1594416
Entropy (8bit):	6.7258941177685365
Encrypted:	false
SSDEEP:	24576:h9m1ERwuDhMrhn7WiDogqoPFunerUFh9jhzPyv2xR0Le:h9m6RwwhMrhn7WiDogqoMlLcLe
MD5:	8DDA6713AEDC164717847F0E9FD76942
SHA1:	122F819D360410516222812F12ABE0A0C1E4F779
SHA-256:	AC03D6B781F85BADCC6CE2B0565C66601BEA9BD53A5977878BAE600E79494FB8
SHA-512:	D620766FCE49F50A3858FCBCE32E59FDEA0BF452437FC59C3E39398E2579D2C94C28130BE4C754207B7CCC5368884ADA4F37C4077F1DC0974276AAE337DF888
Malicious:	false
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(..LY(.`...x.;.^U....,6A...5K/.#..DS.....Q..... .PE..L...'X..... .....@.....P.....~.....@..... .....0...t..... .....`..... .....@....rsrc....t...0...t.....@..@.....|.....@..... .....z/.AQ.....=...3..|....N}..

C:\Users\user\Pictures\Adobe Films\B9sunPpJzOhhqi2LNmnFA1Vf.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	421376
Entropy (8bit):	7.113053483334034
Encrypted:	false
SSDEEP:	6144:BqztsmVs7Z1tyFvD1EFBEmHvKzjVQAARnB8cmP6UlFwK+eBvfxg4S1:BqB5sZSD1EF2WvKQR8cc6gFwAJg4S
MD5:	6F9E546026262180D94EB594EAB11705
SHA1:	34C797AFD80531BD114C86759078AAC8073E8562
SHA-256:	1A88073C331184DF09635FA1A9A73A67C064EE49F57D896F304347D6357A14C4
SHA-512:	B60BBB8474A99EE98E388501D4BEAABEC407AFF4EBFCD305E38F9583CE63D51995D089B22ED8DF2E3A39082528FACBD76F4DA0A94742DB232FCB40516848A5F8
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e.hD!...!..!...?...;...?.....?.....n}.&...!.....?... ...?... ...?... ...Rich!..... .....PE..L....._.....d...Z.....=7.....@.....P.....@.....@..... .....text....b.....d..... ..`.rdata..\l.....J...h.....@..@.data.....@....rsrc...@.....V.....@..@..... .....

C:\Users\user\Pictures\Adobe Films\BFuUkLJxjHnJ56WPRhHz3ign.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	275
Entropy (8bit):	5.24627283865109
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3G0CezoIR+kn7gLcXaoD:J0+oxBeRmR9etdzRxGezH0q7gLma+
MD5:	978489E2DDB94E1A8F3C4842596BED8B
SHA1:	CCDAA1B6E674D7D7F6E2FE7233239ADD9D62CC75
SHA-256:	222FF59C7DCD2FFE6BBFAA15DDA759C48F5F205DF0B82BCF969FAF845C1F12E2
SHA-512:	A99B30607BF0FD80458374DE3688C7E1AE5FF2CEDE946DA308B13BA5639B0500E69A09E2B8A94BEDB0D59B4B5B031149AFEE6E98C2556254EFFC1A6D8EECE837
Malicious:	false
Reputation:	unknown

C:\Users\user\Pictures\Adobe Films\BFuUkLJxjHnJ56WPRhHz3ign.exe	
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL was not found on this server. .<hr>.<address>Apache/2.4.41 (Ubuntu) Server at 212.193.30.29 Port 80</address>.</body></html>.

C:\Users\user\Pictures\Adobe Films\EH2UqXkmGsdM7d8RuuDQ7km6.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1578224
Entropy (8bit):	**7.9928378769172745**
Encrypted:	**true**
SSDEEP:	24576:clGlNx98yVwfEKNH65IBL6ms0vkfEOFGXymBrcAKUkLkAtFmYACmkEaHNYK3CcNc:vJ+a3G652m/08MOaxcHUkLkAOImNa81
MD5:	0B56264E088E314A09B492F32C114BED
SHA1:	1A09102B8BE902645A050D07E0C800E03D069D5C
SHA-256:	0BB8BE09C9E61B14EE083456E19769D7B778C6D974C2F0DCAD721D6111E5F2E6
SHA-512:	88D9A45FAACF4071956865D63B5F052F7DF9142BC2D1EEE8FF9DEE16C0F930D2C4B745781968D15073DA79D9C6A7DDB41568DFAAAA8DA22FBFEE4A29B0E56B8
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...<.b.....0..... ... .@.. .....<.. ..u.6. .....|.7.....`..z..... .....@..... .....@..... ..... .....@.....@.....@..... ...@.....@....rsrc... ...`.....@..... 5.....@....YrFQrLs.....7.....d.....@....adata... ...` <.....@..... .....

C:\Users\user\Pictures\Adobe Films\G2_EIY9DOQs4sNlH3UBGIHNs.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1791712
Entropy (8bit):	**7.994286100518312**
Encrypted:	**true**
SSDEEP:	49152:ud3+YjGSkgxjmxnCe06IUkfLkoNauU6NV4+:uUYjGWcCeUZowpK+
MD5:	5525DB91A602F578DE98EB9AF0B767D2
SHA1:	0F5EF84853E2EDC7F1399852051D04855AF1ADD0
SHA-256:	D7AE0785ECBECB35BC33FD7B50687037F439AAFC2EAA436C220A14EDC41D8F12
SHA-512:	5B4218D8A9B88A4EDA6841C1A3FFAB5A13D000CC6741F6C41E1C2D411CE04CD330FD8B12713BAA9490B42D30C4920A2974AD684E794130C550AA666B88A43F8B
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...ig.....0..... ... .@.. .....?.. ....9. .....|.:.....`..... .....@..... .....@..... ..... .....@.....@.....@..... ...@.....@....rsrc... ...`.....@.....@8.....@....rz7RpXi.....:.....@....adata... .... ?.....N.....@..... .....

