ID: 749948
Sample Name:
q4Z52wRd28.exe
Cookbook: default.jbs
Time: 16:56:08
Date: 19/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

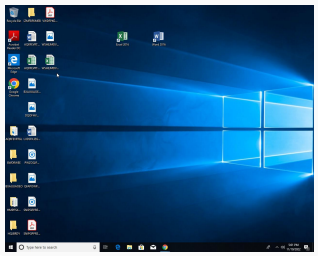
Windows Analysis Report

q4Z52wRd28.exe

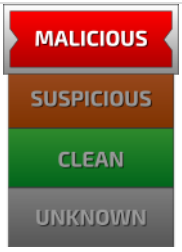
Overview

General Information

Sample Name:	q4Z52wRd28.exe
Analysis ID:	749948
MD5:	a687e1c326c9f0…
SHA1:	1993746a547c67..
SHA256:	8c2b385622de52..
Tags:	exe SmokeLoader
Infos:	



Detection



Ursnif, Amadey, RedLine, SmokeLoader, Vidar

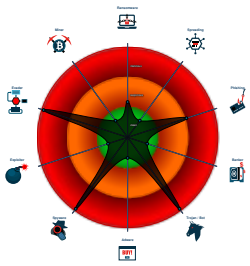
Score:

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

Signatures

- Yara detected RedLine Stealer
- Yara detected Amadeys stealer DLL
- Detected unpacking (overwrites its o…
- Yara detected Go Stealer
- Yara detected Ursnif
- Yara detected SmokeLoader
- Yara detected Amadey bot
- 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

Classification



Process Tree

- **System is w10x64**
- q4Z52wRd28.exe (PID: 5708 cmdline: C:\Users\user\Desktop\q4Z52wRd28.exe MD5: A687E1C326C9F03569BBFEF53E21C315)
  - explorer.exe (PID: 3452 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - A852.exe (PID: 6000 cmdline: C:\Users\user\AppData\Local\Temp\A852.exe MD5: 0E455D9C65E7D53A67C227DCD8D70FB8)
      - rovwer.exe (PID: 4852 cmdline: "C:\Users\user\AppData\Local\Temp\99e342142d\rovwer.exe" MD5: 0E455D9C65E7D53A67C227DCD8D70FB8)
        - schtasks.exe (PID: 2384 cmdline: "C:\Windows\System32\schtasks.exe" /Create /SC MINUTE /MO 1 /TN rovwer.exe /TR "C:\Users\user\AppData\Local\Temp\99e342142d\rovwer.exe" /F MD5: 15FF7D8324231381BAD48A052F85DF04)
          - conhost.exe (PID: 2364 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 6140 cmdline: "C:\Windows\System32\cmd.exe" /k echo Y|CACLS "rovwer.exe" /P "user:N"&&CACLS "rovwer.exe" /P "user:R" /E&&echo Y|CACLS "..\99e342142d" /P "user:N"&&CACLS "..\99e342142d" /P "user:R" /E&&Exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 2820 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - cmd.exe (PID: 68 cmdline: C:\Windows\system32\cmd.exe /S /D /c" echo Y" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - cacls.exe (PID: 2016 cmdline: CACLS "rovwer.exe" /P "user:N" MD5: 4CBB1C027DF71C53A8EE4C855FD35B25)
          - cacls.exe (PID: 5168 cmdline: CACLS "rovwer.exe" /P "user:R" /E MD5: 4CBB1C027DF71C53A8EE4C855FD35B25)
          - cmd.exe (PID: 5444 cmdline: C:\Windows\system32\cmd.exe /S /D /c" echo Y" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - cacls.exe (PID: 5484 cmdline: CACLS "..\99e342142d" /P "user:N" MD5: 4CBB1C027DF71C53A8EE4C855FD35B25)
          - cacls.exe (PID: 5608 cmdline: CACLS "..\99e342142d" /P "user:R" /E MD5: 4CBB1C027DF71C53A8EE4C855FD35B25)
        - rundll32.exe (PID: 4964 cmdline: "C:\Windows\System32\rundll32.exe" C:\Users\user\AppData\Roaming\a091ec0a6e2227\cred64.dll, Main MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - B4A7.exe (PID: 3080 cmdline: C:\Users\user\AppData\Local\Temp\B4A7.exe MD5: F96144B1D5B53D93CAADDDADE38DB5E9)
    - CF35.exe (PID: 4392 cmdline: C:\Users\user\AppData\Local\Temp\CF35.exe MD5: 44A7E13ECC55CE9797C5121B230D9927)
      - RegSvcs.exe (PID: 5128 cmdline: C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegSvcs.exe MD5: 59FCE79E9D81AB9E2ED4C3561205F5DF)
    - E35A.exe (PID: 4252 cmdline: C:\Users\user\AppData\Local\Temp\E35A.exe MD5: 19A79DADDFAAC09499E79ADE27E756F8)
    - EB2B.exe (PID: 5512 cmdline: C:\Users\user\AppData\Local\Temp\EB2B.exe MD5: F46063253FF38E6B2452BF4410C5FEC0)
      - EB2B.exe (PID: 5628 cmdline: C:\Users\user\AppData\Local\Temp\EB2B.exe MD5: F46063253FF38E6B2452BF4410C5FEC0)
        - EB2B.exe (PID: 5828 cmdline: C:\Users\user\AppData\Local\Temp\EB2B.exe MD5: F46063253FF38E6B2452BF4410C5FEC0)
          - cmd.exe (PID: 1852 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 6 & del /f /q "C:\Users\user\AppData\Local\Temp\EB2B.exe" & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
            - conhost.exe (PID: 5944 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
            - timeout.exe (PID: 5980 cmdline: timeout /t 6 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
    - F771.exe (PID: 5640 cmdline: C:\Users\user\AppData\Local\Temp\F771.exe MD5: DF920AEBFABB8C4CCCEB4DCEAD922ABD)
    - explorer.exe (PID: 5644 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
    - explorer.exe (PID: 5656 cmdline: C:\Windows\explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - explorer.exe (PID: 5816 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
    - explorer.exe (PID: 5876 cmdline: C:\Windows\explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - explorer.exe (PID: 5068 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)

- explorer.exe (PID: 3932 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
- explorer.exe (PID: 408 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
- explorer.exe (PID: 4972 cmdline: C:\Windows\explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- explorer.exe (PID: 5248 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)

- cttgcew (PID: 4220 cmdline: C:\Users\user\AppData\Roaming\cttgcew MD5: A687E1C326C9F03569BBFEF53E21C315)
- rovwer.exe (PID: 5372 cmdline: C:\Users\user\AppData\Local\Temp\99e342142d\rovwer.exe MD5: 0E455D9C65E7D53A67C227DCD8D70FB8)
- **cleanup**

Malware Configuration

Threatname: RedLine


```
{
  "C2 url": "185.106.92.111:2510",
  "Bot Id": "New2022",
  "Authorization Header": "ef6fe7baf59e3191ff2f569e3bf0e2c7"
}
```


Threatname: Ursnif


```
{
  "RSA Public Key":
"9YTR8AStfTOVxekPy7nye/rJL/CYnuMKiTBMit/N9dFJomCZQw3gdJ20hYjZiaY5PCNTRgc/z2gXfPlfCRRq0/mF+oSBOgliUoJHNN6O1Nl/zAv1hC+MVoITbvAJoj6LnOzFs9h/l3E4DMphz+dHiiDgppDXx4StPfi30EoQByvOIhjndZV3g8kYMJyGj8dxlmi3X9wSz6RHT9/HWCOS/i2phbREwr7oohHwh6mObxVhJVx0tZ18f2U+SsDunGdf1nLcyWHfM0cx6e8zBNRaXlZ1HhTEFzQdz5EF2h+r74n2bFODhb+ozhtKQ1CBEf0hf+5D8mLZuH2C+VOO+s90bjJxpTvGseErYwzAwE2lC4o=",
  "c2_domain": [
    "lentaphoto.at",
    "iujdhsndjfks.ru",
    "gameindikdowd.ru",
    "jhgfdlkjhaoiu.su"
  ],
  "botnet": "20",
  "server": "50",
  "serpent_key": "izoHlMTDxrB6IFB3",
  "sleep_time": "1",
  "CONF_TIMEOUT": "20",
  "SetWaitableTimer_value": "0"
}
```


Threatname: SmokeLoader


```
{
  "C2 list": [
    "http://o3l3roozuidudu.com/",
    "http://o3npxslymcyfi2.com/",
    "http://o3b1wk8sfk74tf.com/"
  ]
}
```


Threatname: Vidar


```
{
  "C2 url": [
    "https://t.me/deadftx",
    "https://www.tiktok.com/@user6068972597711"
  ],
  "Botnet": "1148",
  "Version": "55.7"
}
```


Yara Signatures

PCAP (Network Traffic)

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

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll	INDICATOR_TOOL_PWS_Amady	Detects password stealer DLL. Dropped by Amadey	ditekSHen	• 0xd86c:$s1: Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData • 0x15608:$s1: Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData • 0x16078:$s1: Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData • 0x1515c:$s2: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook • 0x151c0:$s2: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook • 0xdd10:$s3: \Mikrotik\Winbox\Addresses.cdb • 0x190dc:$s4: \HostName • 0x19104:$s5: \Password • 0x17c08:$s6: SOFTWARE\RealVNC\ • 0x17c34:$s6: SOFTWARE\RealVNC\ • 0x17c60:$s6: SOFTWARE\RealVNC\ • 0x17ca8:$s6: SOFTWARE\RealVNC\ • 0x17cd4:$s6: SOFTWARE\RealVNC\ • 0x1800c:$s7: SOFTWARE\TightVNC\ • 0x18038:$s7: SOFTWARE\TightVNC\ • 0x18064:$s7: SOFTWARE\TightVNC\ • 0x180b0:$s7: SOFTWARE\TightVNC\ • 0x1c43c:$s8: cred.dll
C:\Users\user\AppData\Roaming\a091ec0a6e2227\cred64.dll	JoeSecurity_Amadey_2	Yara detected Amadey\'s stealer DLL	Joe Security	
C:\Users\user\AppData\Roaming\a091ec0a6e2227\cred64.dll	INDICATOR_TOOL_PWS_Amady	Detects password stealer DLL. Dropped by Amadey	ditekSHen	• 0xd86c:$s1: Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData • 0x15608:$s1: Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData • 0x16078:$s1: Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\AppData • 0x1515c:$s2: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook • 0x151c0:$s2: Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook • 0xdd10:$s3: \Mikrotik\Winbox\Addresses.cdb • 0x190dc:$s4: \HostName • 0x19104:$s5: \Password • 0x17c08:$s6: SOFTWARE\RealVNC\ • 0x17c34:$s6: SOFTWARE\RealVNC\ • 0x17c60:$s6: SOFTWARE\RealVNC\ • 0x17ca8:$s6: SOFTWARE\RealVNC\ • 0x17cd4:$s6: SOFTWARE\RealVNC\ • 0x1800c:$s7: SOFTWARE\TightVNC\ • 0x18038:$s7: SOFTWARE\TightVNC\ • 0x18064:$s7: SOFTWARE\TightVNC\ • 0x180b0:$s7: SOFTWARE\TightVNC\ • 0x1c43c:$s8: cred.dll

Memory Dumps

Source	Rule	Description	Author	Strings
00000018.00000003.726670268.00000000017A8000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000018.00000003.726670268.00000000017A8000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_fd494041	unknown	unknown	• 0xff0:$a1: /C ping localhost -n %u && del "%s" • 0xf20:$a2: /C "copy "%s" "%s" /y && "%s" "%s" • 0xec8:$a3: /C "copy "%s" "%s" /y && rundll32 "%s",%S" • 0xca8:$a5: filename="%.4u.%lu" • 0x803:$a7: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0x63a:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xa41:$a8: %08X-%04X-%04X-%04X-%08X%04X • 0xe72:$a9: &whoami=%s • 0xe5a:$a10: %u.%u_%u_%u_x%u • 0xc22:$a11: size=%u&hash=0x%08x • 0xc13:$a12: &uptime=%u • 0xda7:$a13: %systemroot%\system32\c_1252.nls • 0x1416:$a14: IE10RunOnceLastShown_TIMESTAMP

Source	Rule	Description	Author	Strings
00000018.00000003.726670268.00000000017A8000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Gozi_261f5ac5	unknown	unknown	• 0xbd3:$a1: soft=%u&version=%u&user=%08x%08x%08x%08x&server=%u&id=%u&crc=%x • 0x803:$a2: version=%u&soft=%u&user=%08x%08x%08x%08x&server=%u&id=%u&type=%u&name=%s • 0xc74:$a3: Content-Disposition: form-data; name="upload_file"; filename="%.4u.%lu" • 0xafa:$a5: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT %u.%u%s) • 0xd4b:$a9: Software\AppDataLow\Software\Microsoft\ • 0x1c88:$a9: Software\AppDataLow\Software\Microsoft\
00000000.00000003.256917988.0000000000970000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000018.00000002.792008341.0000000000870000.00000040.00001000.00020000.00000000.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
Click to see the 97 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.3.cttgcew.870000.0.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
32.3.F771.exe.9c6b90.1.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
32.3.F771.exe.9c6b90.1.raw.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x34f0e:$pat14: , CommandLine: • 0x23dd6:$v2_1: ListOfProcesses • 0x2228c:$v4_3: base64str • 0x2224b:$v4_4: stringKey • 0x22296:$v4_5: BytesToStringConverted • 0x22281:$v4_6: FromBase64 • 0x23a93:$v4_8: procName • 0x20e54:$v5_1: DownloadAndExecuteUpdate • 0x20e7c:$v5_2: ITaskProcessor • 0x20e42:$v5_3: CommandLineUpdate • 0x20e6d:$v5_4: DownloadUpdate • 0x20db6:$v5_5: FileScanning • 0x21054:$v5_7: RecordHeaderField • 0x20f7e:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
13.3.B4A7.exe.716f68.3.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
13.3.B4A7.exe.716f68.3.unpack	MALWARE_Win_RedLine	Detects RedLine infostealer	ditekSHen	• 0x1f430:$pat14: , CommandLine: • 0x17162:$v2_1: ListOfProcesses • 0x16eed:$v4_3: base64str • 0x17f81:$v4_4: stringKey • 0x14b08:$v4_5: BytesToStringConverted • 0x13b70:$v4_6: FromBase64 • 0x152dc:$v4_8: procName • 0x1565f:$v5_1: DownloadAndExecuteUpdate • 0x16dfd:$v5_2: ITaskProcessor • 0x1564d:$v5_3: CommandLineUpdate • 0x1563e:$v5_4: DownloadUpdate • 0x15cf1:$v5_5: FileScanning • 0x14e77:$v5_7: RecordHeaderField • 0x14896:$v5_9: BCRYPT_KEY_LENGTHS_STRUCT
Click to see the 54 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 193.56.146.174 −

Timestamp:	192.168.2.3193.56.146.17449747802027700 11/19/22-16:58:50.225468
SID:	2027700
Source Port:	49747
Destination Port:	80
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 193.56.146.174	
Timestamp:	192.168.2.3193.56.146.17449753802027700 11/19/22-16:58:52.314328
SID:	2027700
Source Port:	49753
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 193.56.146.174	
Timestamp:	192.168.2.3193.56.146.17449744802027700 11/19/22-16:58:49.534930
SID:	2027700
Source Port:	49744
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 193.56.146.174	
Timestamp:	192.168.2.3193.56.146.17449746802027700 11/19/22-16:58:49.809680
SID:	2027700
Source Port:	49746
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18 - Source IP: 192.168.2.3 - Destination IP: 77.232.37.228	
Timestamp:	192.168.2.377.232.37.22849727802851815 11/19/22-16:58:32.473174
SID:	2851815
Source Port:	49727
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18 - Source IP: 192.168.2.3 - Destination IP: 77.232.37.228	
Timestamp:	192.168.2.377.232.37.22849736802851815 11/19/22-16:58:36.653112
SID:	2851815
Source Port:	49736
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 193.56.146.174	
Timestamp:	192.168.2.3193.56.146.17449752802027700 11/19/22-16:58:52.037330
SID:	2027700
Source Port:	49752
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 193.56.146.174	
Timestamp:	192.168.2.3193.56.146.17449748802027700 11/19/22-16:58:50.604993
SID:	2027700
Source Port:	49748
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 193.56.146.174	
Timestamp:	192.168.2.3193.56.146.17449751802027700 11/19/22-16:58:51.692909