C:\Users\user\Pictures\Adobe Films\Kjf6fop4TDCFGr6Z3sfik8Kr.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	754176
Entropy (8bit):	7.6268048303431595
Encrypted:	false
SSDEEP:	12288:vE9QeBQNnbQZdxcBRQHLdcgoE0wuwmUI+V/SXaQqzYZsery5gWYgEMuNv:vElBQNnbiznLosI+4XaQ7CzVYbp
MD5:	2723D98B26317C5D99B2087D4FB1849B
SHA1:	5CFD6394A62D276CF27ADD924A4BDB7D6AE2F851
SHA-256:	36AB109DF90DF5825124E0AB7118D23D82DC32942D8A4CF37AA5C183C061B10B
SHA-512:	0F022351A1546E73932DCD504B328BD43FF6FEA8A5650D4156C11227E33D30A20DB703D19F5D1731579617AB327F779EA3CB8484FE80F2CC6A15BB22A6803034
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e.kD!...!...!...?...;...?.....?.....n~.&...!.....?... ...?... ...?... ...Rich!.....PE..L...._.....x...^.....=7.....@.....b].....P.....@.....@..... .....text...-v.....x..... ..`.rdata..4I.....J...|.....@..@.data.....@....rsrc...@.....j.....@..@..... ....

C:\Users\user\Pictures\Adobe Films\Km91VWEL8QlQMf6PXBcS7CUg.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1650160
Entropy (8bit):	6.835466888014812
Encrypted:	false
SSDEEP:	24576:o9m1ERwuDhMrhn7WiDogqoPrZNUDI2A3rHik117wmZS4:o9m6RwwhMrhn7WiDogqozp3rHik11zV
MD5:	294C381E6D73739319D5162013F72162
SHA1:	06A8C8EC3C016BC9C381CF5F3B2FF4F1F048EE02
SHA-256:	45BD65B7EC522C1E8AEC332D7C29DF30036709FF7EB3D69E013D97DAD7C6C3DE
SHA-512:	9B06C050E1B6988F2DA0234E42F92B5B9EBFD5614D5E49ADC07E9EDA7E0E5A8D0CCE40914B1441AD31A8738AC977DCEDF03550385F638C2FEEDD60B19312FF 10
Malicious:	false
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(..LY(.`...x.;.^U....,6A...5K/.#..DS.....Q..... .PE..L.....h..... .....@..... ..... .....<#....@..... ..... .....0..<M..... .....`..... .....@....rsrc...<M...0..<M.....@..@.....T.....@..... .....O\..d.@.bOS...I.....L.eR.C.

C:\Users\user\Pictures\Adobe Films\MMMy7Y8hjR6Y29cpH6i8H_U7.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	675840
Entropy (8bit):	7.606676906121715
Encrypted:	false
SSDEEP:	12288:O7VvDGQGh+/E/4Im+1Pj6o3QJamyiwpBwfJJgCJbxVeJMakn+SfyQE:OhvDGQGh+/EBPj6oqPyxpSvlTINkn+7
MD5:	45CF4EA0F9268E7306DA20DEA9D14210
SHA1:	3574746D1D089F9989EE2C9E2048F014A61100CA
SHA-256:	919CCC1F90BAE8D58CC6EF51359E15AF853DE90A7083C640B5C2A99EB1A61281
SHA-512:	3996F207A4973428F7ECB419F16FDAFB7FA6213CB0A9A7B48405BAAE10F85A4A381664291F4C59D5C6BC7158335CA07944FB712DC7DC14A3A393F9AF490DFE6
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....A.k...k...k...9z..k...9l..k...9k..k.....k...k..ck...9e..k...9{..k...9~..k..Ric h.k.....PE..L.....n`.....F...\.....4.....`....@.....Dl.....P.....@.....@.....`..... .....text....E.....F..... ..`.rdata...H..`...J...J.....@..@.data.....@....rsrc...@.....8.....@..@..... .....

C:\Users\user\Pictures\Adobe Films\MVqkmKxpMmLZNmFpGwUpdGg4.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	420864
Entropy (8bit):	7.108935296953452
Encrypted:	false
SSDEEP:	6144:+oztsDVs7Z1tyFvDDQCysshSzXOMlS6JmLcA2LE9B+0hOKzZo4A1:+oBAsZSDDQCyssQX+6QL3T9B+rK24A
MD5:	E59FE8EBCC566952658B3D0AFC3AFCB1
SHA1:	66A2A99F16B66F67492FF8AD3C9895B283988F76
SHA-256:	79B245557B3B30E1D7DF10D212F6BC8EAA7134FB99BE5B1C7E93B9A61D080AD8
SHA-512:	34173D80AE89EE825E25D7CB326E3131CA07749C9324865740949BD235484D4A49C45A8B8E72A1E20ACAF1076F38854F0B1A7CE0936807ACFA3CBA477E203E25
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e.hD!...!...!...?...;...?.....?.....n}.&...!.....?... ...?... ...?... ...Rich!..... .....PE..L...0uG`.....b...Z.....=7.....@.....O.....P.....@.....@..... .....text....`.....b..... ..`.rdata..\l.....J...f.....@..@.data.....@....rsrc...@.....T.....@..@..... .....

C:\Users\user\Pictures\Adobe Films\NikB4LocWiKFuKasNcrhRDqo.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	1616624
Entropy (8bit):	6.596891349625164
Encrypted:	false

C:\Users\user\Pictures\Adobe Films\NikB4LocWiKFuKasNcrhRDqo.exe

SSDEEP:	24576:62WuJrCAfYGN7gsWkyH+Kpy1njJgVxy7i:623JOAfYGRikFPt8
MD5:	64F650349CFBE25B805DA784A4ECCB7C
SHA1:	0EC1F6FA84AEADD43368E30132F70CD6F4B95B06
SHA-256:	CB863AC7D9B78CC71825CFF93EAEFC18D5574EFCE160505AAA0D6A63730C99F6
SHA-512:	488BEE67C577A7A53CE8F14E20C79350C40A9822209EC9AEE763F21FC8D9E3773D541E3387C92F20DF33EB32DBE89BEC07FE85DDDCDB7D1772C882FED45F9F C7
Malicious:	false
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(.W...1....&ci!..N...T..5...l....qd.....b.....Q..... .....PE..L.....o..... ....@..... .....@..... ....0..,..... ..... `..... .....@....rsrc...,....0..,.....@..@...../y.....@..... .....5@d.....4...z.W..jey....

C:\Users\user\Pictures\Adobe Films\OWtr97fJ3mDnO4VToTTzkR9p.exe

Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	396800
Entropy (8bit):	7.027534750128602
Encrypted:	false
SSDEEP:	6144:xmTNLmVs7XZj0vjGgc+MtFEQ5R6h6qBFLiwJCuqV:xmBLmMXZSjrcVtHqBYq
MD5:	C2995AAAE4BBFFC3E883D36E10AC3C16
SHA1:	43E97FA4520E62133000174D9DF74B4C728A3C29
SHA-256:	725AD6618F1043A925591A5F93ED2F78C51CD7440007E80BFDC3F9072285392D
SHA-512:	7EF96772F79CA068F6486A803C426D8C1371A5C3C760F4A2126F41254B4F35A162E52A07915775E22232BDE8B897967C538B9319640BCEE1AC2DC1B94039A802
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e.hD!...!...!...?...;...?.....?.....n}.&...!.....?... ...?... ...?... ...Rich!..... .....PE..L...X._.....Z.....=7..... ....@.....M.....]..P....`..@.....K..@..... ..... .....text..... ..`.rdata..\l... ...J.....@..@.data.....p.....R.....@....rsrc...@....`.....@..@..... .....

C:\Users\user\Pictures\Adobe Films\Rd4mWWpY8ZOYLzPUXbMr48g7.exe

Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1655576
Entropy (8bit):	6.671392068379385
Encrypted:	false
SSDEEP:	24576:E9m1ERwuDhMrhn7WiDogqoPWmw646lQmlaI+wbL1pV1:E9m6RwwhMrhn7WiDogqowb0aNyLPb
MD5:	4DF0D4BE3B3ABB5CA237D11013411885
SHA1:	7B9376E633769EB52A70EC887143826F924F6FEE
SHA-256:	2CF6A392704EB1EDE9545577028283A714D4ABD1B53318CA11B3075DEE799813
SHA-512:	14E1543C4F8A5C331EF1DE493C7AAF8E2ADE61B6A4CC9E15E2E3CE988BE4CD5C72A2558C78E39EBE8F71DE592945192DF7CB2093CE71D62D5A417F5CF6858 B7
Malicious:	false
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(..LY(.`...x.;.^U....,6A...5K/.#..DS.....Q..... .PE..L..... .....@.....P.....I....@..... .....0...}.....*..... ..... `..... .....@....rsrc....}...0...}.....@..@.....@..... .....k..@-f..7r...>.....&..r\%..

C:\Users\user\Pictures\Adobe Films\SSceGixduBzhWNhNwAlLoQH9.exe

Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	766721
Entropy (8bit):	6.100484546820966
Encrypted:	false
SSDEEP:	6144:d/QiQXCi5m+ksmpk3U9j0ltjuwsoxvjFEOTb9WmZX/8shzdsY4CpHPhn+UBE:VQi3ic6m6UR0lt6wp1hf39Wkv8xwJ3E
MD5:	BCB9F3E57C6CA459DD8408A7D7EF6C9E
SHA1:	6ADCDD9DFE71929F266C87D4713138AE3A8224DC
SHA-256:	9E987CF65077DE7825606813039AF92F72B685950CC2A055C5FD8EC676FF1EEB
SHA-512:	C61BED55533DA8766EC532D6AF10766C4460780F6E0E63A0E34BF1E9BF401793068F067B8E168AEF3261AC6029D7C3441149800997802265 1CB29B724DF91155

C:\Users\user\Pictures\Adobe Films\SSceGixduBzhWNhNwAlLoQH9.exe	
Malicious:	false
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\Pictures\Adobe Films\So_nQ0f6036W5A_oTVjjj7ec.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1515520
Entropy (8bit):	6.6504077407296345
Encrypted:	false
SSDEEP:	24576:qEpfLmZkUtN/Wy+jtYkQkbF7vZjHYdG/9QDkMhJgXgaFJAIQiFX:bpylrKY2m4+7/gXgaFJT9FX
MD5:	F41CF108FA69603EAC9C6876E15DF7F4
SHA1:	1769AD4196D67936025E7CA2EBD73EB5475ED559
SHA-256:	0BE56CF2F98C19535B17E425094EBC300AB4FD020DDC82A7B955126ACFC59D4A
SHA-512:	A1FF7A27334F8FBE00324E52CBDAD702264494E1BECEB12587708A65740391B97AE5E56FE44A2915A76050D062C464C81AC970A9111388E3F19391CF32F6D68F
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Socelars, Description: Yara detected Socelars, Source: C:\Users\user\Pictures\Adobe Films\So_nQ0f6036W5A_oTVjjj7ec.exe, Author: Joe Security
Reputation:	unknown
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....@.....-.....+.w.....+.....*.....-.....&.....*.....(...../...../.7.... .*.....+.....,.....Rich.....PE..L.....a.....z.....S].....@.....@.....|4.....6..... ..`.....8..... ...@.....H...@.....text..... ..... ..`.yukiess.X...0...Z...$..... ..`.rdata..:.....~.....@..@.data....w...P.....6.....@.... yukiessP.....d.....@....rsrc....6.....8...f.....@..@.reloc..`.... .....@..B..... .....