SID:	2027700
Source Port:	49751
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 193.56.146.174	−
Timestamp:	192.168.2.3193.56.146.17449749802027700 11/19/22-16:58:51.029782
SID:	2027700
Source Port:	49749
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 193.56.146.174	−
Timestamp:	192.168.2.3193.56.146.17449750802027700 11/19/22-16:58:51.366139
SID:	2027700
Source Port:	49750
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18 - Source IP: 192.168.2.3 - Destination IP: 77.232.37.228	−
Timestamp:	192.168.2.377.232.37.22849730802851815 11/19/22-16:58:34.840324
SID:	2851815
Source Port:	49730
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Amadey CnC Check-In - Source IP: 192.168.2.3 - Destination IP: 193.56.146.174	−
Timestamp:	192.168.2.3193.56.146.17449745802027700 11/19/22-16:58:49.249164
SID:	2027700
Source Port:	49745
Destination Port:	80
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

Uses known network protocols on non-standard ports

May check the online IP address of the machine

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing

Yara detected Go Stealer

Yara detected Ursnif

Yara detected SmokeLoader

E-Banking Fraud

Yara detected Ursnif

System Summary

Malicious sample detected (through community Yara rule)

Writes or reads registry keys via WMI

Writes registry values via WMI

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Persistence and Installation Behavior

Yara detected Amadey bot

Boot Survival

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

Creates an undocumented autostart registry key

Hooking and other Techniques for Hiding and Protection

Yara detected Ursnif

Uses known network protocols on non-standard ports

Deletes itself after installation

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

Malware Analysis System Evasion

Opens the same file many times (likely Sandbox evasion)

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)

Anti Debugging

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

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
Allocates memory in foreign processes
Injects a PE file into a foreign processes
Contains functionality to inject code into remote processes
Creates a thread in another existing process (thread injection)
Writes to foreign memory regions
Injects code into the Windows Explorer (explorer.exe)
Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information

Yara detected RedLine Stealer
Yara detected Amadeys stealer DLL
Yara detected Ursnif
Yara detected SmokeLoader
Yara detected Amadey bot
Yara detected Vidar stealer
Tries to steal Mail credentials (via file / registry access)
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)
Tries to harvest and steal ftp login credentials
Tries to steal Instant Messenger accounts or passwords

Remote Access Functionality

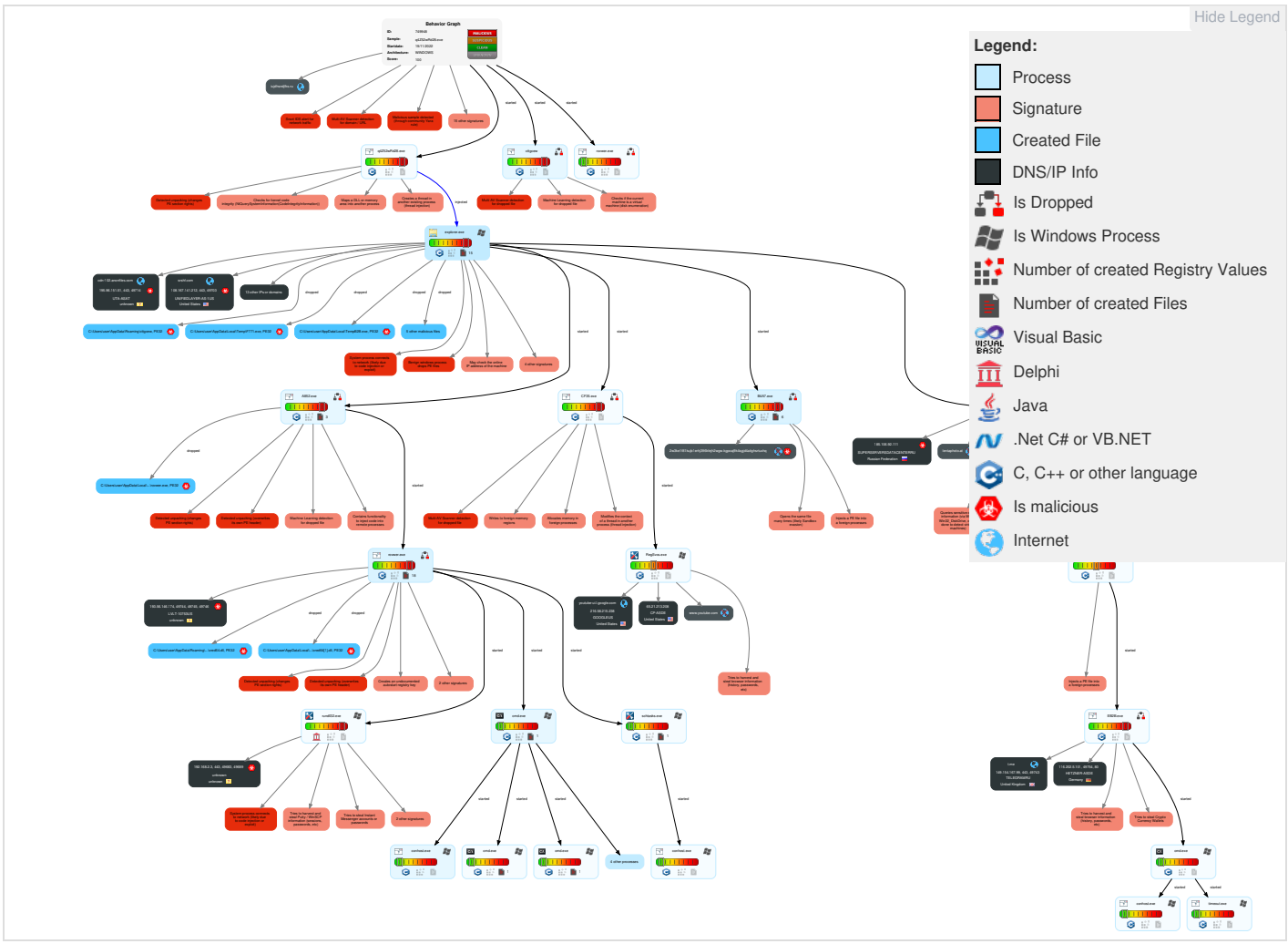
Yara detected RedLine Stealer
Yara detected Ursnif
Yara detected SmokeLoader
Yara detected Vidar stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	3 1 1 Windows Management Instrumentation	1 DLL Side-Loading	1 Exploitation for Privilege Escalation	1 Disable or Modify Tools	2 OS Credential Dumping	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 5 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Exploitation for Client Execution	1 Scheduled Task/Job	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	1 Input Capture	1 Account Discovery	Remote Desktop Protocol	4 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 Scheduled Task/Job	1 Registry Run Keys / Startup Folder	9 1 2 Process Injection	3 1 Obfuscated Files or Information	2 Credentials in Registry	3 File and Directory Discovery	SMB/Windows Admin Shares	1 Screen Capture	Automated Exfiltration	1 1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	1 Services File Permissions Weakness	1 Scheduled Task/Job	2 3 Software Packing	1 Credentials In Files	1 4 7 System Information Discovery	Distributed Component Object Model	1 Email Collection	Scheduled Transfer	5 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	1 Registry Run Keys / Startup Folder	1 DLL Side-Loading	LSA Secrets	4 4 1 Security Software Discovery	SSH	1 Input Capture	Data Transfer Size Limits	1 2 6 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	1 Services File Permissions Weakness	1 File Deletion	Cached Domain Credentials	3 3 1 Virtualization/Sandbox Evasion	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 3 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	3 3 1 Virtualization/Sandbox Evasion	Proc Filesystem	1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	9 1 2 Process Injection	/etc/passwd and /etc/shadow	1 System Owner/User 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 Remote System 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 Services File Permissions Weakness	Input Capture	1 System Network Configuration Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	1 Rundll32	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS			Inhibit System Recovery

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
q4Z52wRd28.exe	32%	Virustotal		Browse
q4Z52wRd28.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\a091ec0a6e2227\cred64.dll	100%	Avira	HEUR/AGEN.1233121	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll	100%	Avira	HEUR/AGEN.1233121	
C:\Users\user\AppData\Local\Temp\F771.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\cttgcew	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\B4A7.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\99e342142d\rovwer.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\A852.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\E35A.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\CF35.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll	88%	ReversingLabs	Win32.Infostealer.Decred	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll	71%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\B4A7.exe	21%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\CF35.exe	23%	ReversingLabs	Win64.Trojan.Lazy	
C:\Users\user\AppData\Local\Temp\E35A.exe	38%	ReversingLabs	Win32.Downloader.Deyma	
C:\Users\user\AppData\Local\Temp\EB2B.exe	27%	ReversingLabs	Win32.Trojan.Lazy	
C:\Users\user\AppData\Roaming\a091ec0a6e2227\cred64.dll	88%	ReversingLabs	Win32.Infostealer.Decred	
C:\Users\user\AppData\Roaming\a091ec0a6e2227\cred64.dll	71%	Metadefender		Browse
C:\Users\user\AppData\Roaming\cttgcew	27%	ReversingLabs	Win32.Trojan.Convagent	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.q4Z52wRd28.exe.960e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.3.E35A.exe.880000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
47.0.RegSvcs.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1216913		Download File
0.3.q4Z52wRd28.exe.970000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.2.E35A.exe.870e67.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.q4Z52wRd28.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.2.E35A.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
11.2.cttgcew.860e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.cttgcew.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.2.E35A.exe.bb0000.2.unpack	100%	Avira	HEUR/AGEN.1245293		Download File
11.3.cttgcew.870000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
cdn-102.anonfiles.com	3%	Virustotal		Browse
iujdhsndjfks.ru	0%	Virustotal		Browse
raw.githubusercontent.com	1%	Virustotal		Browse
o36fafs3sn6xou.com	15%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://o3b1wk8sfk74tf.com/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24Response	0%	URL Reputation	safe	
http://https://www.youtube.comindex	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://o3npxslymcyfi2.com/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	
http://o3l3roozuidudu.com/	0%	URL Reputation	safe	
http://o36fafs3sn6xou.com/Mozilla/5.0	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13Response	0%	URL Reputation	safe	
http://o36fafs3sn6xou.com/	0%	URL Reputation	safe	
http://https://raw.githubusercontent.com/decoder1989/Wallet/main/Crypted.exe	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://tempuri.org/Entity/Id2ResponseX%	0%	Avira URL Cloud	safe	
http://65.21.213.208:3000inconsistent	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id1ResponseinX%	0%	Avira URL Cloud	safe	
http://116.202.5.101/446391140202.zip	100%	Avira URL Cloud	malware	
http://https://cdn-102.anonfiles.com/p8DdCeH9yd/c1844f86-1668548628/TELEGRAM.exe	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/@user6068972597711	0%	Avira URL Cloud	safe	
http://193.56.146.168/mia/solt.exe	100%	Avira URL Cloud	malware	
http://116.202.5.101:80	100%	Avira URL Cloud	malware	
http://193.56.146.174/g84kvj4jck/index.php?scr=1	100%	Avira URL Cloud	malware	
http://tempuri.org/Entity/Id4X%	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id22ResponseX%	0%	Avira URL Cloud	safe	
http://https://studio.youtube.com28421709430404007434844970703125:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdn-102.anonfiles.com	195.96.151.51	true	true	• 3%, Virustotal, Browse	unknown
bitbucket.org	104.192.141.1	true	false		high
github.com	140.82.121.4	true	false		high
iujdhsndjfks.ru	134.0.118.203	true	false	• 0%, Virustotal, Browse	unknown
raw.githubusercontent.com	185.199.108.133	true	true	• 1%, Virustotal, Browse	unknown
t.me	149.154.167.99	true	false		high
o36fafs3sn6xou.com	77.232.37.228	true	true	• 15%, Virustotal, Browse	unknown
anonfiles.com	45.154.253.151	true	true		unknown
hoteldostyk.com	43.231.112.109	true	true		unknown
iplogger.com	148.251.234.93	true	false		high
s3-w.us-east-1.amazonaws.com	3.5.21.195	true	false		high
youtube-ui.l.google.com	216.58.215.238	true	false		high
srshf.com	108.167.141.212	true	true		unknown
transfer.sh	144.76.136.153	true	false		high
1ecosolution.it	46.252.148.24	true	true		unknown
bbuseruploads.s3.amazonaws.com	unknown	unknown	false		high
2w3ke1f81kujb1erhj396kfejh2wgw.kgpoaj9k4sgjd4aitghsrtuxhq	unknown	unknown	true		unknown
lentaphoto.at	unknown	unknown	true		unknown
www.youtube.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://193.56.146.168/mia/solt.exe	true	• Avira URL Cloud: malware	unknown
http://https://iplogger.com/2bibu4	false		high
http://https://raw.githubusercontent.com/decoder1989/Wallet/main/Crypted.exe	false	• Avira URL Cloud: safe	unknown
http://193.56.146.174/g84kvj4jck/index.php?scr=1	true	• Avira URL Cloud: malware	unknown
http://o3b1wk8sfk74tf.com/	true	• URL Reputation: safe	unknown
http://https://bitbucket.org/globallinstall/updatenow1.3.5/downloads/downloadsupdated.now-1.3.5.exe	false		high
http://https://t.me/deadftx	false		high
http://o3npxslymcyfi2.com/	true	• URL Reputation: safe	unknown
http://o3l3roozuidudu.com/	true	• URL Reputation: safe	unknown
http://https://cdn-102.anonfiles.com/p8DdCeH9yd/c1844f86-1668548628/TELEGRAM.exe	false	• Avira URL Cloud: safe	unknown
http://116.202.5.101/446391140202.zip	true	• Avira URL Cloud: malware	unknown
http://https://www.tiktok.com/@user6068972597711	true	• Avira URL Cloud: safe	unknown
http://o36fafs3sn6xou.com/	true	• 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	F771.exe, 00000020.00000002.853522237.00000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/sc/sct	F771.exe, 00000020.00000002.853522237.00000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/chrome_newtab	F771.exe, 00000020.00000002.856653515.00000000002CBA000.00000004.00000800.00020000.00000000.sdmp, EB2B.exe, 00000024.00000003.491597267.00000000275E1000.00000004.00000800.00020000.00000000.sdmp, 45253720055769576867799735.36.dr, 396800001610779748367819 23.36.dr	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/sc/dk	F771.exe, 00000020.00000002.853522237.00000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	396800001610779748367819 23.36.dr	false		high
http://116.202.5.101:80	EB2B.exe, 00000024.00000002.525842671.00000000002EB0000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://tempuri.org/Entity/Id12Response	F771.exe, 00000020.00000002.852334346.00000000002A61000.00000004.00000800.00020000.00000000.sdmp, F771.exe, 00000020.00000002.853313389.0000000002AF6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/rm8Dh	F771.exe, 00000020.00000002.852334346.00000000002A61000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.google.com/intl/en_uk/chrome/https://www.google.com/intl/en_uk/chrome/https://www.google	EB2B.exe, 00000024.00000003.486203645.000000275DE000.00000004.00000800.00020000.00000000.sdmp, EB2B.exe, 00000024.00000003.488632208.00000000273DD000.00000004.00000800.00020000.00000000.sdmp, 65329382289861898742549564.36.dr, 42917201296364153697665931.36.dr	false		high
http://tempuri.org/Entity/Id2ResponseX%	F771.exe, 00000020.00000002.853313389.0000000002AF6000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://tempuri.org/	F771.exe, 00000020.00000002.852334346.00000000002A61000.00000004.00000800.00020000.00000000.sdmp, F771.exe, 00000020.00000002.853522237.0000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id2Response	F771.exe, 00000020.00000002.852334346.00000000002A61000.00000004.00000800.00020000.00000000.sdmp, F771.exe, 00000020.00000002.853522237.0000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/sc/dk/p_sha1	F771.exe, 00000020.00000002.853522237.00000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id21Response	F771.exe, 00000020.00000002.852334346.00000000002A61000.00000004.00000800.00020000.00000000.sdmp, F771.exe, 00000020.00000002.853313389.0000000002AF6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/2005/02/trust/spnego#GSS_Wrap	F771.exe, 00000020.00000002.853522237.00000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID	F771.exe, 00000020.00000002.853522237.00000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/answer/6315198?product=	42917201296364153697665931.36.dr	false		high
http://https://www.youtube.com	RegSvcs.exe, 0000002F.00000002.623396941.000000C0000AA000.00000004.00001000.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust#BinarySecret	F771.exe, 00000020.00000002.853522237.00000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	F771.exe, 00000020.00000002.853522237.00000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://studio.youtube.com/youtubei/v1/security/get_web_reauth_url?alt=json&key=tls:	RegSvcs.exe, 0000002F.00000002.570733528.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false		high