C:\Users\user\Pictures\Adobe Films\TITkxzS0gfvs2KvVCeBpa4X_.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1271300
Entropy (8bit):	7.87640376820829
Encrypted:	false
SSDEEP:	24576:zry2uXzmwLNSKlimkMoCD0DnNZFx4jnnEI9j7YLWsoqncRfW3SuQSOIdaKrj75dJ:zunjww6nPFGjn/2hmfW31TTaKrF
MD5:	EC9337A368174E058F2CDD041D083531
SHA1:	759C4153BDF2A97827703F6AC85C18DE2FFE60F0
SHA-256:	6D0DE728692D6F7FF7BB93CDC93B716155DB4EB3AB8514F33BF817B6A2DBE23E
SHA-512:	594B6861D063C59EBC6CC016ABEC9ED818D374CE3FA49F8B7A765295CC033097D5EB1762CE52FA7464F3D0DEC33F6E8356C012FC147A95C9C472D4F94FF37E 8
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....}.o...o...o..#.a..o..#.c..o..#.b..o....W..o...1./.o...1./.o...1./.o.....o.... ...o...o..mo...1./.o...1./.o...1o..o...1./.o..Rich.o.....PE..L....`.....f.....A.....@.....@.....4.....<.....`..,(.. . ..T.....H...@..... .....text...zd.....f..... ..`.rdata..4.....j.....@..@.data....M.. .....@....didat..`....p.....@....r src.....@..@.reloc..,(..`...*.....@..B..... .....

C:\Users\user\Pictures\Adobe Films\Tm0qqnTEi1cYOqiY563QdqH0.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	275
Entropy (8bit):	5.24627283865109
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3G0CezoIR+kn7gLcXaoD:J0+oxBeRmR9etdzRxGezH0q7gLma+
MD5:	978489E2DDB94E1A8F3C4842596BED8B
SHA1:	CCDAA1B6E674D7D7F6E2FE7233239ADD9D62CC75
SHA-256:	222FF59C7DCD2FFE6BBFAA15DDA759C48F5F205DF0B82BCF969FAF845C1F12E2
SHA-512:	A99B30607BF0FD80458374DE3688C7E1AE5FF2CEDE946DA308B13BA5639B0500E69A09E2B8A94BEDB0D59B4B5B031149AFEE6E98C2556254EFFC1A6D8EECE8 37
Malicious:	false
Reputation:	unknown

C:\Users\user\Pictures\Adobe Films\Tm0qqnTEi1cYOqiY563QdqH0.exe	
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL was not found on this server. .<hr>.<address>Apache/2.4.41 (Ubuntu) Server at 212.193.30.29 Port 80</address>.</body></html>.

C:\Users\user\Pictures\Adobe Films\VkFchiXGaREjCGp6k2Ktr5lS.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1896234
Entropy (8bit):	7.921840655641192
Encrypted:	false
SSDEEP:	49152:7847rx6xgJW+GUy10f8rx3Su0H+fVLFZAKVS7eF1Hm6:7NAyJW+ny10f8rx3SupfVLFZdsQf
MD5:	C02926A3207BC28691D4FD6CED55D036
SHA1:	ABD050B7474651627E2FFF413E0DB8DCD1F27943
SHA-256:	239CA58590920FEF69005486D9B95FB7C556EA080EA2E349A360A869D8ADDB3F
SHA-512:	266DBDC406805E4773C34CE81412868E92832B1C9B8073F4226D2650154E377C068A385B64F501DCF3A51B329A8347AD75C4A681E7BC1D080D3006D11B5A6E72
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b`..&...&...&.....h.+....j.....k.>....^.$...._..0..._..5..._...../y.../y ..#...&...+..._....._..'..._f.'..._..'...Rich&.....PE..L...).`.....0....@.....@.....@.....0...4...d...<....0..p.....|".....T..... .....U..@.....0..`..... .....text..... ..`.rdata..".....0.....@..@.data...(7.....@....didat..... .....@....rsrc..... ..0.....@..@.reloc..|".....$.....@..B.....

C:\Users\user\Pictures\Adobe Films\XgI7PQbAfdnaXrmuKlSbD1tN.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	275
Entropy (8bit):	5.24627283865109
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3G0CezoIR+kn7gLcXaoD:J0+oxBeRmR9etdzRxGezH0q7gLma+
MD5:	978489E2DDB94E1A8F3C4842596BED8B
SHA1:	CCDAA1B6E674D7D7F6E2FE7233239ADD9D62CC75
SHA-256:	222FF59C7DCD2FFE6BBFAA15DDA759C48F5F205DF0B82BCF969FAF845C1F12E2
SHA-512:	A99B30607BF0FD80458374DE3688C7E1AE5FF2CEDE946DA308B13BA5639B0500E69A09E2B8A94BEDB0D59B4B5B031149AFEE6E98C2556254EFFC1A6D8EECE837
Malicious:	false
Reputation:	unknown
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL was not found on this server. .<hr>.<address>Apache/2.4.41 (Ubuntu) Server at 212.193.30.29 Port 80</address>.</body></html>.

C:\Users\user\Pictures\Adobe Films\Z_vRblvz9Nut3_fUjgc3y2tG.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1584992
Entropy (8bit):	6.670729345513266
Encrypted:	false
SSDEEP:	24576:/9m1ERwuDhMrhn7WiDogqoP7lq1SHgy5UN/47N:/9m6RwwhMrhn7WiDogqo5+SHeBm
MD5:	85E45F70FC0FF31D729D9235638D6114
SHA1:	4B66770469E9D44CD1E91D03887353F692543399
SHA-256:	07A8734B91F962531D72CA2BBC884460BC4C69262CCED40C1F6026EB6E98BF64
SHA-512:	5CBE7EEB59E4AADC674E86E660F8363469B51555F0BBC7F6B33DECAA021179F6EEB0F5012EF3A9A70A15BE8CE0C96124CADE25FF61756D0D2FC96663DFA2BF7D
Malicious:	false
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(..LY(.`...x.;.^U....,6A...5K/.#..DS.....Q..... .PE..L...i.....n..... .....@.....0.....6.....@..... .....0...Q..... .....`..... .....@....rsrc....Q...0...Q.....@..@.....|....X.....@..... .....y.E....u...s.ON.....*...+%.