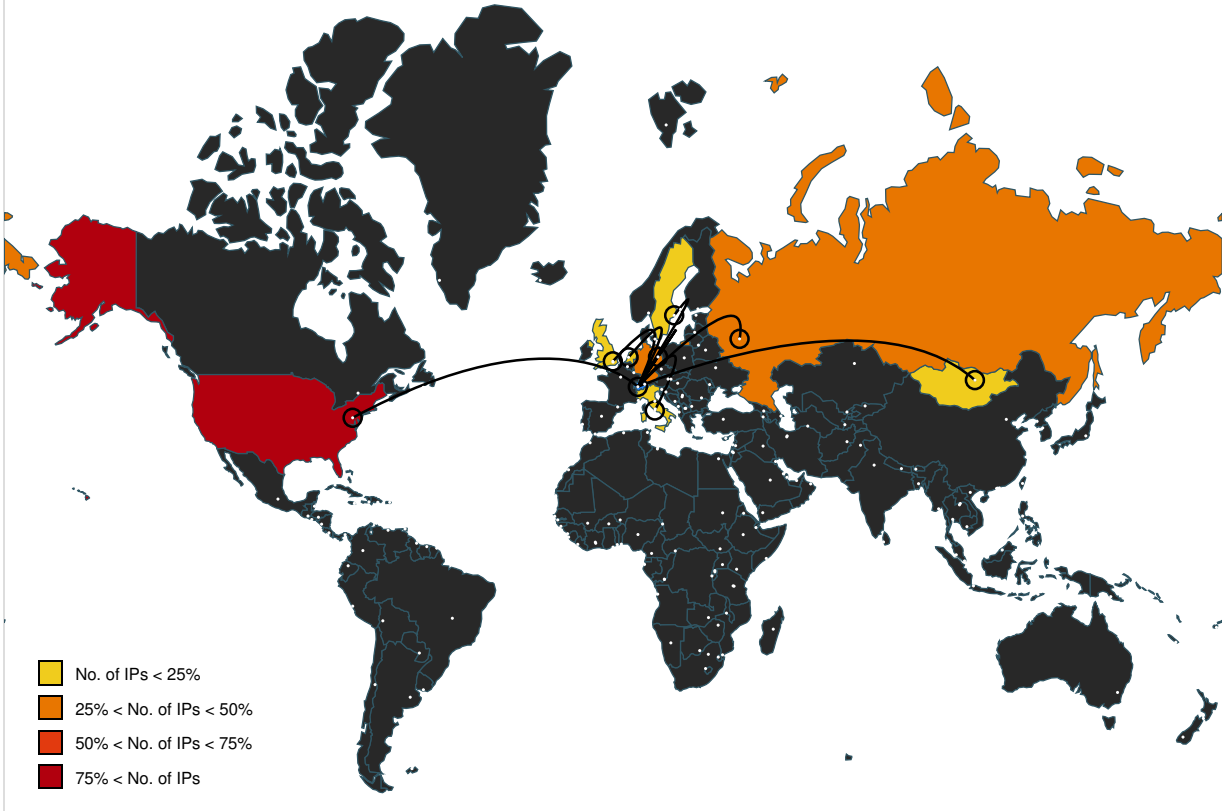
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.google.com/intl/en_uk/chrome/thank-you.html?statcb=0&installdataindex=empty&defaultbrows	42917201296364153697665931.36.dr	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Aborted	F771.exe, 00000020.00000002.853522237.0000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/TerminateSequence	F771.exe, 00000020.00000002.852334346.0000000002A61000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/fault	F771.exe, 00000020.00000002.853522237.0000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat	F771.exe, 00000020.00000002.853522237.0000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id15Response	F771.exe, 00000020.00000002.852334346.0000000002A61000.00000004.00000800.00020000.00000000.sdmp, F771.exe, 00000020.00000002.853313389.0000000002AF6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://support.google.com/chrome?p=update_error	EB2B.exe, 00000024.00000002.584817068.000000276DC000.00000004.00000800.00020000.00000000.sdmp, EB2B.exe, 00000024.00000003.488205767.00000000273DD000.00000004.00000800.00020000.00000000.sdmp, EB2B.exe, 00000024.00000003.488388825.00000000275EA000.00000004.00000800.00020000.00000000.sdmp, 65329382289861898742549564.36.dr, 42917201296364153697665931.36.dr	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	F771.exe, 00000020.00000002.853522237.0000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://studio.youtube.com/reauth	RegSvcs.exe, 0000002F.00000002.570733528.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Renew	F771.exe, 00000020.00000002.853522237.0000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/Register	F771.exe, 00000020.00000002.853522237.0000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://65.21.213.208:3000inconsistent	RegSvcs.exe, 0000002F.00000002.570733528.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://schemas.xmlsoap.org/ws/2004/04/trust/SymmetricKey	F771.exe, 00000020.00000002.853522237.0000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.google.com/intl/en_uk/chrome/Google	65329382289861898742549564.36.dr, 42917201296364153697665931.36.dr	false		high
http://https://api.ip.sb/ip	B4A7.exe, 0000000D.00000003.527908931.0000000D290000.00000004.00000800.00020000.00000000.sdmp, B4A7.exe, 0000000D.00000003.533006922.000000000D292000.00000040.00000800.00020000.00000000.sdmp, F771.exe, 00000020.00000002.848936854.000000000263A000.00000004.00000800.00020000.00000000.sdmp, F771.exe, 00000020.00000002.850270333.00000000027A0000.00000004.08000000.00040000.00000000.sdmp, F771.exe, 00000020.00000002.853522237.0000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id1ResponseinX%	F771.exe, 00000020.00000002.853313389.0000000002AF6000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Cancel	F771.exe, 00000020.00000002.853522237.0000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	39680000161077974836781923.36.dr	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/CK/PSHA1	F771.exe, 00000020.00000002.853522237.0000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id24Response	F771.exe, 00000020.00000002.852334346.0000000002A61000.00000004.00000800.00020000.00000000.sdmp, F771.exe, 00000020.00000002.853313389.0000000002AF6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	F771.exe, 00000020.00000002.856653515.00000000CBA000.00000004.00000800.00020000.00000000.sdmp, EB2B.exe, 00000024.00000003.491597267.00000000275E1000.00000004.00000800.00020000.00000000.sdmp, 452537200557695768677995735.36.dr, 396800001610779748367819 23.36.dr	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/AckRequested	F771.exe, 00000020.00000002.852334346.00000000002A61000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/tlsnego	F771.exe, 00000020.00000002.853522237.00000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://search.yahoo.com/search	explorer.exe, 00000027.00000002.772302955.00000000008F1000.00000040.80000000.00040000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing	F771.exe, 00000020.00000002.852334346.00000000002A61000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.youtube.comindex	RegSvcs.exe, 0000002F.00000002.570733528.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	F771.exe, 00000020.00000002.853522237.00000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoordinationContextResponse	F771.exe, 00000020.00000002.853522237.00000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id5Response	F771.exe, 00000020.00000002.852334346.00000000002A61000.00000004.00000800.00020000.00000000.sdmp, F771.exe, 00000020.00000002.853522237.0000000002B2B000.00000004.00000800.00020000.00000000.sdmp, F771.exe, 00000020.00000002.853313389.0000000002AF6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dns	F771.exe, 00000020.00000002.852334346.00000000002A61000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10Response	F771.exe, 00000020.00000002.852334346.00000000002A61000.00000004.00000800.00020000.00000000.sdmp, F771.exe, 00000020.00000002.853522237.0000000002B2B000.00000004.00000800.00020000.00000000.sdmp, F771.exe, 00000020.00000002.853313389.0000000002AF6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/Renew	F771.exe, 00000020.00000002.853522237.00000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8Response	F771.exe, 00000020.00000002.852334346.00000000002A61000.00000004.00000800.00020000.00000000.sdmp, F771.exe, 00000020.00000002.853522237.0000000002B2B000.00000004.00000800.00020000.00000000.sdmp, F771.exe, 00000020.00000002.853313389.0000000002AF6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t.me/deadftxhttps://www.tiktok.com/	EB2B.exe, 0000001C.00000002.454935093.00000000B40000.00000004.00000800.00020000.00000000.sdmp, EB2B.exe, 0000001F.00000002.471247692.0000000000C50000.00000004.00000800.00020000.00000000.sdmp, EB2B.exe, 00000024.00000002.519975927.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLAssertionID	F771.exe, 00000020.00000002.853522237.00000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/SCT	F771.exe, 00000020.00000002.853522237.00000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2006/02/addressingidentity	F771.exe, 00000020.00000002.853522237.00000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://studio.youtube.com/youtubei/v1/ars/grst?alt=json&key=net/http:	RegSvcs.exe, 0000002F.00000002.570733528.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey	F771.exe, 00000020.00000002.853522237.000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Rollback	F771.exe, 00000020.00000002.853522237.000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/SCT	F771.exe, 00000020.00000002.853522237.000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/06/addressingex	F771.exe, 00000020.00000002.853522237.000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://o36fafs3sn6xou.com/Mozilla/5.0	explorer.exe, 00000021.00000000.45633319 3.0000000000540000.00000040.80000000.00040000.00000000.sdmp, explorer.exe, 00000022.00000000.459238945.0000000000540000.00000040.80000000.00040000.00000000.sdmp, explorer.exe, 00000022.00000002.777469766.0000000009D0000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000023.00000000.462429473.0000000000120000.00000040.80000000.00040000.00000000.sdmp, explorer.exe, 00000025.00000000.465274597.0000000001400000.00000040.80000000.00040000.00000000.sdmp, explorer.exe, 00000025.00000002.771553703.0000000580000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000026.00000002.784028840.0000000003497000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000027.00000000.474180010.000000000900000.00000040.80000000.00040000.00000000.sdmp, explorer.exe, 00000029.00000000.476884087.000000000A70000.00000040.80000000.00040000.00000000.sdmp, explorer.exe, 0000002A.00000000.479766782.0000000000510000.00000040.80000000.00040000.00000000.sdmp, explorer.exe, 0000002A.00000002.774664749.00000000009D0000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000002B.00000000.482523463.0000000000650000.00000040.80000000.00040000.00000000.sdmp, explorer.exe, 0000002B.00000002.778517394.00000000009B8000.00000004.00000020.00020000.00000000.sdmp	true	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id22ResponseX%	F771.exe, 00000020.00000002.852334346.000000002A61000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/trust/Nonce	F771.exe, 00000020.00000002.853522237.000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/CreateSequenceResponse	F771.exe, 00000020.00000002.852334346.000000002A61000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id4X%	F771.exe, 00000020.00000002.852334346.000000002A61000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://studio.youtube.com28421709430404007434844970703125:	RegSvcs.exe, 0000002F.00000002.570733528.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://support.google.com/chrome/answer/111996?visit_id=637962485686793996-3320600880&p=update_erro	42917201296364153697665931.36.dr	false		high
http://https://www.google.com/intl/en_uk/chrome/	42917201296364153697665931.36.dr	false		high
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_REQ1510	F771.exe, 00000020.00000002.853522237.000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://studio.youtube.com/youtubei/v1/att/esr?alt=json&key=https://studio.youtube.com/youtubei/v1/a	RegSvcs.exe, 0000002F.00000002.570733528.0000000000400000.00000040.00000400.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id13Response	F771.exe, 00000020.00000002.852334346.000000002A61000.00000004.00000800.00020000.00000000.sdmp, F771.exe, 00000020.00000002.853313389.0000000002AF6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd	F771.exe, 00000020.00000002.853522237.000000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509SubjectKeyIdentif	F771.exe, 00000020.00000002.853522237.00000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Committed	F771.exe, 00000020.00000002.853522237.00000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/CK/PSHA1	F771.exe, 00000020.00000002.853522237.00000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-soap-message-security-1.1#ThumbprintSHA1	F771.exe, 00000020.00000002.853522237.00000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/right/possessproperty	F771.exe, 00000020.00000002.852334346.00000002A61000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/sc/sct	F771.exe, 00000020.00000002.853522237.00000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/SequenceAcknowledgement	F771.exe, 00000020.00000002.852334346.00000002A61000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT	F771.exe, 00000020.00000002.853522237.00000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	F771.exe, 00000020.00000002.856653515.00000002CBA000.00000004.00000800.00020000.00000000.sdmp, EB2B.exe, 00000024.00000003.491597267.00000000275E1000.00000004.00000800.00020000.00000000.sdmp, 45253720055769576867799735.36.dr, 396800001610779748367819 23.36.dr	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous	F771.exe, 00000020.00000002.852334346.00000002A61000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/2005/02/trust/tlsnego#TLS_Wrap	F771.exe, 00000020.00000002.853522237.00000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2002/12/policy	F771.exe, 00000020.00000002.853522237.00000002B2B000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
43.231.112.109	hoteldostyk.com	Mongolia		63962	ITOOLS-ASiToolsJSCMN	true
65.21.213.208	unknown	United States		199592	CP-ASDE	false
216.58.215.238	youtube-ui.l.google.com	United States		15169	GOOGLEUS	false
195.96.151.51	cdn-102.anonfiles.com	unknown		8437	UTA-ASAT	true
140.82.121.4	github.com	United States		36459	GITHUBUS	false
185.106.92.111	unknown	Russian Federation		50113	SUPERSERVERSDATACENTERRU	true
149.154.167.99	t.me	United Kingdom		62041	TELEGRAMRU	false
108.167.141.212	srshf.com	United States		46606	UNIFIEDLAYER-AS-1US	true
144.76.136.153	transfer.sh	Germany		24940	HETZNER-ASDE	false
104.192.141.1	bitbucket.org	United States		16509	AMAZON-02US	false
116.202.5.101	unknown	Germany		24940	HETZNER-ASDE	false
3.5.21.195	s3-w.us-east-1.amazonaws.com	United States		14618	AMAZON-AESUS	false
148.251.234.93	iplogger.com	Germany		24940	HETZNER-ASDE	false
185.199.108.133	raw.githubusercontent.com	Netherlands		54113	FASTLYUS	true
193.56.146.174	unknown	unknown		10753	LVLT-10753US	true
77.232.37.228	o36fafs3sn6xou.com	Russian Federation		28968	EUT-ASEUTIPNetworkRU	true
46.252.148.24	1ecosolution.it	Italy		60087	ASSUPERNOVAIT	true
45.154.253.151	anonfiles.com	Sweden		41634	SVEASE	true
193.56.146.168	unknown	unknown		10753	LVLT-10753US	true

Private

IP
192.168.2.3

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	749948
Start date and time:	2022-11-19 16:56:08 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	q4Z52wRd28.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:	47
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.phis.troj.spyw.evad.winEXE@67/24@47/20
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 30.8% (good quality ratio 21%) • Quality average: 34.6% • Quality standard deviation: 30%
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, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, login.live.com, watson.telemetry.microsoft.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 exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtDeviceIoControlFile 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 NtQueryAttributesFile 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
16:58:02	Task Scheduler	Run new task: Firefox Default Browser Agent 6797C828451BEB6A path: C:\Users\user\AppData\Roaming\cttgcew
16:58:34	API Interceptor	849x Sleep call for process: rovwer.exe modified
16:58:35	Task Scheduler	Run new task: rovwer.exe path: C:\Users\user\AppData\Local\Temp\99e342142d\rovwer.exe
16:58:48	API Interceptor	1077x Sleep call for process: explorer.exe modified
17:01:07	API Interceptor	3x Sleep call for process: F771.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:\ProgramData\074775062885300292736707l4

Process:	C:\Users\user\AppData\Local\Temp\EB2B.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 2, database pages 23, cookie 0x19, schema 4, UTF-8, version-valid-for 2

Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.7876734657715041
Encrypted:	false
SSDEEP:	48:43KzOIIY3HzrkNSs8LKvUf9KnmIG0UX9q4lCm+KLka+yJqhM0ObVEq8Ma0D0HOlx:Sq0NFeymDlGD9qlm+KL2y0Obn8MouO
MD5:	CF7758A2FF4A94A5D589DEBAED38F82E
SHA1:	D3380E70D0CAEB9AD78D14DD970EA480E08232B8
SHA-256:	6CA783B84D01BFCF9AA7185D7857401D336BAD407A182345B97096E1F2502B7F
SHA-512:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804CB F
Malicious:	false
Preview:	SQLite format 3.....@ .....[5..... ....