C:\Users\user\Pictures\Adobe Films\Zq6kcg5lJKuuEaFuudf7gjaI.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	HTML document, ASCII text
Category:	dropped

C:\Users\user\Pictures\Adobe Films\Zq6kcg5lJKuuEaFuudf7gjal.exe	
Size (bytes):	186
Entropy (8bit):	4.391224151129538
Encrypted:	false
SSDEEP:	3:qVv/ZSGcv1Dm00qRXAEtvpL//PhroEsMygWGRHE+L6dNxQKXBcwUKHJNVLFgac4O:qF/sGcg00qRXAEdpJoEslT5xcwRpHLmz
MD5:	2E4EF016A899AF5598F8BAACD5EA3F9D
SHA1:	C2F5C217D38F963904B1FEB25A2D010DC4CD1EC4
SHA-256:	C2DC37E4767C439DE923DEEEDFF5241D48B99A6916BFB4F9D3BC7084DAA20BEE
SHA-512:	C4483B76D1011488EA2B7E016E8CCBFF62AD92899485F69BBDBCC9B7A19184645C47856AB9A1A26CADBB7D4258EF9E5E48BE3332841247D99D0F9E2EA867B9 0
Malicious:	false
Reputation:	unknown
Preview:	<html>. <head>. <title>offline</title>. </head>. <body>. Deze website is tijdelijk niet beschikbaar. . This website is temporarely unavailable. . </body>.</html>

C:\Users\user\Pictures\Adobe Films_I840nW0W0BkPi0VRC8fXhgb.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	4323
Entropy (8bit):	4.966457667673525
Encrypted:	false
SSDEEP:	96:1j9jwIjYjyDK/DZD8jH+k16cvJADh/pRs5sXszbGD:1j9jhjYjWK/lyH+k6cRADh/pm5sXsfGD
MD5:	1F04720AF4B12E3300187B4031260214
SHA1:	1B54FC1A51CD128580EB0E0D7EB3DABA5EBA4832
SHA-256:	FA55E173B327E08882519D28EE60482B7C81EE6FDB1F5A9E358629D69C0E80E3
SHA-512:	86FF0B926A1F5DD2C767459FEDCBF086B9C4D594B4AB66A64E873EEA111C01F773F92E7DC09EC4B4C13ADA0F376734BC74D5CABFF4C43CCC7E01CBA3A62C D19
Malicious:	false
Reputation:	unknown
Preview:	<!DOCTYPE html>. [if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->. [if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->. [if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->. [if gt IE 8]> > <html class="no-js" lang="en-US"> <![endif]-->.<head>.<title>Suspected phishing site | Cloudfl are</title>.<meta charset="UTF-8" />.<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />.<meta http-equiv="X-UA-Compatible" content="IE=Edge,c hrome=1" />.<meta name="robots" content="noindex, nofollow" />.<meta name="viewport" content="width=device-width,initial-scale=1" />.<link rel="stylesheet" id=" cf_styles-css" href="/cdn-cgi/styles/cf.errors.css" type="text/css" media="screen,projection" />. [if lt IE 9]><link rel="stylesheet" id='cf_styles-ie-css' href="/cdn-cgi/styles/c f.errors.ie.css" type="text/css" media="screen,projection" /><![endif]-->.<style type="text/css">body{margin:0;padding:0}</style>...

C:\Users\user\Pictures\Adobe Films\bClhmhZlpCeoCXI8ug2wg8mi.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1584992
Entropy (8bit):	6.670729345513266
Encrypted:	false
SSDEEP:	24576:/9m1ERwuDhMrhn7WiDogqoP7lq1SHgy5UN/47N:/9m6RwwhMrhn7WiDogqo5+SHeBm
MD5:	85E45F70FC0FF31D729D9235638D6114
SHA1:	4B66770469E9D44CD1E91D03887353F692543399
SHA-256:	07A8734B91F962531D72CA2BBC884460BC4C69262CCED40C1F6026EB6E98BF64
SHA-512:	5CBE7EEB59E4AADC674E86E660F8363469B51555F0BBC7F6B33DECAA021179F6EEB0F5012EF3A9A70A15BE8CE0C96124CADE25FF61756D0D2FC96663DFA2B 7D
Malicious:	false
Reputation:	unknown
Preview:	MZ.....o...g.'.:.(..LY(.`...x.;.^U....,6A...5K/.#..DS.....Q..... .PE..L...i.....n..... .....@.....0.....6.....@..... .....0...Q..... .....`..... .....@....rsrc....Q...0...Q.....@..@.....|....X.....@..... .....y.E....u...s.ON.....*...+%.

C:\Users\user\Pictures\Adobe Films\biQtzmlvUuePquCyc26WOk81.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	29676504
Entropy (8bit):	**7.99622998723258**
Encrypted:	**true**
SSDEEP:	786432:kPLBBBAarluFO0Y2LiZsBlQ04FN4Tn4EGK:uXAjAvwiZsBlPTnhT
MD5:	BF7E997F53E2FC3BD8D0E6E5E8782FA2

C:\Users\user\Pictures\Adobe Films\biQtzmIvUuePquCyc26WOk81.exe	
SHA1:	7497EBAA4D19912B838372430DE65D671054F5E5
SHA-256:	C2B27A37E47861DE9994783D85F661162C9E9B4EAA450348748639BF1E7DC99F
SHA-512:	DD65F41420D3DBB7F0F460DA35B235E950D750C8FDD76DD63BD21E16257D3EE7FBEB0B9EBF28BD1F4E466C749A88C3AB71348CAA9F7BA92B64B43518F10339BF
Malicious:	false
Reputation:	unknown
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...I.m^.....`.....n.....@.....0.....50....@.....@.....P.....0..... ....*.....p..... ...2..@....@.....text...HF.....H..... ..`.itext..h....`.....L..... ..`.data....7.....8...d.....@....bss....xg.....idata.....0..... @....didata.....@.....@....edata.....P.....@..@.tls.....`.....rdata..]....p.....@..@.rsrc.....@..@..... .....@..@.....