C:\ProgramData\34118869306534953191217255

Process:	C:\Users\user\AppData\Local\Temp\EB2B.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 17, database pages 7, 1st free page 5, free pages 2, cookie 0x13, schema 4, UTF-8, version-valid-for 17
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	1.4755077381471955
Encrypted:	false
SSDEEP:	96:oesz0Rwhba5DX1tHQOd0AS4mcAMmgAU7MxTWbKSS:o+RwE55tHQOKB4mcmgAU7MxTWbNS
MD5:	DEE86123FE48584BA0CE07793E703560
SHA1:	E80D87A2E55A95BC937AC24525E51AE39D635EF7
SHA-256:	60DB12643ECF5B13E6F05E0FBC7E0453D073E0929412E39428D431DB715122C8
SHA-512:	65649B808C7AB01A65D18BF259BF98A4E395B091D17E49849573275B7B93238C3C9D1E5592B340ABCE3195F183943CA8FB18C1C6C2B5974B04FE99FCCF582BFI
Malicious:	false
Preview:	SQLite format 3.....@ .....[5.....g...$..... ....

C:\ProgramData\39680000161077974836781923

Process:	C:\Users\user\AppData\Local\Temp\EB2B.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\ProgramData\42917201296364153697665931

Process:	C:\Users\user\AppData\Local\Temp\EB2B.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 7, database pages 36, 1st free page 10, free pages 1, cookie 0x29, schema 4, UTF-8, version-valid-for 7
Category:	dropped
Size (bytes):	147456
Entropy (8bit):	0.7217007190866341
Encrypted:	false
SSDEEP:	384:kab+d5neKTnuRpHDiEwABBE3umab+QuJdi:kab+dVeK8iEZBBjmab+QuJdi

MD5:	FEF7F4B210100663DC7731400BAC534E
SHA1:	E3F17C46A2DB6861F22B3F4222B97DCB5EBBD47A
SHA-256:	E81118F5C967EA342A16BDEFB28919F8039E772F8BDCF4A65684E3F56D31EA0E
SHA-512:	6134CC2118FBADD137C4FC3204028B088C7E73A7B985A64D84C60ABD5B1DBFD0AA352C6DF199F43164FEC92378571B5FAC4F801E9AF7BE1DEA8FB6C3C799F 95
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....).....[5..... ....

C:\ProgramData\4525372005576957686867799735

Process:	C:\Users\user\AppData\Local\Temp\EB2B.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 4, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2882898331044472
Encrypted:	false
SSDEEP:	192:go1/8dpUXbSzTPJPn6UVuUhoEwn7PrH944:gS/inPvVuUhoEwn7b944
MD5:	4822E6A71C88A4AB8A27F90192B5A3B3
SHA1:	CC07E541426BFF64981CE6DE7D879306C716B6B9
SHA-256:	A6E2CCBD736E5892E658020543F4DF20BB422253CAC06B37398AA4935987446E
SHA-512:	C4FCA0DBC8A6B00383B593046E30C5754D570AA2009D4E26460833FB1394D348776400174C898701F621C305F53DC03C1B42CF76AA5DC33D5CCD8FA44935B03
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\ProgramData\65329382289861898742549564

Process:	C:\Users\user\AppData\Local\Temp\EB2B.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 7, database pages 36, 1st free page 10, free pages 1, cookie 0x29, schema 4, UTF-8, version-valid-for 7
Category:	dropped
Size (bytes):	147456
Entropy (8bit):	0.7217007190866341
Encrypted:	false
SSDEEP:	384:kab+d5neKTnuRpHDiEwABBE3umab+QuJdi:kab+dVeK8iEZBBjmab+QuJdi
MD5:	FEF7F4B210100663DC7731400BAC534E
SHA1:	E3F17C46A2DB6861F22B3F4222B97DCB5EBBD47A
SHA-256:	E81118F5C967EA342A16BDEFB28919F8039E772F8BDCF4A65684E3F56D31EA0E
SHA-512:	6134CC2118FBADD137C4FC3204028B088C7E73A7B985A64D84C60ABD5B1DBFD0AA352C6DF199F43164FEC92378571B5FAC4F801E9AF7BE1DEA8FB6C3C799F 95
Malicious:	false
Preview:	SQLite format 3.....@ .....$.....).....[5..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll

Process:	C:\Users\user\AppData\Local\Temp\99e342142d\rovwer.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	129024
Entropy (8bit):	6.5122035629449355
Encrypted:	false
SSDEEP:	3072:Yx7pOYzBekK3tiINwyP7XSSJds3zhrjPcnqULv4G9:Yx7ZNhK3vwyOztPc3L
MD5:	507E9DC7B9C42F535B6DF96D79179835
SHA1:	ACF41FB549750023115F060071AA5CA8C33F249E
SHA-256:	3B82A0EA49D855327B64073872EBB6B63EEE056E182BE6B1935AA512628252AF
SHA-512:	70907EC4C395B0D2219BFE98907EC130BFCBC6D4BEC7BD73965A9B1E422553E27DAAEAD3D6647620FCF5392D85A2E975BCE0F7C79C0BC665DD33CE65F7D44 302
Malicious:	**true**

Yara Hits:	• Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll, Author: Joe Security • Rule: INDICATOR_TOOL_PWS_Amady, Description: Detects password stealer DLL. Dropped by Amadey, Source: C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 88% • Antivirus: Metadefender, Detection: 71%, Browse
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....X.....|.....@.....@.....O.....&... ....CODE..... ..`DATA.....@...BSS.....idata..&.....@....edata..O.....@..P.reloc .....@..P.rsrc..... .....@..P.....@.....@..P..... .....

C:\Users\user\AppData\Local\Temp\853321935212

Process:	C:\Users\user\AppData\Local\Temp\99e342142d\rovwer.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, components 3
Category:	dropped
Size (bytes):	83622
Entropy (8bit):	7.896233698964525
Encrypted:	false
SSDEEP:	1536:CQK+hI2P4mo0keu1RQ99zoHIgtO7czx4997CGPdOjT06SejjnhiVxp669P:JAmo081RQfzbgtOm4HrlO/jTjhKhZ
MD5:	B06A833A71D8716720C60C23DF02F550
SHA1:	2FD374453D9C4CB2846545FDDC72DA9E180D59AA
SHA-256:	A0B3FEDED6D6FA5822265F0F232E491533488D14AB18ABE177E34C2CC0F8828A
SHA-512:	756F671F4FC63F0D36E263C6AC591F06D0CA3F6E3A58A1E184E25F53214495F147FA36AE7E4B6287F7940148EF53A657C7BF19B2831C5F25916FEAA90C70A875
Malicious:	false
Preview:	......JFIF.....`.`.....C..... $.' ",#..(7),01444.'9=82<.342...C.....2!.!2222222222222222222222222222222222222222222222222222..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..01KK...lq\....xcS.m..#Hm.....T.....<!...wq5...v1.?S.....rHj-.U:...5.....\|..+.....}...<.>...H.....Wo.CK`/l.1./...C...W.....,1....R.0.W.M.!.l7.~S....."SW.^..c.....^s.....u,-n....A..?.2.....I.(.?....7..~.q$.f..1\.q[.....oS:.gOY".....f-%.P.b.Z...../.....)f..9^v..H .....U.J.L4k)J..c...^...<.....T.....y.....5..}.....

C:\Users\user\AppData\Local\Temp\99e342142d\rovwer.exe

Process:	C:\Users\user\AppData\Local\Temp\A852.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	385536
Entropy (8bit):	6.960915435029956
Encrypted:	false
SSDEEP:	6144:jUN5jZipJMHjeMigfbk532zhVVPE+O1voXc:U5tipJMDDiKkpCDO
MD5:	0E455D9C65E7D53A67C227DCD8D70FB8
SHA1:	F776A9F8165D6E41FB249223B5568D9C3FFA23B4
SHA-256:	29BF9DAF2F5FFC7DF253FA7FDD78E4A02669DF89FD7F0517A599F6C70EA1F121
SHA-512:	D441908A743FECD572518624238C138C7C7F4A88779963D8134AC7B5E9CB89C52259A2F601BB8891A565DEF48B07771AB4EA623C81B54306F3290FFC364C5BC/
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....P...1x.1x.1x.c..1x.c..!1x.c..1x....1x.1y..1x.c..1x.c..1x.c..1x.Rich.1x. .....PE..L.....a.....*....D.....P.....@....@.....F....aZ.....t/..(....pC.xE.....E..... -..@..... .....text...R(.....*..... ..`.data....*B..@...*.....@....rsrc...xE...pC..F...X.....@..@.reloc...B....E..D.....@..B..... .....

C:\Users\user\AppData\Local\Temp\A852.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	385536
Entropy (8bit):	6.960915435029956
Encrypted:	false
SSDEEP:	6144:jUN5jZipJMHjeMigfbk532zhVVPE+O1voXc:U5tipJMDDiKkpCDO
MD5:	0E455D9C65E7D53A67C227DCD8D70FB8
SHA1:	F776A9F8165D6E41FB249223B5568D9C3FFA23B4
SHA-256:	29BF9DAF2F5FFC7DF253FA7FDD78E4A02669DF89FD7F0517A599F6C70EA1F121
SHA-512:	D441908A743FECD572518624238C138C7C7F4A88779963D8134AC7B5E9CB89C52259A2F601BB8891A565DEF48B07771AB4EA623C81B54306F3290FFC364C5BC/

Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....P...1x.1x.1x.c..1x.c..!1x.c..1x....1x.1y..1x.c..1x.c..1x.c..1x.Rich.1x. .....PE..L.....a.....*....D.....P.....@....@.....F.....aZ.....t/..(....pC.xE.....E..... -..@..... .....text...R(.....*..... ..`.data....*B..@..*.....@....rsrc...xE...pC..F...X.....@..@.reloc...B....E..D.....@..B..... ....

C:\Users\user\AppData\Local\Temp\B4A7.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1235912
Entropy (8bit):	7.847488370221355
Encrypted:	false
SSDEEP:	24576:tpoG1/LlgEyH9QhH0slclslX6ptmEh4NqYJUo02O7RVUCshnSVjGMY0tZ8bMyqZs:tpocLlac0s5Ih4Ny/Ybb
MD5:	F96144B1D5B53D93CAADDDADE38DB5E9
SHA1:	1587E66F9A4D83060EE597F983A7323A556BC1C0
SHA-256:	63018F38311387AA7F511F090FD154EA6EC3799C2F4762890082793912C68146
SHA-512:	824A86438150DF143C7475605600B4A03DBFA819806F193BE248650A3A70E97BDCD3D20CAC9B8B00693D464B5CBD168E1F0C78BEAA00D167B8A877CFBCE3C3C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 21%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....?..{..M{..M{..M..fMg..M..SMi..M..gM...Mr.^Mr..M{..M&..M..bMy.. M..WMz..M{.ZM}..M..PMz..MRich{..M.....PE..L...O.wc.....X.....mk.....p....@..... .....d.....3..... .....p..\.....text....V.....X..... ..`.rdata...%...p...&...\.....@..@.data...,5.....@....rsrc....3.....4..... ...@..@..... .....

C:\Users\user\AppData\Local\Temp\CF35.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	3188224
Entropy (8bit):	7.964888519163398
Encrypted:	false
SSDEEP:	98304:9R5aeXkEIsmuDvFmvNtLmVLF5HLiBrvpPFI:9Dv5lJz4v3LMLiBrh2
MD5:	44A7E13ECC55CE9797C5121B230D9927
SHA1:	B99F1D86E6D9C7E0D694CA605ABD205663278487
SHA-256:	9E0425E14520485FA7E86057D07D26E8064F99A7AD09E35211EDD4A428EE57AE
SHA-512:	74DF06B20D23483F854B5A88E5CCDFE534497630A105614E6CD87F3238398E0FB03218CB864FD6F7798B69E083C1098225010AECD959FBEC28D63C0626711A9F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 23%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....}!...O...O...O..wL...O..wK...O..wJ.e.O..wN...O...N..O.fK...O. fL...O.fJ..O.fJ...O.fM...O.Rich..O.....PE..d....0xc.....".... .6.....4.....@.....1.....`.....^..(.....0.$$.....0. (...P).....(..@.....P.....text....5.....6..... ..`.rdata.....P.....:.....@..@.data....6-..p... -..T.....@....pdata..$$....0..&...t0.. .....@..@_RDATA..\.....0.....0.....@..@.reloc..(.....0.....0.....@..B..... .....

C:\Users\user\AppData\Local\Temp\E35A.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	342528
Entropy (8bit):	6.812640405950158
Encrypted:	false
SSDEEP:	6144:CV8MTz4fnz5/zNOCVmcUh+3oQ9gOU+fzYBb6:bMYfz5smmM9gT6
MD5:	19A79DADDFAAC09499E79ADE27E756F8
SHA1:	6BFD114AF2D1A68C4724961C6E761373EFE66C52
SHA-256:	3F2EA3CA90B2DF0D2A93DF0E4328F58077A5BDBB97B2DFFE81B589C057F93216
SHA-512:	AEA9D6CF93EB6ADA5D895C70DA8CBF4CA56BEB1125FC33961E112DCBAEA122F82DD4CBC9FE241DDCC5F5EBC6A71F83B03BEAF645F3A6E2724ACB03E7D61007A3

Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 38%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....{..?iB.?iB.?iB.!;..iB.!;..iB.!;..AiB...9.<iB.?iC.FiB.!;.>iB.!;.>iB.!;.> iB.Rich?iB.....PE..L...^Na..... ....D.....H.....0....@.....pE.....!.....t%..(.....B..A..... E..... -..@..... .....text...V..... ....`.data.....A..0.....$.....@....rsrc....A....B..B.....@..@.reloc...A... E..B.....@..B..... ....

C:\Users\user\AppData\Local\Temp\EB2B.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	341006
Entropy (8bit):	7.632238569480827
Encrypted:	false
SSDEEP:	6144:mYCc3GK5cRKFKT0Am1GaDgj9cBtrttZbzT1+lq0UMNpBfO/6kjDt/JwrkgdxEy:mA3GKiRzTLQWKBtrzdpx/u6kBJwvjz
MD5:	F46063253FF38E6B2452BF4410C5FEC0
SHA1:	C2444E21CC72BFC1CD74197E327323EB2E3E3815
SHA-256:	D0A4986CEA15C050DEE854CCD21CFF84179A950A70FAEC28526C7AEBD25A0970
SHA-512:	BFA09A46DACD3138448A93782229B24993F47F6EF6C7B283B55A32E056BB76DC63F043FC4BB64D57F49FB6D5B3A97551B55EC0363B2F7DF3193E5144F85A3A5(
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 27%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....=Y.S..S..S.....S...W..S...P..S...V...S...R..S...R..S..R...S._.V..S._. ...S._.Q..S.Rich.S.....PE..L....uxc.....".j...<.....+m.....@.....A.....@.....8..... .....@.....text....i.....j..... ..`.rdata...%.....&...n.....@..@.data...P.....@....rsrc.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\F771.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	459264
Entropy (8bit):	7.1855716974211346
Encrypted:	false
SSDEEP:	6144:2nj+jLGbR5prANXqK4ULWttLmBr3C7JVMUjpPnFwCLLObfwB:A+He6NXpWRmBrgfxqC3O
MD5:	DF920AEBFABB8C4CCCEB4DCEAD922ABD
SHA1:	BE09CF240FBB15B7EAFC3D875C17B0EE30E94AA1
SHA-256:	46DC1985999FC34875C1110E2E9A177A5A637B7668657525F6148AAC2CD23996
SHA-512:	075AB9409F4DB41ADBA43652F3CF00DDA51799D9146AD7502B4B04524C68EBC2A0108307E979B49D86C45051F9D31684514F96490B5D782107C279BFF90C8CA6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....P...1x.1x.1x.c..1x.c..!1x.c..1x....1x.1y..1x.c..1x.c..1x.c..1x.Rich.1x. .....PE..L...y..a.....*....E.....JP.....@....@.....0G.....$/..(.....D..F.....F.....,..@..... .....text....(.....*..... ..`.data...hGC..@...H.....@....rsrc....F....D..H...v.....@..@.reloc..FC....F..D.....@..B..... ....

C:\Users\user\AppData\Local\Temp\prefix3648256442

Process:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegSvcs.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, file counter 17, database pages 7, 1st free page 5, free pages 2, cookie 0x13, schema 4, UTF-8, version-valid-for 17
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	1.4755077381471955
Encrypted:	false
SSDEEP:	96:oesz0Rwhba5DX1tHQOd0AS4mcAMmgAU7MxTWbKSS:o+RwE55tHQOKB4mcmgAU7MxTWbNS
MD5:	DEE86123FE48584BA0CE07793E703560
SHA1:	E80D87A2E55A95BC937AC24525E51AE39D635EF7
SHA-256:	60DB12643ECF5B13E6F05E0FBC7E0453D073E0929412E39428D431DB715122C8
SHA-512:	65649B808C7AB01A65D18BF259BF98A4E395B091D17E49849573275B7B93238C3C9D1E5592B340ABCE3195F183943CA8FB18C1C6C2B5974B04FE99FCCF582BF
Malicious:	false

Preview:	SQLite format 3.....@ .....[5.....g...$..... ....

C:\Users\user\AppData\Roaming\a091ec0a6e2227\cred64.dll

Process:	C:\Users\user\AppData\Local\Temp\99e342142d\rovwer.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	129024
Entropy (8bit):	6.5122035629449355
Encrypted:	false
SSDEEP:	3072:Yx7pOYzBekK3tiINwyP7XSSJds3zhrjPcnqULv4G9:Yx7ZNhK3vwyOztPc3L
MD5:	507E9DC7B9C42F535B6DF96D79179835
SHA1:	ACF41FB5497500231150060071AA5CA8C33F249E
SHA-256:	3B82A0EA49D855327B64073872EBB6B63EEE056E182BE6B1935AA512628252AF
SHA-512:	70907EC4C395B0D2219BFE98907EC130BFCBC6D4BEC7BD73965A9B1E422553E27DAAEAD3D6647620FCF5392D85A2E975BCE0F7C79C0BC665DD33CE65F7D44302
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: C:\Users\user\AppData\Roaming\a091ec0a6e2227\cred64.dll, Author: Joe Security • Rule: INDICATOR_TOOL_PWS_Amady, Description: Detects password stealer DLL. Dropped by Amadey, Source: C:\Users\user\AppData\Roaming\a091ec0a6e2227\cred64.dll, Author: ditekSHen
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 88% • Antivirus: Metadefender, Detection: 71%, Browse
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....X.....|.....@.....@.....O.....&.... ....CODE..... ..`DATA.....@...BSS.....idata..&.....@....edata..O.....@..P.reloc .....@..P.rsrc..... .....@..P.....@.....@..P..... ....

C:\Users\user\AppData\Roaming\cttgcew

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	346112
Entropy (8bit):	6.783777931421013
Encrypted:	false
SSDEEP:	3072:OJvvbtjLGg1cSgH7P7AGkZ2gdRJvh2vOfPztr+c+PEG7lOmV25lKE1miUO1a1e4Y:mtfGg0b8Gkfvh2v0BohVVPE+O1voXc
MD5:	A687E1C326C9F03569BBFEF53E21C315
SHA1:	1993746A547C67807C1118501E1A7FF9261F7C8B
SHA-256:	8C2B385622DE52145317D9E740B62EDFB74260EFAB3478810D6C87CA41183F74
SHA-512:	69C6D3A228AD0DF876CA3259A1CBD62893C48409AF271D9C4871FC8BDBB8E35ECF0C2D382086B65FC155A86D9CCD6101379A4D02D2F54545A5F746A6558D6AC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 27%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....P...1x.1x.1x.c..1x.c..!1x.c..1x....1x.1y..1x.c..1x.c..1x.c..1x.Rich.1x. .....PE..L.....a.....*....D.....P.....@....@.....E.....2.....t/..(.....B.xE.....0E..... -..@..... .....text...R(.....*..... ..`.data.....A..@.....@....rsrc...xE....B..F.....@..@.reloc..8B...0E..D.....@..B..... ....

C:\Users\user\AppData\Roaming\cttgcew: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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\ghjhtic

Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	160970
Entropy (8bit):	**7.998900883724737**
Encrypted:	**true**
SSDEEP:	3072:iFVVQpnXXKcnOEKdQWGFs+Um9HLUqgoDAQnXerfTky0f3Pi2v:zHpnBKBG6+Um9HRTnXSTVm3Pi2v
MD5:	C66EE78ED2EAEECD82D2A2BB7C48AE08
SHA1:	04AB951005835DA0DBF2A8E5E611D538621C355B
SHA-256:	16C7C2BBB880B27F2760880B05E1F62BB7267C26A12540111A56853812DC1375
SHA-512:	836F2B0C46D7F13204F4534B4BF00F98DFD82C2C5F2AE41B5F44CE93376380BC2B97B92190CB9EA41E376DDEE01D183FAAFB92E595AD842A5B44780C3515B82F
Malicious:	false
Preview:	i.<.m.....qbjm.....!..\.,...E...;.`^...0..k.+%.j..Q.....Tw;..-P..!L.3...g.`Cw.q\./.. t3<T#. _a...2...Tf.V1.'.....#.l[.u)'....v)....tP;.....^....g.....Q....|.....c..Q....i_KO..S{._....._..D..4nlyI.wv .....V1....b.....@..1.H.%.....9.&.W.g....?..*6.W\..w... 1...Z.S..P.'...{.....;..F...G.5w.PZ.&A:e....Ax.....&zD...L#.....'7....$.0h.Lhc.....?...S.%....Eq)..\..bjq..'..-.....Yg.. ..Lz..... ..8P.%N.Mm-h$...l.x...d.X..GA.....;D..b.f-.n.....9.8....%'...m.am^.c...Z...=g.....y4..i.,.....]i.s3'..O:.....^IA....O.s.)..z.Ok....'.%...~..*. ....&.1..L;d..v..Yz..o.!..=,....E.zy#.V..M. t.+T...rzU{...I6..Y.1..8.X..]J8.=&<>g..M.1^:....X.....3.....j..w....A.?O..aI7E....a....%...~..3N...J....PY.....u..._...WLip,f.....d...\.B.o.39f@X!b..gc3.l.So.....R#...'.]-p.gT.m.Kz6 k....R^V.!.\..a.Q..a!.:^q..P.U;Qh.....).a:....P+}.g.ng,.0.....V.....5..1.Ffw;KM..j.p'k..W..vL....*.b.v.u.*0.a.p..H..A..j{...j.....bt..L*.d.....V.4..`.wg."e._...X.Y&CY.(..3..l%.b.8

\Device\ConDrv

Process:	C:\Windows\SysWOW64\cacls.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	15
Entropy (8bit):	3.240223928941852
Encrypted:	false
SSDEEP:	3:o3F:o1
MD5:	509B054634B6DE74F111C3E646BC80FD
SHA1:	99B4C0F39144A92FE42E22473A2A2552FB16BD13
SHA-256:	07C7C151ADD6D955F3C876359C0E2A3A3FB0C519DD1E574413F0B68B345D8C36
SHA-512:	A9C2D23947DBE09D5ECFBF6B3109F3CF8409E43176AE10C18083446EDE006E60E41C3EA2D2765036A967FC81B085D5F271686606AED4154AE45287D412CF6D4
Malicious:	false
Preview:	processed dir:

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.783777931421013
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:	q4Z52wRd28.exe
File size:	346112
MD5:	a687e1c326c9f03569bbfef53e21c315
SHA1:	1993746a547c67807c1118501e1a7ff9261f7c8b
SHA256:	8c2b385622de52145317d9e740b62edfb74260efab3478810d6c87ca41183f74
SHA512:	69c6d3a228ad0df876ca3259a1cbd62893c48409af271d9c4871fc8bdbb8e35ecf0c2d382086b65fc155a86d9ccd6101379a4d02d2f54545a5f746a6558d6a1c
SSDEEP:	3072:OJvvbtjLGg1cSgH7P7AGkZ2gdRJvh2vOfPztr+c+PEG7lOmV25lKE1miUO1a1e4Y:mtfGg0b8Gkfvh2v0BohVVPE+O1voXc
TLSH:	4D74BF10FFD8C4E6C57DC4707A25CBE86638BCA27915DA1373787A5E6FB02818E62235
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....P...1x..1x..1x..c...1x..c..l1x..c...1x.....1x..1y..1x..c...1x..c...1x..c...1x.Rich.1x.....PE..L.....a.....

File Icon

Icon Hash:	b4fcb6b6b69486e2

Static PE Info

General

Entrypoint:	0x40509a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x619DE380 [Wed Nov 24 07:02:24 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:	063e5449636b8762744e9ce9f5564a0d

Entrypoint Preview

Instruction
call 00007F69949EA88Eh
jmp 00007F69949E5DEDh
push 00000008h
push 00412B58h
call 00007F69949E6759h
mov ecx, dword ptr [ebp+08h]
test ecx, ecx
je 00007F69949E5F9Ch
cmp dword ptr [ecx], E06D7363h
jne 00007F69949E5F94h
mov eax, dword ptr [ecx+1Ch]
test eax, eax
je 00007F69949E5F8Dh
mov eax, dword ptr [eax+04h]
test eax, eax
je 00007F69949E5F86h
and dword ptr [ebp-04h], 00000000h
push eax
push dword ptr [ecx+18h]
call 00007F69949EAA17h
mov dword ptr [ebp-04h], FFFFFFFEh
call 00007F69949E6768h
ret
xor eax, eax
cmp byte ptr [ebp+0Ch], al
setne al
ret
mov esp, dword ptr [ebp-18h]
call 00007F69949EA955h
int3
call 00007F69949E6F32h

Instruction
xor ecx, ecx
cmp dword ptr [eax+00000090h], ecx
setne cl
mov al, cl
ret
mov edi, edi
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
mov dword ptr [0042CF90h], eax
pop ebp
ret
mov edi, edi
push ebp
mov ebp, esp
sub esp, 00000328h
mov eax, dword ptr [00414454h]
xor eax, ebp
mov dword ptr [ebp-04h], eax
and dword ptr [ebp-00000328h], 00000000h
push ebx
push 0000004Ch
lea eax, dword ptr [ebp-00000324h]
push 00000000h
push eax
call 00007F69949EAD3Dh
lea eax, dword ptr [ebp-00000328h]
mov dword ptr [ebp-000002D8h], eax
lea eax, dword ptr [ebp-000002D0h]
add esp, 0Ch
mov dword ptr [ebp+00FFFD2Ch], eax

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C] VS2008 build 21022 • [C++] VS2008 build 21022 • [IMP] VS2005 build 50727 • [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	0x12f74	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x42e000	0x24578	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x453000	0xba8	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x11d0	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	0x2d20	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x184	.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	0x12852	0x12a00	False	0.582778418624161	data	6.708277757836571	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x14000	0x4190a8	0x19000	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x42e000	0x24578	0x24600	False	0.6301613509450171	data	6.346796819372492	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x453000	0x4238	0x4400	False	0.14981617647058823	data	1.7315741222067773	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
AFX_DIALOG_LAYOUT	0x4501b8	0x2	data	Setsuana	South Africa
AFX_DIALOG_LAYOUT	0x4501a0	0x2	data	Setsuana	South Africa
AFX_DIALOG_LAYOUT	0x450190	0xe	data	Setsuana	South Africa
AFX_DIALOG_LAYOUT	0x450180	0xe	data	Setsuana	South Africa
AFX_DIALOG_LAYOUT	0x4501a8	0xe	data	Setsuana	South Africa
NAMUFILAZOXOGOJUNOCILI	0x44e160	0x1f9c	ASCII text, with very long lines (8092), with no line terminators	Setsuana	South Africa
SIYOBOVEJAH	0x44d358	0x7d1	ASCII text, with very long lines (2001), with no line terminators	Setsuana	South Africa
ZONAGOPEGOVERUXAZAVIFAZE	0x44db30	0x629	ASCII text, with very long lines (1577), with no line terminators	Setsuana	South Africa
RT_CURSOR	0x4501c0	0x330	Device independent bitmap graphic, 48 x 96 x 1, image size 0	Setsuana	South Africa
RT_CURSOR	0x4504f0	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0	Setsuana	South Africa
RT_CURSOR	0x450648	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Setsuana	South Africa
RT_CURSOR	0x4514f0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Setsuana	South Africa
RT_CURSOR	0x451dc0	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0	Setsuana	South Africa
RT_CURSOR	0x451ef0	0xb0	Device independent bitmap graphic, 16 x 32 x 1, image size 0	Setsuana	South Africa
RT_ICON	0x42edd0	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Setsuana	South Africa
RT_ICON	0x42fc78	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Setsuana	South Africa
RT_ICON	0x430520	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Setsuana	South Africa
RT_ICON	0x430a88	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x433030	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x4340d8	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x434a60	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x434f30	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Setsuana	South Africa
RT_ICON	0x435dd8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Setsuana	South Africa
RT_ICON	0x436680	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x438c28	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x439cd0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x43a188	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Setsuana	South Africa
RT_ICON	0x43b030	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Setsuana	South Africa

Name	RVA	Size	Type	Language	Country
RT_ICON	0x43b8d8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Setsuana	South Africa
RT_ICON	0x43be40	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x43e3e8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x43f490	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x43fe18	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x4402e8	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	Setsuana	South Africa
RT_ICON	0x441190	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Setsuana	South Africa
RT_ICON	0x441a38	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	Setsuana	South Africa
RT_ICON	0x442100	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	Setsuana	South Africa
RT_ICON	0x442668	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	Setsuana	South Africa
RT_ICON	0x444c10	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	Setsuana	South Africa
RT_ICON	0x445cb8	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	Setsuana	South Africa
RT_ICON	0x446640	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	Setsuana	South Africa
RT_ICON	0x446b20	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Setsuana	South Africa
RT_ICON	0x4479c8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Setsuana	South Africa
RT_ICON	0x448270	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Setsuana	South Africa
RT_ICON	0x448938	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Setsuana	South Africa
RT_ICON	0x448ea0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x44b448	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x44c4f0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x44ce78	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Setsuana	South Africa
RT_STRING	0x4521b8	0x3bc	data	Setsuana	South Africa
RT_ACCELERATOR	0x450100	0x40	data	Setsuana	South Africa
RT_GROUP_CURSOR	0x450620	0x22	data	Setsuana	South Africa
RT_GROUP_CURSOR	0x451d98	0x22	data	Setsuana	South Africa
RT_GROUP_CURSOR	0x451fa0	0x22	data	Setsuana	South Africa
RT_GROUP_ICON	0x434ec8	0x68	data	Setsuana	South Africa
RT_GROUP_ICON	0x43a138	0x4c	data	Setsuana	South Africa
RT_GROUP_ICON	0x440280	0x68	data	Setsuana	South Africa
RT_GROUP_ICON	0x446aa8	0x76	data	Setsuana	South Africa
RT_GROUP_ICON	0x44d2e0	0x76	data	Setsuana	South Africa
RT_VERSION	0x451fc8	0x1f0	MS Windows COFF PowerPC object file	Setsuana	South Africa
None	0x450150	0xa	data	Setsuana	South Africa
None	0x450140	0xa	data	Setsuana	South Africa
None	0x450160	0xa	data	Setsuana	South Africa
None	0x450170	0xa	data	Setsuana	South Africa

Imports

DLL	Import

DLL	Import
KERNEL32.dll	GetComputerNameA, SetProcessAffinityMask, WriteConsoleOutputCharacterA, OpenJobObjectA, GetCommState, AddConsoleAliasW, CreateHardLinkA, GetSystemDefaultLCID, GetModuleHandleW, GetTickCount, GetConsoleAliasesA, WaitNamedPipeW, LoadLibraryW, CopyFileW, GetFileAttributesA, EnumSystemCodePagesA, GetFileAttributesW, WriteConsoleW, GetVolumePathNameA, FillConsoleOutputCharacterW, GetLastError, GetProcAddress, VirtualAlloc, RemoveDirectoryA, LoadLibraryA, WriteConsoleA, GetProcessWorkingSetSize, LocalAlloc, GetModuleHandleA, CreateMutexA, FindNextFileW, GetStringTypeW, GetFileAttributesExW, SetFileShortNameA, GetVolumeNameForVolumeMountPointW, LCMapStringW, GetCommandLineA, GetStartupInfoA, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, EnterCriticalSection, LeaveCriticalSection, SetHandleCount, GetStdHandle, GetFileType, DeleteCriticalSection, HeapAlloc, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, SetLastError, GetCurrentThreadId, InterlockedDecrement, Sleep, HeapSize, ExitProcess, RtlUnwind, SetFilePointer, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, WriteFile, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, WideCharToMultiByte, GetEnvironmentStringsW, HeapCreate, VirtualFree, HeapFree, QueryPerformanceCounter, GetCurrentProcessId, GetSystemTimeAsFileTime, GetConsoleCP, GetConsoleMode, InitializeCriticalSectionAndSpinCount, HeapReAlloc, CloseHandle, CreateFileA, SetStdHandle, LCMapStringA, MultiByteToWideChar, GetStringTypeA, GetLocaleInfoA, FlushFileBuffers, GetConsoleOutputCP, SetEndOfFile, GetProcessHeap, ReadFile