C:\Users\user\Pictures\Adobe Films\ekfeDHeefrpVeOLF_zEospRe.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1623256
Entropy (8bit):	**7.99347389624365**
Encrypted:	**true**
SSDEEP:	24576:1oDwgVcoQE40zzcsLr9KccgEWPW4rIFUAuy2eiAdmMUq6IK+JOkEaHNYK3/E+ZUX:1ocgV5vnYqRigJO46LaRq6FNa5zS
MD5:	089B918ECB3EF4E737F1F299C92B55A9
SHA1:	8B588524FEA66B318344B490A5F388B0B81EC582
SHA-256:	1E2E3CF9DFA80E5BB025559C3E6F5F9DE3771A59646EAB24D8C1B8F1874DB587
SHA-512:	867487088652FEB6972E7D1D560958E76620135C065C28A2D994833714738449AAE78C9D2EC089863E2D34C4E9CFB2AE09998794CA63AE4AF10C0CC2FD9BA6FE
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...8S.a.....0..P..... ... .@.. .....@>.. ...]7.....|l9..... ....`... ...\.....@..... .....`.....@..... .....d.....@.....@.....f.....@..... .....l.....@....rsrc... ... .n.....@..... 5..@.....t.....@....qVDOdje.....`9.....@....ada ta... ... >.....@..... .....

C:\Users\user\Pictures\Adobe Films\eyCAN_PVePYm1Gl5JhE7GSOh.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	278528
Entropy (8bit):	6.35166785962771
Encrypted:	false
SSDEEP:	3072:7yTB8F8fejmNpVsYWJZYIDx9pJi8dKgMXUaFv1gnwaj03AHYegQMwu56Tv6X:21JfBVMsIVN67v17a4D4MaTSX
MD5:	F118C5D35478B3F97A4EA01DE61E4C85
SHA1:	7D31DFDE5DCECD20396EC1FD0D061BC63ECCD23C
SHA-256:	78BCB8651339AB0460A3C5D5DC8CC726B68B382A0F8D7DF60215C99BDF102C49
SHA-512:	0CC102D31C12491C52D74FC63CD3CA52DEF262DC5A3CE6BBEE46E3EC4525AAE7996D16B70792ACDAC9E20A2126813B3BBDA40AC57D3C9B222E4556624DB9B2C
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e.hD!...!..!...?...;..?.....?.....n}.&...!.....?... ...?... ...?... ...Rich!..... .....PE..L...n._.....6....X.....=7.....P....@.....uo.....P.....@.....P..... .....text...]5.....6..... ..`.rdata..\I...P...J...:.....@..@.data.....@....rsrc...@.....(.....@..@..... ....

C:\Users\user\Pictures\Adobe Films\g_MknxqsfTsoo1ZWGLulW9rc.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	419840
Entropy (8bit):	6.639390634578847
Encrypted:	false
SSDEEP:	6144:lPfqWOl5+qUoFFcZYHavq4+5cyhty0DITESqUbO9hLIBxvbXC10A:lXqSqUoTcG6tScyhty0DITJqUbxvb5A
MD5:	5745C83C4352A4BC0783814F19532004
SHA1:	F7F287C50EABB014D73D418947325B620585EE70
SHA-256:	2AD18ED0044EB8ED610F6E966BEE363DC7A3650F380188D9CBC0F71B00CAEF1B
SHA-512:	6BCE3C561B2058B524C1ED470C00DF8A6E74C0B87B1C6DDB9BFFAFB466ADBF0F6423C4C6A49671CBB0810467CABF30D127E7A72FBCEACF8381016510377D4B89

C:\Users\user\Pictures\Adobe Films\g_MknxqsfTsoo1ZWGLulW9rc.exe	
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....[...5..5..5.$....5.....5.....5....6.5.....5..4.W.5.....5.....5.....5.Rich..5..... .....PE..L...5._.....:.....P..... ....@.....p.....6.....\...(.....=.....0.....H.....@.....`..... .....text..... ..`.data...`.... .....@....tls.....@....rsrc....=.....>.....@..@.reloc...:...0...<...,.....@..B..... ....

C:\Users\user\Pictures\Adobe Films\hl_J5ttTbMmf2AhgPYwvzG__.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.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:	false
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\Pictures\Adobe Films\i4HzLCX9ix_xgRHB3fQN7Sf0.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1407488
Entropy (8bit):	6.463710025379365
Encrypted:	false
SSDEEP:	24576:QH+9mwfaxNwTnfWKZrAZ/LD47RHQ9WFqc804cYq4IVJt:QH+9mBLwbfWirA5LsQ9W402YVJ
MD5:	90E040AD0BC66EF17D109D03218040D6
SHA1:	D70ECC79996CE88FDB1DEA83A012C586F2E8BC9A
SHA-256:	EF1A6DE96A75C8541E856D1811CD41E19EC65FF98D7ECA00DAF73615AE6C790C
SHA-512:	C0FB44FE1B4771599FB641DD3F11EFE776C2C2B767A14E5943B964FF594DE619B242EC3DEA63B4CF9597491ECCDCBCBCDA6D4117DE6BEE5344B3FE8685608E4
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Generic_malware, Description: Yara Generic_malware, Source: C:\Users\user\Pictures\Adobe Films\i4HzLCX9ix_xgRHB3fQN7Sf0.exe, Author: Joe Security
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0...^...^...^...Z...^...]...^...[.Q.^.Q.[...^.Q.]...^..Z...^..]...^..[..^..._... ^..._.'.^.\.W...^.\.....^.\.\...^.Rich..^.....PE..d.....a....."......@...6.....4".....@.....`.....x.....8..... ...J..p.....L..(...0K..8.....P..0.....text....?.....@..... ..`.rdata..`....P.....D.....@..@.data...d.....@....pdata..... ....@..@_RDATA.....R.....@..@.rsrc...8.....T.....@..@.reloc... ....."...X.....@..B..... .....

C:\Users\user\Pictures\Adobe Films\i9v9KeSPU8TebYFmPJaLjDAO.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	227
Entropy (8bit):	4.965512331813944
Encrypted:	false
SSDEEP:	6:qzxqObRKr6TQzetSzRx3G0CezowhR+knJUwcXtZmz:kxqeRKWTQzetSzRxGezz0qCwmt8
MD5:	CAFD973A406C557106D3E6D6080AE842
SHA1:	EFD4CCC681921C21A66AF69E84491B29413FBAFD
SHA-256:	FA9DED2DB16E626F7D760893E93B143E1075928376A23CE41F1D3F4985A884DD
SHA-512:	A734CB2F4BB18F684921354DF31DB34F12AA66E07CB85D77C4D9FEBAA769B4297FE6EFC11F7B40807A223B9BF65E484ED6699D754CACC8D00F9F9BC06CCFBF1A
Malicious:	false
Reputation:	unknown

C:\Users\user\Pictures\Adobe Films\i9v9KeSPU8TebYFmPJaLjDAO.exe	
Preview:	<html><head>..<title>404 Not Found</title>..</head><body>.. Not Found .. The requested URL was not found on this server. ..<hr>..<address>Apache/2.4.41 (Ubuntu) Server at 2.56.59.42 Port 80</address>..</body></html>

C:\Users\user\Pictures\Adobe Films\i_OjgwShp6vSNPTHoCRKJq5M.exe	
Process:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	858520
Entropy (8bit):	5.987726670125973
Encrypted:	false
SSDEEP:	12288:Kp5DkSnomwlvuSeznUUZeAaEjw127ipPGUPFzjOpHb/wZSnHRk9ryKAuq:u6mMGeAaoy2iUpLwZQYGj
MD5:	D848EEEEB11725A8D74841F9EDE3A762
SHA1:	3625E6081EC523DCBFCDF0CA333104CBC5EFF9CD
SHA-256:	0C46C1530A378D33708AD4D7C1322E2A8637710C0126674B0488DE4B3E6C47E6
SHA-512:	4E0FAFC1E5A59251B2B5CF531DFF3341E0777645CEBECC58C5C4608860E1BA4A98DBC2A9AC3BEB1A9A37084466840D844AE62BFEE4CD49F4B42BCA413A424 19
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....."...0..... ... .@.. .....`..... ..@.....d...W.... .....#...@..... .....H.....text..... ..... ..`.rsrc..... .....@..@.rel oc.....@.....@..B.....H.....@...$6.....4...0..t.....g.....y...ZsR...%r...po.....*.s.0..:...**....(V...*R....(W...r+..p(X...*f....oY...(Z...oY...o[...*.*.s.4..._...*R....oY...r+..po[...*R....o....r=..po[...*R....o....rg..p(X...*....o....r...pri..prq..p(g...o[...*R....o....r...p(X...*R....o....r...p(X...*R....o....r...p(X...*R....o....r...p(X...*R....o....r-..p(X.. .*.s.....m...*.~n...:....r;..p.....(!...o....s.....n...~n...*.~o...**.....o...*.~p...**....(....*Vs3

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.995039892451414
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	912534A5380738D96E8DDB7873ECB004667D72D5DF 783.exe
File size:	4250831
MD5:	8b7b82eb83d4a6760ecf8e9398ffda64
SHA1:	e827272cd42a9030741f4acb6004a97f6e13ba40
SHA256:	912534a5380738d96e8ddb7873ecb004667d72d5df783c abce2e398c11b14912
SHA512:	25b91ea923ab9b187c46f860769c1475e726226c5438a4 adb20ce372978b0b8c2f10b706a15bd86e5fde4e6864b85 34d82ec5cabba03825ad87350d559a98bbf
SSDEEP:	98304:xECvLUBsg2UgIhYr0/6nicI8HIDfPg6aiwm0CPtN XQCslQymye0:xZLUCgUIuw/6i8oDfY6Bwm0QtNX52Qp 0
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....#...B...B ...B...]...B...^...B...]...B...]...B...J...B...B...B...J...B...d...B... d...B....6..B.....B..]D...B..Rich.B.....

File Icon

Icon Hash:	8484d4f2b8f47434

Static PE Info

General

Entrypoint:	0x41910c
Entrypoint Section:	.text
Digitally signed:	false

General

Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NX_COMPAT
Time Stamp:	0x5C6ECB00 [Thu Feb 21 16:00:00 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	32569d67dc210c5cb9a759b08da2bdb3

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x19745	0x19800	False	0.583438648897	DOS executable (COM)	6.6301384284	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x1b000	0x3a98	0x3c00	False	0.3345703125	data	4.39318766185	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1f000	0x23f0	0x200	False	0.369140625	data	3.30022863793	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.sxdata	0x22000	0x4	0x200	False	0.02734375	data	0.0203931352361	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_LNK_INFO, IMAGE_SCN_MEM_READ
.rsrc	0x23000	0xab0	0xc00	False	0.344401041667	data	3.32928574611	IMAGE_SCN_CNT_INITIALIZED_DATA, 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: 912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe PID: 5000 Parent PID: 5604

General

Start time:	23:27:55
Start date:	04/12/2021
Path:	C:\Users\user\Desktop\912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\912534A5380738D96E8DDB7873ECB004667D72D5DF783.exe"
Imagebase:	0x400000
File size:	4250831 bytes
MD5 hash:	8B7B82EB83D4A6760ECF8E9398FFDA64
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: 00000000.00000003.286410815.00000000033AF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Socelars, Description: Yara detected Socelars, Source: 00000000.00000003.285629989.0000000002FC0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000003.286622786.0000000003687000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: setup_install.exe PID: 5528 Parent PID: 5000

General

Start time:	23:28:03
Start date:	04/12/2021
Path:	C:\Users\user\AppData\Local\Temp\7zS883210E8\setup_install.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\7zS883210E8\setup_install.exe"
Imagebase:	0x400000

File size:	2250181 bytes
MD5 hash:	74EFCE83CAF33BD4AA9A18A87B48B584
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 3744 Parent PID: 5528

General

Start time:	23:28:04
Start date:	04/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 1952 Parent PID: 5528

General

Start time:	23:28:05
Start date:	04/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c powershell -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Local\Temp"
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 1500 Parent PID: 5528