Possible Origin

Language of compilation system	Country where language is spoken	Map
Setsuana	South Africa	

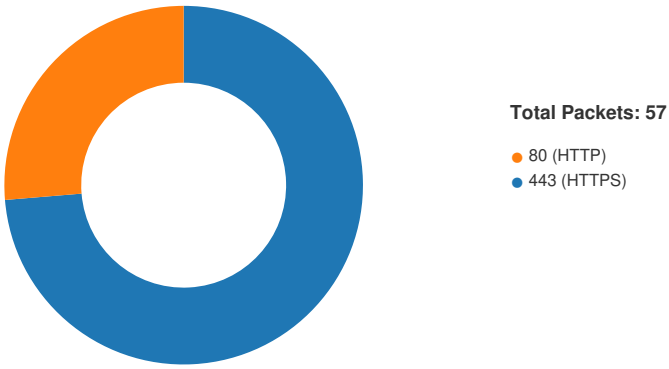
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3193.56.146.17 449747802027700 11/19/22-16:58:50.225468	TCP	2027700	ET TROJAN Amadey CnC Check-In	49747	80	192.168.2.3	193.56.146.174
192.168.2.3193.56.146.17 449753802027700 11/19/22-16:58:52.314328	TCP	2027700	ET TROJAN Amadey CnC Check-In	49753	80	192.168.2.3	193.56.146.174
192.168.2.3193.56.146.17 449744802027700 11/19/22-16:58:49.534930	TCP	2027700	ET TROJAN Amadey CnC Check-In	49744	80	192.168.2.3	193.56.146.174
192.168.2.3193.56.146.17 449746802027700 11/19/22-16:58:49.809680	TCP	2027700	ET TROJAN Amadey CnC Check-In	49746	80	192.168.2.3	193.56.146.174
192.168.2.377.232.37.228 49727802851815 11/19/22-16:58:32.473174	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49727	80	192.168.2.3	77.232.37.228
192.168.2.377.232.37.228 49736802851815 11/19/22-16:58:36.653112	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49736	80	192.168.2.3	77.232.37.228
192.168.2.3193.56.146.17 449752802027700 11/19/22-16:58:52.037330	TCP	2027700	ET TROJAN Amadey CnC Check-In	49752	80	192.168.2.3	193.56.146.174
192.168.2.3193.56.146.17 449748802027700 11/19/22-16:58:50.604993	TCP	2027700	ET TROJAN Amadey CnC Check-In	49748	80	192.168.2.3	193.56.146.174
192.168.2.3193.56.146.17 449751802027700 11/19/22-16:58:51.692909	TCP	2027700	ET TROJAN Amadey CnC Check-In	49751	80	192.168.2.3	193.56.146.174
192.168.2.3193.56.146.17 449749802027700 11/19/22-16:58:51.029782	TCP	2027700	ET TROJAN Amadey CnC Check-In	49749	80	192.168.2.3	193.56.146.174

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3193.56.146.17 449750802027700 11/19/22-16:58:51.366139	TCP	2027700	ET TROJAN Amadey CnC Check-In	49750	80	192.168.2.3	193.56.146.174
192.168.2.377.232.37.228 49730802851815 11/19/22-16:58:34.840324	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49730	80	192.168.2.3	77.232.37.228
192.168.2.3193.56.146.17 449745802027700 11/19/22-16:58:49.249164	TCP	2027700	ET TROJAN Amadey CnC Check-In	49745	80	192.168.2.3	193.56.146.174

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2022 16:57:08.058345079 CET	49697	443	192.168.2.3	23.35.236.109
Nov 19, 2022 16:57:08.058401108 CET	443	49697	23.35.236.109	192.168.2.3
Nov 19, 2022 16:57:08.058489084 CET	49697	443	192.168.2.3	23.35.236.109
Nov 19, 2022 16:57:08.059912920 CET	49697	443	192.168.2.3	23.35.236.109
Nov 19, 2022 16:57:08.059953928 CET	443	49697	23.35.236.109	192.168.2.3
Nov 19, 2022 16:57:08.140129089 CET	443	49697	23.35.236.109	192.168.2.3
Nov 19, 2022 16:57:08.140327930 CET	49697	443	192.168.2.3	23.35.236.109
Nov 19, 2022 16:57:08.146105051 CET	49697	443	192.168.2.3	23.35.236.109
Nov 19, 2022 16:57:08.146142006 CET	443	49697	23.35.236.109	192.168.2.3
Nov 19, 2022 16:57:08.146509886 CET	443	49697	23.35.236.109	192.168.2.3
Nov 19, 2022 16:57:08.172379017 CET	49697	443	192.168.2.3	23.35.236.109
Nov 19, 2022 16:57:08.172431946 CET	443	49697	23.35.236.109	192.168.2.3
Nov 19, 2022 16:57:08.191869020 CET	443	49697	23.35.236.109	192.168.2.3
Nov 19, 2022 16:57:08.192020893 CET	443	49697	23.35.236.109	192.168.2.3
Nov 19, 2022 16:57:08.192104101 CET	49697	443	192.168.2.3	23.35.236.109
Nov 19, 2022 16:57:08.192143917 CET	49697	443	192.168.2.3	23.35.236.109
Nov 19, 2022 16:57:08.192166090 CET	443	49697	23.35.236.109	192.168.2.3
Nov 19, 2022 16:57:08.192178011 CET	49697	443	192.168.2.3	23.35.236.109
Nov 19, 2022 16:57:08.192184925 CET	443	49697	23.35.236.109	192.168.2.3
Nov 19, 2022 16:57:08.221401930 CET	49698	443	192.168.2.3	23.35.236.109
Nov 19, 2022 16:57:08.221453905 CET	443	49698	23.35.236.109	192.168.2.3
Nov 19, 2022 16:57:08.221540928 CET	49698	443	192.168.2.3	23.35.236.109
Nov 19, 2022 16:57:08.221740961 CET	49698	443	192.168.2.3	23.35.236.109
Nov 19, 2022 16:57:08.221754074 CET	443	49698	23.35.236.109	192.168.2.3
Nov 19, 2022 16:57:08.286056995 CET	443	49698	23.35.236.109	192.168.2.3
Nov 19, 2022 16:57:08.287530899 CET	49698	443	192.168.2.3	23.35.236.109
Nov 19, 2022 16:57:08.287563086 CET	443	49698	23.35.236.109	192.168.2.3
Nov 19, 2022 16:57:08.288429022 CET	49698	443	192.168.2.3	23.35.236.109

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2022 16:57:08.288435936 CET	443	49698	23.35.236.109	192.168.2.3
Nov 19, 2022 16:57:08.323719025 CET	443	49698	23.35.236.109	192.168.2.3
Nov 19, 2022 16:57:08.323815107 CET	443	49698	23.35.236.109	192.168.2.3
Nov 19, 2022 16:57:08.323868036 CET	49698	443	192.168.2.3	23.35.236.109
Nov 19, 2022 16:57:08.325581074 CET	49698	443	192.168.2.3	23.35.236.109
Nov 19, 2022 16:57:08.325602055 CET	443	49698	23.35.236.109	192.168.2.3
Nov 19, 2022 16:57:08.325639963 CET	49698	443	192.168.2.3	23.35.236.109
Nov 19, 2022 16:57:08.325645924 CET	443	49698	23.35.236.109	192.168.2.3
Nov 19, 2022 16:57:21.010063887 CET	49699	443	192.168.2.3	131.253.33.200
Nov 19, 2022 16:57:21.010099888 CET	443	49699	131.253.33.200	192.168.2.3
Nov 19, 2022 16:57:21.010169983 CET	49699	443	192.168.2.3	131.253.33.200
Nov 19, 2022 16:57:21.013591051 CET	49699	443	192.168.2.3	131.253.33.200
Nov 19, 2022 16:57:21.013603926 CET	443	49699	131.253.33.200	192.168.2.3
Nov 19, 2022 16:57:21.101368904 CET	443	49699	131.253.33.200	192.168.2.3
Nov 19, 2022 16:57:21.101532936 CET	49699	443	192.168.2.3	131.253.33.200
Nov 19, 2022 16:57:21.102304935 CET	443	49699	131.253.33.200	192.168.2.3
Nov 19, 2022 16:57:21.102359056 CET	49699	443	192.168.2.3	131.253.33.200
Nov 19, 2022 16:57:21.141957045 CET	49699	443	192.168.2.3	131.253.33.200
Nov 19, 2022 16:57:21.141976118 CET	443	49699	131.253.33.200	192.168.2.3
Nov 19, 2022 16:57:21.142425060 CET	443	49699	131.253.33.200	192.168.2.3
Nov 19, 2022 16:57:21.142478943 CET	49699	443	192.168.2.3	131.253.33.200
Nov 19, 2022 16:57:21.143492937 CET	49699	443	192.168.2.3	131.253.33.200
Nov 19, 2022 16:57:21.143502951 CET	443	49699	131.253.33.200	192.168.2.3
Nov 19, 2022 16:57:21.143558979 CET	49699	443	192.168.2.3	131.253.33.200
Nov 19, 2022 16:57:21.143570900 CET	443	49699	131.253.33.200	192.168.2.3
Nov 19, 2022 16:57:21.143579006 CET	49699	443	192.168.2.3	131.253.33.200
Nov 19, 2022 16:57:21.143584967 CET	443	49699	131.253.33.200	192.168.2.3
Nov 19, 2022 16:57:21.143654108 CET	49699	443	192.168.2.3	131.253.33.200
Nov 19, 2022 16:57:21.143670082 CET	443	49699	131.253.33.200	192.168.2.3
Nov 19, 2022 16:57:21.143686056 CET	49699	443	192.168.2.3	131.253.33.200
Nov 19, 2022 16:57:21.143692970 CET	443	49699	131.253.33.200	192.168.2.3
Nov 19, 2022 16:57:21.143727064 CET	49699	443	192.168.2.3	131.253.33.200
Nov 19, 2022 16:57:21.143753052 CET	49699	443	192.168.2.3	131.253.33.200
Nov 19, 2022 16:57:21.143767118 CET	49699	443	192.168.2.3	131.253.33.200
Nov 19, 2022 16:57:21.143796921 CET	443	49699	131.253.33.200	192.168.2.3
Nov 19, 2022 16:57:21.298422098 CET	443	49699	131.253.33.200	192.168.2.3
Nov 19, 2022 16:57:21.298506021 CET	49699	443	192.168.2.3	131.253.33.200
Nov 19, 2022 16:57:21.298516989 CET	443	49699	131.253.33.200	192.168.2.3
Nov 19, 2022 16:57:21.298566103 CET	49699	443	192.168.2.3	131.253.33.200
Nov 19, 2022 16:57:21.317090034 CET	49699	443	192.168.2.3	131.253.33.200
Nov 19, 2022 16:57:21.317126989 CET	443	49699	131.253.33.200	192.168.2.3
Nov 19, 2022 16:57:21.317140102 CET	49699	443	192.168.2.3	131.253.33.200
Nov 19, 2022 16:57:21.317197084 CET	49699	443	192.168.2.3	131.253.33.200
Nov 19, 2022 16:57:45.591207027 CET	80	49683	93.184.220.29	192.168.2.3
Nov 19, 2022 16:57:45.591434002 CET	49683	80	192.168.2.3	93.184.220.29
Nov 19, 2022 16:57:49.495512009 CET	49687	443	192.168.2.3	23.35.237.194
Nov 19, 2022 16:57:49.496159077 CET	49688	80	192.168.2.3	93.184.220.29
Nov 19, 2022 16:57:49.800894022 CET	49689	443	192.168.2.3	23.50.106.206
Nov 19, 2022 16:57:49.845913887 CET	443	49689	23.50.106.206	192.168.2.3
Nov 19, 2022 16:57:49.845969915 CET	443	49689	23.50.106.206	192.168.2.3
Nov 19, 2022 16:57:49.846116066 CET	49689	443	192.168.2.3	23.50.106.206
Nov 19, 2022 16:57:49.846200943 CET	49689	443	192.168.2.3	23.50.106.206
Nov 19, 2022 16:57:50.009917021 CET	49691	80	192.168.2.3	8.241.126.249
Nov 19, 2022 16:57:50.011009932 CET	49690	443	192.168.2.3	204.79.197.200
Nov 19, 2022 16:57:50.011015892 CET	49683	80	192.168.2.3	93.184.220.29
Nov 19, 2022 16:57:50.644383907 CET	49693	80	192.168.2.3	93.184.220.29
Nov 19, 2022 16:57:50.644514084 CET	49692	80	192.168.2.3	8.248.147.254
Nov 19, 2022 16:57:50.644565105 CET	49694	80	192.168.2.3	173.222.108.226
Nov 19, 2022 16:57:50.644644976 CET	49695	80	192.168.2.3	8.248.147.254

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2022 16:57:50.644901037 CET	49696	80	192.168.2.3	93.184.221.240
Nov 19, 2022 16:57:50.656058073 CET	80	49694	173.222.108.226	192.168.2.3
Nov 19, 2022 16:57:50.656167030 CET	49694	80	192.168.2.3	173.222.108.226
Nov 19, 2022 16:57:50.664350986 CET	80	49693	93.184.220.29	192.168.2.3
Nov 19, 2022 16:57:50.664375067 CET	80	49696	93.184.221.240	192.168.2.3
Nov 19, 2022 16:57:50.664437056 CET	49693	80	192.168.2.3	93.184.220.29
Nov 19, 2022 16:57:50.664479017 CET	49696	80	192.168.2.3	93.184.221.240
Nov 19, 2022 16:57:50.668303967 CET	80	49692	8.248.147.254	192.168.2.3
Nov 19, 2022 16:57:50.668392897 CET	49692	80	192.168.2.3	8.248.147.254
Nov 19, 2022 16:57:50.678309917 CET	80	49695	8.248.147.254	192.168.2.3
Nov 19, 2022 16:57:50.678441048 CET	49695	80	192.168.2.3	8.248.147.254
Nov 19, 2022 16:58:01.455888987 CET	49700	80	192.168.2.3	77.232.37.228
Nov 19, 2022 16:58:01.522022009 CET	80	49700	77.232.37.228	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 19, 2022 16:58:01.160134077 CET	192.168.2.3	8.8.8.8	0x612	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:01.919708014 CET	192.168.2.3	8.8.8.8	0x2dc1	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:02.407712936 CET	192.168.2.3	8.8.8.8	0x831b	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:02.568012953 CET	192.168.2.3	8.8.8.8	0x7f71	Standard query (0)	srshf.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:03.491904974 CET	192.168.2.3	8.8.8.8	0xe145	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:03.984349966 CET	192.168.2.3	8.8.8.8	0xd0c3	Standard query (0)	iplogger.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:04.147842884 CET	192.168.2.3	8.8.8.8	0xe423	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:04.567305088 CET	192.168.2.3	8.8.8.8	0x1d8c	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:04.728820086 CET	192.168.2.3	8.8.8.8	0xf26c	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:04.891732931 CET	192.168.2.3	8.8.8.8	0xcd2	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:05.062556028 CET	192.168.2.3	8.8.8.8	0xd03b	Standard query (0)	1ecosolution.it	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:13.176884890 CET	192.168.2.3	8.8.8.8	0x82cc	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:13.590037107 CET	192.168.2.3	8.8.8.8	0x2b18	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:13.755465031 CET	192.168.2.3	8.8.8.8	0x5033	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:14.192063093 CET	192.168.2.3	8.8.8.8	0x5938	Standard query (0)	cdn-102.anonfiles.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:17.774099112 CET	192.168.2.3	8.8.8.8	0xc05a	Standard query (0)	anonfiles.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:17.997459888 CET	192.168.2.3	8.8.8.8	0x3a04	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:18.159235954 CET	192.168.2.3	8.8.8.8	0xb498	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:19.462356091 CET	192.168.2.3	8.8.8.8	0x34f8	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:19.622137070 CET	192.168.2.3	8.8.8.8	0x9f0e	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:19.784775019 CET	192.168.2.3	8.8.8.8	0xe54f	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:19.948282003 CET	192.168.2.3	8.8.8.8	0x6473	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:23.004631996 CET	192.168.2.3	8.8.8.8	0xbe99	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:23.176175117 CET	192.168.2.3	8.8.8.8	0xced9	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:23.339287043 CET	192.168.2.3	8.8.8.8	0x1631	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 19, 2022 16:58:23.508014917 CET	192.168.2.3	8.8.8.8	0xbf2c	Standard query (0)	hoteldostyk.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:32.394125938 CET	192.168.2.3	8.8.8.8	0xdc9f	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:32.553194046 CET	192.168.2.3	8.8.8.8	0x2f4f	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:32.742621899 CET	192.168.2.3	8.8.8.8	0x19a9	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:34.758660078 CET	192.168.2.3	8.8.8.8	0x353c	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:34.962809086 CET	192.168.2.3	8.8.8.8	0x6752	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:35.193367004 CET	192.168.2.3	8.8.8.8	0xa1ec	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:35.406321049 CET	192.168.2.3	8.8.8.8	0x9818	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:35.570811033 CET	192.168.2.3	8.8.8.8	0xfa0f	Standard query (0)	github.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:35.680458069 CET	192.168.2.3	8.8.8.8	0x26c7	Standard query (0)	raw.githubusercontent.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:36.569705963 CET	192.168.2.3	8.8.8.8	0x7fe0	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:36.733948946 CET	192.168.2.3	8.8.8.8	0x5716	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:36.897253990 CET	192.168.2.3	8.8.8.8	0x8ea9	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:37.078887939 CET	192.168.2.3	8.8.8.8	0x2e50	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:37.255276918 CET	192.168.2.3	8.8.8.8	0xe432	Standard query (0)	bitbucket.org	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:37.858977079 CET	192.168.2.3	8.8.8.8	0xbcb5	Standard query (0)	bbuseruploads.s3.amazonaws.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:40.124414921 CET	192.168.2.3	8.8.8.8	0xaca	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:45.903089046 CET	192.168.2.3	8.8.8.8	0x71c3	Standard query (0)	t.me	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:59:12.424742937 CET	192.168.2.3	8.8.8.8	0x1728	Standard query (0)	2w3ke1f81kujb1erhj396kfejh2wgw.kgpoaj9k4sgjd4aitghsrtuxhq	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:59:31.145158052 CET	192.168.2.3	8.8.8.8	0x6676	Standard query (0)	www.youtube.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:59:46.107234955 CET	192.168.2.3	8.8.8.8	0x3551	Standard query (0)	lentaphoto.at	A (IP address)	IN (0x0001)	false
Nov 19, 2022 17:01:06.986499071 CET	192.168.2.3	8.8.8.8	0x127d	Standard query (0)	iujdhsndjfks.ru	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
Nov 19, 2022 16:58:01.452234030 CET	8.8.8.8	192.168.2.3	0x612	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:02.261224031 CET	8.8.8.8	192.168.2.3	0x2dc1	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:02.427973986 CET	8.8.8.8	192.168.2.3	0x831b	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:02.741633892 CET	8.8.8.8	192.168.2.3	0x7f71	No error (0)	srshf.com		108.167.141.212	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:03.841243029 CET	8.8.8.8	192.168.2.3	0xe145	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:04.001168013 CET	8.8.8.8	192.168.2.3	0xd0c3	No error (0)	iplogger.com		148.251.234.93	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 19, 2022 16:58:04.424365997 CET	8.8.8.8	192.168.2.3	0xe423	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:04.584631920 CET	8.8.8.8	192.168.2.3	0x1d8c	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:04.746968031 CET	8.8.8.8	192.168.2.3	0xf26c	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:04.911199093 CET	8.8.8.8	192.168.2.3	0xcd2	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:05.103020906 CET	8.8.8.8	192.168.2.3	0xd03b	No error (0)	1ecosolution.it		46.252.148.24	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:13.446790934 CET	8.8.8.8	192.168.2.3	0x82cc	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:13.607109070 CET	8.8.8.8	192.168.2.3	0x2b18	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:14.050710917 CET	8.8.8.8	192.168.2.3	0x5033	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:14.606645107 CET	8.8.8.8	192.168.2.3	0x5938	No error (0)	cdn-102.anonfiles.com		195.96.151.51	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:17.792520046 CET	8.8.8.8	192.168.2.3	0xc05a	No error (0)	anonfiles.com		45.154.253.151	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:17.792520046 CET	8.8.8.8	192.168.2.3	0xc05a	No error (0)	anonfiles.com		45.154.253.150	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:17.792520046 CET	8.8.8.8	192.168.2.3	0xc05a	No error (0)	anonfiles.com		45.154.253.152	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:18.014646053 CET	8.8.8.8	192.168.2.3	0x3a04	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:18.192998886 CET	8.8.8.8	192.168.2.3	0xb498	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:19.481662035 CET	8.8.8.8	192.168.2.3	0x34f8	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:19.641381025 CET	8.8.8.8	192.168.2.3	0x9f0e	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:19.803828001 CET	8.8.8.8	192.168.2.3	0xe54f	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:19.966825008 CET	8.8.8.8	192.168.2.3	0x6473	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:23.021636963 CET	8.8.8.8	192.168.2.3	0xbe99	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:23.193491936 CET	8.8.8.8	192.168.2.3	0xced9	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:23.358150005 CET	8.8.8.8	192.168.2.3	0x1631	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:23.749830961 CET	8.8.8.8	192.168.2.3	0xbf2c	No error (0)	hoteldostyk.com		43.231.112.109	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:32.411025047 CET	8.8.8.8	192.168.2.3	0xdc9f	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:32.572393894 CET	8.8.8.8	192.168.2.3	0x2f4f	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:32.761758089 CET	8.8.8.8	192.168.2.3	0x19a9	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 19, 2022 16:58:34.777826071 CET	8.8.8.8	192.168.2.3	0x353c	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:34.982450008 CET	8.8.8.8	192.168.2.3	0x6752	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:35.212619066 CET	8.8.8.8	192.168.2.3	0xa1ec	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:35.423413038 CET	8.8.8.8	192.168.2.3	0x9818	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:35.594837904 CET	8.8.8.8	192.168.2.3	0xfa0f	No error (0)	github.com		140.82.121.4	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:35.700153112 CET	8.8.8.8	192.168.2.3	0x26c7	No error (0)	raw.githubusercontent.com		185.199.108.133	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:35.700153112 CET	8.8.8.8	192.168.2.3	0x26c7	No error (0)	raw.githubusercontent.com		185.199.111.133	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:35.700153112 CET	8.8.8.8	192.168.2.3	0x26c7	No error (0)	raw.githubusercontent.com		185.199.109.133	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:35.700153112 CET	8.8.8.8	192.168.2.3	0x26c7	No error (0)	raw.githubusercontent.com		185.199.110.133	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:36.588682890 CET	8.8.8.8	192.168.2.3	0x7fe0	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:36.752307892 CET	8.8.8.8	192.168.2.3	0x5716	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:36.915503025 CET	8.8.8.8	192.168.2.3	0x8ea9	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:37.099838018 CET	8.8.8.8	192.168.2.3	0x2e50	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:37.275063992 CET	8.8.8.8	192.168.2.3	0xe432	No error (0)	bitbucket.org		104.192.141.1	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:37.876419067 CET	8.8.8.8	192.168.2.3	0xbcb5	No error (0)	bbuseruploads.s3.amazonaws.com	s3-1-w.amazonaws.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 19, 2022 16:58:37.876419067 CET	8.8.8.8	192.168.2.3	0xbcb5	No error (0)	s3-1-w.amazonaws.com	s3-w.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 19, 2022 16:58:37.876419067 CET	8.8.8.8	192.168.2.3	0xbcb5	No error (0)	s3-w.us-east-1.amazonaws.com		3.5.21.195	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:37.876419067 CET	8.8.8.8	192.168.2.3	0xbcb5	No error (0)	s3-w.us-east-1.amazonaws.com		52.216.177.187	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:37.876419067 CET	8.8.8.8	192.168.2.3	0xbcb5	No error (0)	s3-w.us-east-1.amazonaws.com		52.216.92.75	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:37.876419067 CET	8.8.8.8	192.168.2.3	0xbcb5	No error (0)	s3-w.us-east-1.amazonaws.com		52.217.99.44	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:37.876419067 CET	8.8.8.8	192.168.2.3	0xbcb5	No error (0)	s3-w.us-east-1.amazonaws.com		52.216.220.65	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:37.876419067 CET	8.8.8.8	192.168.2.3	0xbcb5	No error (0)	s3-w.us-east-1.amazonaws.com		52.216.25.68	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:37.876419067 CET	8.8.8.8	192.168.2.3	0xbcb5	No error (0)	s3-w.us-east-1.amazonaws.com		52.217.174.25	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:37.876419067 CET	8.8.8.8	192.168.2.3	0xbcb5	No error (0)	s3-w.us-east-1.amazonaws.com		52.216.35.241	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:58:40.144412041 CET	8.8.8.8	192.168.2.3	0xaca	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 19, 2022 16:58:45.921497107 CET	8.8.8.8	192.168.2.3	0x71c3	No error (0)	t.me		149.154.167.99	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:59:12.443828106 CET	8.8.8.8	192.168.2.3	0x1728	Name error (3)	2w3ke1f81kujb1erhj396kfejh2wgw.kgpoaj9k4sgjd4aitghsrtuxhq	none	none	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:59:31.164213896 CET	8.8.8.8	192.168.2.3	0x6676	No error (0)	www.youtube.com	youtube-ui.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 19, 2022 16:59:31.164213896 CET	8.8.8.8	192.168.2.3	0x6676	No error (0)	youtube-ui.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:59:31.164213896 CET	8.8.8.8	192.168.2.3	0x6676	No error (0)	youtube-ui.l.google.com		172.217.168.14	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:59:31.164213896 CET	8.8.8.8	192.168.2.3	0x6676	No error (0)	youtube-ui.l.google.com		172.217.168.46	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:59:31.164213896 CET	8.8.8.8	192.168.2.3	0x6676	No error (0)	youtube-ui.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Nov 19, 2022 16:59:46.472574949 CET	8.8.8.8	192.168.2.3	0x3551	Server failure (2)	lentaphoto.at	none	none	A (IP address)	IN (0x0001)	false
Nov 19, 2022 17:01:07.054994106 CET	8.8.8.8	192.168.2.3	0x127d	No error (0)	iujdhsndjfks.ru		134.0.118.203	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

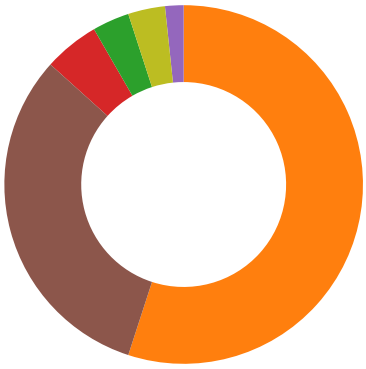
- fs.microsoft.com
- https:
  - www.bing.com
- srshf.com
- iplogger.com
- cdn-102.anonfiles.com
- anonfiles.com
- transfer.sh
- hoteldostyk.com
- github.com
- raw.githubusercontent.com
- bitbucket.org
- bbuseruploads.s3.amazonaws.com
- t.me
- www.youtube.com
- login.live.com
- watson.telemetry.microsoft.com

- ijksciexii.com
  - o36fafs3sn6xou.com
- bpbdsdk.net
- umixvvejem.com
- qqfarpecak.com
- oorjfnwj.net
- awjddgg.com
- vewejolrw.net
- ttvgdova.com
- ujapeckwwf.net
- llobgypg.org
- bqrca.net
- vovqsb.net
- xqiywpnnx.com
- 193.56.146.168
- hebuwvwfs.net
- kjwivofpbv.net
- uflscskn.org
- wnamt.org
- pbxlqwo.com
- hpnwth.net
- uilamexewu.net
- xqqjug.org
- eewqpkgoat.org
- ipmxouwmp.com
- pccxxtjnt.com
- dygmllr.com
- mwcxqjbc.com
- pmgurxcfse.com
- anhnwnhtgc.net

- xqculhri.net
- lruucyh.com
- 193.56.146.174
- 116.202.5.101
- 65.21.213.208:3000
- iujdhsndjfks.ru

Statistics

Behavior



- q4Z52wRd28.exe
- explorer.exe
- cttgcew
- A852.exe
- B4A7.exe
- rovwer.exe
- CF35.exe
- schtasks.exe
- conhost.exe
- cmd.exe
- conhost.exe
- cmd.exe
- cacls.exe
- E35A.exe
- cacls.exe
- rovwer.exe
- cmd.exe
- EB2B.exe
- cacls.exe
- cacls.exe
- EB2B.exe
- F771.exe
- explorer.exe
- explorer.exe
- explorer.exe
- EB2B.exe
- explorer.exe
- explorer.exe
- explorer.exe
- rundll32.exe
- explorer.exe
- explorer.exe
- explorer.exe
- cmd.exe
- conhost.exe
- timeout.exe
- RegSvcs.exe

Click to jump to process

System Behavior

Analysis Process: q4Z52wRd28.exe PID: **5708**, Parent PID: **3452**

General

Target ID:	0
Start time:	16:57:03
Start date:	19/11/2022

Path:	C:\Users\user\Desktop\q4Z52wRd28.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\q4Z52wRd28.exe
Imagebase:	0x400000
File size:	346112 bytes
MD5 hash:	A687E1C326C9F03569BBFEF53E21C315
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: 00000000.00000003.256917988.0000000000970000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.340457364.0000000000960000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.340559376.000000000A00000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.340559376.000000000A00000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.340166873.0000000000871000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.340651575.000000000C11000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.340651575.000000000C11000.00000004.10000000.00040000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: explorer.exe PID: **3452**, Parent PID: **5708**

General

Target ID:	1
Start time:	16:57:13
Start date:	19/11/2022
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
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000001.00000000.327872359.0000000003851000.00000020.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000001.00000000.327872359.0000000003851000.00000020.80000000.00040000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

Analysis Process: cttgcew PID: **4220**, Parent PID: **1080**

General

Target ID:	11
Start time:	16:58:02
Start date:	19/11/2022
Path:	C:\Users\user\AppData\Roaming\cttgcew
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\cttgcew
Imagebase:	0x400000
File size:	346112 bytes
MD5 hash:	A687E1C326C9F03569BBFEF53E21C315
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000B.00000002.393943988.00000000025E1000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000000B.00000002.393943988.00000000025E1000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000B.00000002.393477736.0000000000880000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000000B.00000002.393477736.0000000000880000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000B.00000003.381680800.0000000000870000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000B.00000002.393611577.00000000008D1000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 0000000B.00000002.393447143.0000000000860000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 27%, ReversingLabs
Reputation:	low

Analysis Process: A852.exe PID: **6000**, Parent PID: **3452**

General

Target ID:	12
Start time:	16:58:19
Start date:	19/11/2022
Path:	C:\Users\user\AppData\Local\Temp\A852.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\A852.exe
Imagebase:	0x400000
File size:	385536 bytes
MD5 hash:	0E455D9C65E7D53A67C227DCD8D70FB8
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000C.00000002.424634553.0000000000891000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 0000000C.00000002.428145666.00000000009B0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\99e342142d	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40B643	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\99e342142d\rovwer.exe	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	40B78F	CopyFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\99e342142d\rovwer.exe	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 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 50 16 fd fd 31 78 a1 31 78 a1 31 78 bf 63 fd b5 31 78 bf 63 fd fd 21 31 78 bf 63 fd 8f 31 78 86 fd 03 a2 31 78 a1 31 79 fd fd 31 78 bf 63 fd a0 31 78 bf 63 fd a0 31 78 bf 63 fd a0 31 78 fd 52 69 63 68 fd 31 78 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd fd 61 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$P1x1x1xc1xc!1xc1x1x1y1xc1xc1xc1xRich1xPELa	success or wait	3	40B78F	CopyFileA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: B4A7.exe PID: **3080**, Parent PID: **3452**