General

Start time:	23:28:05
Start date:	04/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c Mon06885bbdb13fec3.exe
Imagebase:	0xd80000
File size:	232960 bytes

MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: powershell.exe PID: 6004 Parent PID: 1952

General

Start time:	23:28:05
Start date:	04/12/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -inputformat none -outputformat none -NonInteractive -Command Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Local\Temp"
Imagebase:	0x10e0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: cmd.exe PID: 4008 Parent PID: 5528

General

Start time:	23:28:05
Start date:	04/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c Mon06dc62fb7183b9e.exe
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: Mon06885bbdb13fec3.exe PID: 924 Parent PID: 1500

General

Start time:	23:28:05
Start date:	04/12/2021
Path:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06885bbdb13fec3.exe
Wow64 process (32bit):	false
Commandline:	Mon06885bbdb13fec3.exe
Imagebase:	0x550000
File size:	8192 bytes
MD5 hash:	AE0BB0EF615F4606FBE1F050B6F08CA3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: SUSP_PE_Discord_Attachment_Oct21_1, Description: Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN), Source: C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06885bbdb13fec3.exe, Author: Florian Roth
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Registry Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6156 Parent PID: 5528

General

Start time:	23:28:06
Start date:	04/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c Mon06f9c53ffae25af61.exe
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: Mon06dc62fb7183b9e.exe PID: 6188 Parent PID: 4008

General

Start time:	23:28:06
Start date:	04/12/2021
Path:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06dc62fb7183b9e.exe
Wow64 process (32bit):	false
Commandline:	Mon06dc62fb7183b9e.exe
Imagebase:	0x15f593e0000
File size:	1575424 bytes
MD5 hash:	F7AD507592D13A7A2243D264906DE671

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000010.00000002.755737452.0000015F59499000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000010.00000000.294796789.0000015F59499000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06dc62fb7183b9e.exe, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6220 Parent PID: 5528

General

Start time:	23:28:06
Start date:	04/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c Mon06d47d8fde50.exe
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Mon06f9c53ffae25af61.exe PID: 6240 Parent PID: 6156

General

Start time:	23:28:06
Start date:	04/12/2021
Path:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06f9c53ffae25af61.exe
Wow64 process (32bit):	true
Commandline:	Mon06f9c53ffae25af61.exe
Imagebase:	0x400000
File size:	250368 bytes
MD5 hash:	FC6FCC4C6F1AA7674E7EFB71AE759A42
Has elevated privileges:	true

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

Analysis Process: cmd.exe PID: 6256 Parent PID: 5528

General

Start time:	23:28:06
Start date:	04/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c Mon0630c6f1115ad5.exe
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Mon06d47d8fde50.exe PID: 6264 Parent PID: 6220

General

Start time:	23:28:07
Start date:	04/12/2021
Path:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06d47d8fde50.exe
Wow64 process (32bit):	true
Commandline:	Mon06d47d8fde50.exe
Imagebase:	0x3d0000
File size:	455168 bytes
MD5 hash:	BB4D9EA74D539111AF6B40D6ED4452F8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: SUSP_Double_Base64_Encoded_Executable, Description: Detects an executable that has been encoded with base64 twice, Source: 00000014.00000002.356338732.0000000003811000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000014.00000002.356338732.0000000003811000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: cmd.exe PID: 6304 Parent PID: 5528

General

Start time:	23:28:07
Start date:	04/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c Mon06cebe79e9a244.exe
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

Analysis Process: Mon0630c6f1115ad5.exe PID: 6328 Parent PID: 6256

General

Start time:	23:28:07
Start date:	04/12/2021
Path:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon0630c6f1115ad5.exe
Wow64 process (32bit):	true
Commandline:	Mon0630c6f1115ad5.exe
Imagebase:	0x870000
File size:	542208 bytes
MD5 hash:	8A40BAC445ECB19F7CB8995B5AE9390B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira

Analysis Process: cmd.exe PID: 6340 Parent PID: 5528

General

Start time:	23:28:08
Start date:	04/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c Mon067df200a8fd43b.exe /mixone
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: Mon06cebe79e9a244.exe PID: 6360 Parent PID: 6304

General

Start time:	23:28:08
Start date:	04/12/2021
Path:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon06cebe79e9a244.exe
Wow64 process (32bit):	false
Commandline:	Mon06cebe79e9a244.exe
Imagebase:	0xa70000
File size:	51712 bytes
MD5 hash:	9535F08BD5920F84AC344F8884FE155D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: cmd.exe PID: 6368 Parent PID: 5528

General

Start time:	23:28:08

Start date:	04/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /c Mon066b4a7578e0123e.exe
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: Mon067df200a8fd43b.exe PID: 6380 Parent PID: 6340

General

Start time:	23:28:08
Start date:	04/12/2021
Path:	C:\Users\user\AppData\Local\Temp\7zS883210E8\Mon067df200a8fd43b.exe
Wow64 process (32bit):	true
Commandline:	Mon067df200a8fd43b.exe /mixone
Imagebase:	0x400000
File size:	350720 bytes
MD5 hash:	AD56ABB0034DE1257634EA56BE9C8CB6
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: 0000001A.00000000.324919353.00000000007DD000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 0000001A.00000002.734191823.0000000000400000.00000040.00020000.sdmp, Author: Florian Roth • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 0000001A.00000000.323840946.0000000000550000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 0000001A.00000000.322943664.0000000000400000.00000040.00020000.sdmp, Author: Florian Roth • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 0000001A.00000000.328474387.0000000000550000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 0000001A.00000000.329483296.00000000007DD000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 0000001A.00000002.746618380.0000000000550000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 0000001A.00000002.764915300.00000000007DD000.00000040.00000001.sdmp, Author: Florian Roth • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 0000001A.00000000.327784720.0000000000400000.00000040.00020000.sdmp, Author: Florian Roth • Rule: SUSP_XORed_Mozilla, Description: Detects suspicious XORed keyword - Mozilla/5.0, Source: 0000001A.00000003.306556711.00000000005D0000.00000004.00000001.sdmp, Author: Florian Roth
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML

Disassembly

Code Analysis