General

Target ID:	13
Start time:	16:58:22
Start date:	19/11/2022
Path:	C:\Users\user\AppData\Local\Temp\B4A7.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\B4A7.exe
Imagebase:	0x400000
File size:	1235912 bytes
MD5 hash:	F96144B1D5B53D93CAADDDADE38DB5E9
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: 0000000D.00000003.542369400.000000000070F000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000D.00000003.527908931.000000000D290000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 0000000D.00000003.527908931.000000000D290000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: SUSP_XORed_MSDOS_Stub_Message, Description: Detects suspicious XORed MSDOS stub message, Source: 0000000D.00000003.501276183.00000000024E6000.00000040.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000D.00000003.533006922.000000000D292000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000D.00000003.541178072.0000000000701000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000D.00000002.562231967.0000000000714000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 21%, ReversingLabs
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rovwer.exe PID: **4852**, Parent PID: **6000**

General

Target ID:	14
Start time:	16:58:24
Start date:	19/11/2022
Path:	C:\Users\user\AppData\Local\Temp\99e342142d\rovwer.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\99e342142d\rovwer.exe"
Imagebase:	0x400000
File size:	385536 bytes
MD5 hash:	0E455D9C65E7D53A67C227DCD8D70FB8
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Amadey, Description: Yara detected Amadey bot, Source: 0000000E.00000002.806199493.0000000000B07000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey, Description: Yara detected Amadey bot, Source: 0000000E.00000002.793487100.0000000000A81000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 0000000E.00000002.793487100.0000000000A81000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey, Description: Yara detected Amadey bot, Source: 0000000E.00000002.805707000.0000000000B01000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 0000000E.00000002.778202209.0000000000870000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000E.00000002.787937568.0000000000A41000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Amadey, Description: Yara detected Amadey bot, Source: 0000000E.00000003.603169508.0000000000AFF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\a091ec0a6e2227	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4118DC	CreateDirectoryA
C:\Users\user\AppData\Roaming\a091ec0a6e2227\cred64.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	408BB2	CreateFileA
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	409D80	HttpSendRequestA
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	409D80	HttpSendRequestA
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	409D80	HttpSendRequestA
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	409D80	HttpSendRequestA

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	409D80	HttpSendRequestA
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	409D80	HttpSendRequestA
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	409D80	HttpSendRequestA
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	409D80	HttpSendRequestA
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	409D80	HttpSendRequestA
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	409D80	HttpSendRequestA
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	409D80	HttpSendRequestA
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	409D80	HttpSendRequestA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\853321935212	success or wait	11	41F5C3	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\a091ec0a6e2227\cred64.dll	0	16384	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	8	408C17	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\cred64[1].dll	16384	16384	fd fd fd fd fd cb 03 fd fd 74 10 fd fd fd 48 fd 39 fd 7c 02 fd fd fd 5b fd fd fd fd fd fd fd fd fd fd fd 3b 5f 5e 5b cb fd fd 53 56 51 fd fd 0b fd 33 4b fd fd 0a 00 00 00 fd 04 24 fd 04 24 5a 5e 5b fd 53 fd c9 fd 31 45 fd 74 05 fd 4b fd 29 fd 51 fd 16 fd fd fd 59 fd fd 5b fd fd fd fd f0 01 fd 5d fd fd fd c5 fd 74 10 50 6a 00 fd 04 fd fd fd fd 0f fd fd fd fd fd cd 40 00 fd 10 fd fd 74 06 52 fd fd fd fd fd cd 40 00 fd 10 fd fd 74 0e fd 00 00 00 00 00 50 52 fd fd fd fd fd 58 cd 40 00 53 56 fd c9 8b 03 fd fd 74 0c fd 03 00 00 00 00 50 fd fd fd fd fd fd fd 04 4e 75 fd 5e 5b cd 40 00 fd fd 0f fd fd fd fd fd fd 4a fd fd fd 0f fd fd fd fd fd 51 52 50 fd fd fd fd fd fd 0f fd 71 fd fd fd fd 53 56 57 55 fd fd 04	tH9| [;_^[SVQ3$$Z^[S1tK)QY[ ]tPj @tR@tPRX@SVtPNu^[@JQRPqSVWU	success or wait	5	408C26	InternetReadFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\853321935212	unknown	4	success or wait	99400	409747	ReadFile

Registry Activities

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders	Startup	expand unicode	%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	C:\Users\user\AppData\Local\Temp\99e342142d\	success or wait	1	402F97	RegSetValueExA

Analysis Process: CF35.exe PID: 4392, Parent PID: 3452

General

Target ID:	17

Start time:	16:58:29
Start date:	19/11/2022
Path:	C:\Users\user\AppData\Local\Temp\CF35.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\CF35.exe
Imagebase:	0x7ff74f320000
File size:	3188224 bytes
MD5 hash:	44A7E13ECC55CE9797C5121B230D9927
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 23%, ReversingLabs
Reputation:	low

Analysis Process: schtasks.exe PID: **2384**, Parent PID: **4852**

General

Target ID:	18
Start time:	16:58:32
Start date:	19/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\schtasks.exe" /Create /SC MINUTE /MO 1 /TN rovwer.exe /TR "C:\Users\user\AppData\Local\Temp\99e342142d\rovwer.exe" /F
Imagebase:	0xea0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **2364**, Parent PID: **2384**

General

Target ID:	19
Start time:	16:58:33
Start date:	19/11/2022
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
Reputation:	high

Analysis Process: cmd.exe PID: **6140**, Parent PID: **4852**

General	
Target ID:	20
Start time:	16:58:33
Start date:	19/11/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /k echo Y|CACLS "rovwer.exe" /P "user:N"&&CACLS "rovwer.exe" /P "user:R" /E&&echo Y|CACLS "..\99e342142d" /P "user:N"&&CACLS "..\99e342142d" /P "user:R" /E&&Exit
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 2820, Parent PID: 6140

General	
Target ID:	21
Start time:	16:58:33
Start date:	19/11/2022
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
Reputation:	high

Analysis Process: cmd.exe PID: 68, Parent PID: 6140

General	
Target ID:	22
Start time:	16:58:33
Start date:	19/11/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /S /D /c" echo Y"
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cacls.exe PID: **2016**, Parent PID: **6140**

General

Target ID:	23
Start time:	16:58:33
Start date:	19/11/2022
Path:	C:\Windows\SysWOW64\cacls.exe
Wow64 process (32bit):	true
Commandline:	CACLS "rovwer.exe" /P "user:N"
Imagebase:	0xb80000
File size:	27648 bytes
MD5 hash:	4CBB1C027DF71C53A8EE4C855FD35B25
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	1	1	72	r	success or wait	19	B849CC	fprintf
\Device\ConDrv	20	1	72	r	success or wait	16	B849CC	fprintf

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: E35A.exe PID: **4252**, Parent PID: **3452**

General

Target ID:	24
Start time:	16:58:34
Start date:	19/11/2022
Path:	C:\Users\user\AppData\Local\Temp\E35A.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\E35A.exe
Imagebase:	0x400000
File size:	342528 bytes
MD5 hash:	19A79DADDFAAC09499E79ADE27E756F8
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000018.00000003.726670268.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000018.00000003.726670268.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000018.00000003.726670268.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000018.00000002.792008341.0000000000870000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000018.00000003.726853910.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000018.00000003.726853910.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000018.00000003.726853910.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000018.00000003.726739723.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000018.00000003.726739723.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000018.00000003.726739723.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000018.00000003.726364142.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000018.00000003.726364142.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000018.00000003.726364142.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000018.00000003.726589987.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000018.00000003.726589987.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000018.00000003.726589987.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000018.00000002.816564354.0000000001209000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000018.00000003.726819052.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000018.00000003.726819052.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000018.00000003.726819052.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000018.00000002.819270273.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000018.00000002.819270273.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000018.00000002.819270273.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000018.00000002.797855651.00000000008D1000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000018.00000003.726009668.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000018.00000003.726009668.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000018.00000003.726009668.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000018.00000003.726197587.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000018.00000003.726197587.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000018.00000003.726197587.00000000017A8000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 38%, ReversingLabs

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cacls.exe PID: **5168**, Parent PID: **6140**

General

Target ID:	25
Start time:	16:58:34
Start date:	19/11/2022
Path:	C:\Windows\SysWOW64\cacls.exe
Wow64 process (32bit):	true
Commandline:	CACLS "rovwer.exe" /P "user:R" /E

Imagebase:	0xb80000
File size:	27648 bytes
MD5 hash:	4CBB1C027DF71C53A8EE4C855FD35B25
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	1	1	72	r	success or wait	16	B849CC	fprintf

Analysis Process: rovwer.exe PID: **5372**, Parent PID: **1080**

General

Target ID:	26
Start time:	16:58:35
Start date:	19/11/2022
Path:	C:\Users\user\AppData\Local\Temp\99e342142d\rovwer.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\99e342142d\rovwer.exe
Imagebase:	0x400000
File size:	385536 bytes
MD5 hash:	0E455D9C65E7D53A67C227DCD8D70FB8
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000001A.00000002.597295606.0000000000934000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 0000001A.00000002.593292685.0000000000870000.00000040.00001000.00020000.00000000.sdmp, Author: unknown

Analysis Process: cmd.exe PID: **5444**, Parent PID: **6140**

General

Target ID:	27
Start time:	16:58:36
Start date:	19/11/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\system32\cmd.exe /S /D /c" echo Y"
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: EB2B.exe PID: **5512**, Parent PID: **3452**

General	
Target ID:	28
Start time:	16:58:36
Start date:	19/11/2022
Path:	C:\Users\user\AppData\Local\Temp\EB2B.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\EB2B.exe
Imagebase:	0xc40000
File size:	341006 bytes
MD5 hash:	F46063253FF38E6B2452BF4410C5FEC0
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000001C.00000002.454935093.0000000000B40000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 27%, ReversingLabs

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cacls.exe PID: **5484**, Parent PID: **6140**

General	
Target ID:	29
Start time:	16:58:37
Start date:	19/11/2022
Path:	C:\Windows\SysWOW64\cacls.exe
Wow64 process (32bit):	true
Commandline:	CACLS "..\99e342142d" /P "user:N"
Imagebase:	0xb80000
File size:	27648 bytes
MD5 hash:	4CBB1C027DF71C53A8EE4C855FD35B25
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	1	1	72	r	success or wait	19	B849CC	fprintf
\Device\ConDrv	20	1	72	r	success or wait	15	B849CC	fprintf

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cacls.exe PID: **5608**, Parent PID: **6140**

General	
Target ID:	30
Start time:	16:58:38
Start date:	19/11/2022

Path:	C:\Windows\SysWOW64\cacls.exe
Wow64 process (32bit):	true
Commandline:	CACLS "..\99e342142d" /P "user:R" /E
Imagebase:	0xb80000
File size:	27648 bytes
MD5 hash:	4CBB1C027DF71C53A8EE4C855FD35B25
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: EB2B.exe PID: **5628**, Parent PID: **5512**

General

Target ID:	31
Start time:	16:58:39
Start date:	19/11/2022
Path:	C:\Users\user\AppData\Local\Temp\EB2B.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\EB2B.exe
Imagebase:	0xc40000
File size:	341006 bytes
MD5 hash:	F46063253FF38E6B2452BF4410C5FEC0
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 0000001F.00000002.471247692.0000000000C50000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: F771.exe PID: **5640**, Parent PID: **3452**

General

Target ID:	32
Start time:	16:58:39
Start date:	19/11/2022
Path:	C:\Users\user\AppData\Local\Temp\F771.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\F771.exe
Imagebase:	0x400000
File size:	459264 bytes
MD5 hash:	DF920AEBFABB8C4CCCEB4DCEAD922ABD
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: 00000020.00000002.791144627.0000000000880000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000020.00000002.791144627.0000000000880000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000020.00000002.848936854.000000000263A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000020.00000003.463369544.00000000008C0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000020.00000003.463369544.00000000008C0000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000020.00000003.466345682.00000000009C6000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000020.00000002.850270333.00000000027A0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000020.00000002.850270333.00000000027A0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000020.00000002.775109103.0000000000400000.00000040.00000001.01000000.0000000F.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 00000020.00000002.775109103.0000000000400000.00000040.00000001.01000000.0000000F.sdmp, Author: ditekSHen • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000020.00000002.853522237.0000000002B2B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000020.00000002.806650961.0000000000951000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Analysis Process: explorer.exe PID: **5644**, Parent PID: **3452**

General

Target ID:	33
Start time:	16:58:40
Start date:	19/11/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xf80000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000021.00000000.456333193.0000000000540000.00000040.80000000.00040000.00000000.sdmp, Author: unknown

Analysis Process: explorer.exe PID: **5656**, Parent PID: **3452**

General

Target ID:	34
Start time:	16:58:42
Start date:	19/11/2022
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

Analysis Process: explorer.exe PID: **5816**, Parent PID: **3452**

General

Target ID:	35
Start time:	16:58:43

Start date:	19/11/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xf80000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000023.00000000.462429473.0000000000120000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader, Description: Yara detected SmokeLoader, Source: 00000023.00000002.773922476.0000000000111000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security

Analysis Process: EB2B.exe PID: **5828**, Parent PID: **5628**

General

Target ID:	36
Start time:	16:58:43
Start date:	19/11/2022
Path:	C:\Users\user\AppData\Local\Temp\EB2B.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\EB2B.exe
Imagebase:	0xc40000
File size:	341006 bytes
MD5 hash:	F46063253FF38E6B2452BF4410C5FEC0
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000024.00000002.522046166.000000000127B000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000024.00000002.519975927.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: explorer.exe PID: **5876**, Parent PID: **3452**

General

Target ID:	37
Start time:	16:58:44
Start date:	19/11/2022
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
Yara matches:	• Rule: JoeSecurity_SmokeLoader, Description: Yara detected SmokeLoader, Source: 00000025.00000002.770728847.0000000000131000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security

Analysis Process: explorer.exe PID: **5068**, Parent PID: **3452**

General

Target ID:	38
Start time:	16:58:46

Start date:	19/11/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xf80000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000026.00000000.469133580.0000000000B80000.00000040.80000000.00040000.00000000.sdmp, Author: unknown

Analysis Process: explorer.exe PID: **3932**, Parent PID: **3452**

General

Target ID:	39
Start time:	16:58:48
Start date:	19/11/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xf80000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000027.00000000.474180010.0000000000900000.00000040.80000000.00040000.00000000.sdmp, Author: unknown

Analysis Process: rundll32.exe PID: **4964**, Parent PID: **4852**

General

Target ID:	40
Start time:	16:58:50
Start date:	19/11/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\rundll32.exe" C:\Users\user\AppData\Roaming\a091ec0a6e2227\cred64.dll, Main
Imagebase:	0xe20000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi

Analysis Process: explorer.exe PID: **408**, Parent PID: **3452**

General

Target ID:	41
Start time:	16:58:50
Start date:	19/11/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xf80000

File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000029.00000000.476884087.0000000000A70000.00000040.80000000.00040000.00000000.sdmp, Author: unknown

Analysis Process: explorer.exe PID: **4972**, Parent PID: **3452**

General

Target ID:	42
Start time:	16:58:51
Start date:	19/11/2022
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

Analysis Process: explorer.exe PID: **5248**, Parent PID: **3452**

General

Target ID:	43
Start time:	16:58:52
Start date:	19/11/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xf80000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000002B.00000000.482523463.0000000000650000.00000040.80000000.00040000.00000000.sdmp, Author: unknown

Analysis Process: cmd.exe PID: **1852**, Parent PID: **5828**

General

Target ID:	44
Start time:	16:59:09
Start date:	19/11/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 6 & del /f /q "C:\Users\user\AppData\Local\Temp\EB2B.exe" & exit
Imagebase:	0xb0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5944**, Parent PID: **1852**

General	
Target ID:	45
Start time:	16:59:10
Start date:	19/11/2022
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: timeout.exe PID: **5980**, Parent PID: **1852**

General	
Target ID:	46
Start time:	16:59:11
Start date:	19/11/2022
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 6
Imagebase:	0x20000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: RegSvcs.exe PID: **5128**, Parent PID: **4392**

General	
Target ID:	47
Start time:	16:59:14
Start date:	19/11/2022
Path:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\RegSvcs.exe
Imagebase:	0x2adbfe50000
File size:	44640 bytes
MD5 hash:	59FCE79E9D81AB9E2ED4C3561205F5DF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GoStealer, Description: Yara detected Go Stealer, Source: 0000002F.00000002.570733528.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security

Disassembly

No disassembly