ID: 749806
Sample Name:
S2XJ2wbz7u.exe
Cookbook: default.jbs
Time: 10:36:06
Date: 19/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

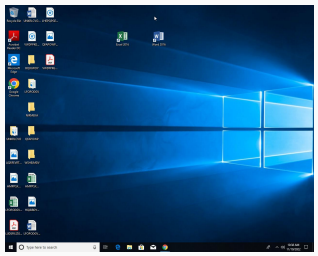
Windows Analysis Report

S2XJ2wbz7u.exe

Overview

General Information

Sample Name:	S2XJ2wbz7u.exe
Analysis ID:	749806
MD5:	ffb4cf34b38f126…
SHA1:	36e558fdb10418..
SHA256:	4a47fdbb09dd09..
Tags:	exe RedLineStealer
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

Ursnif, Amadey, RedLine, SmokeLoader, Vidar

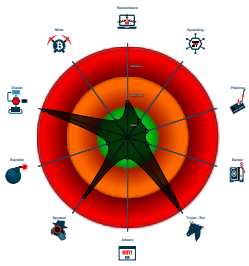
Score:

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

Signatures

- Yara detected RedLine Stealer
- Yara detected Amadeys stealer DLL
- Detected unpacking (overwrites its o…
- Yara detected 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
- Benign windows process drops PE f…

Classification



Process Tree

- **System is w10x64**
- S2XJ2wbz7u.exe (PID: 6020 cmdline: C:\Users\user\Desktop\S2XJ2wbz7u.exe MD5: FFB4CF34B38F126C917E1C1E1D26DF73)
  - explorer.exe (PID: 3452 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - 2B4A.exe (PID: 5260 cmdline: C:\Users\user\AppData\Local\Temp\2B4A.exe MD5: 2DEE200193091BE2F2321D921750C4ED)
    - 3790.exe (PID: 2336 cmdline: C:\Users\user\AppData\Local\Temp\3790.exe MD5: 5E08968D858224A33175069D64DC7F39)
      - rovwer.exe (PID: 4764 cmdline: "C:\Users\user\AppData\Local\Temp\99e342142d\rovwer.exe" MD5: 5E08968D858224A33175069D64DC7F39)
        - schtasks.exe (PID: 1396 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: 2992 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - cmd.exe (PID: 5972 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: 2436 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - cmd.exe (PID: 3012 cmdline: C:\Windows\system32\cmd.exe /S /D /c" echo Y" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - cacls.exe (PID: 4392 cmdline: CACLS "rovwer.exe" /P "user:N" MD5: 4CBB1C027DF71C53A8EE4C855FD35B25)
          - cacls.exe (PID: 4984 cmdline: CACLS "rovwer.exe" /P "user:R" /E MD5: 4CBB1C027DF71C53A8EE4C855FD35B25)
          - cmd.exe (PID: 5640 cmdline: C:\Windows\system32\cmd.exe /S /D /c" echo Y" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - cacls.exe (PID: 5668 cmdline: CACLS "..\99e342142d" /P "user:N" MD5: 4CBB1C027DF71C53A8EE4C855FD35B25)
          - cacls.exe (PID: 3124 cmdline: CACLS "..\99e342142d" /P "user:R" /E MD5: 4CBB1C027DF71C53A8EE4C855FD35B25)
    - 453D.exe (PID: 4024 cmdline: C:\Users\user\AppData\Local\Temp\453D.exe MD5: F96144B1D5B53D93CAADDDADE38DB5E9)
    - 59FE.exe (PID: 5228 cmdline: C:\Users\user\AppData\Local\Temp\59FE.exe MD5: 44A7E13ECC55CE9797C5121B230D9927)
    - 6644.exe (PID: 1916 cmdline: C:\Users\user\AppData\Local\Temp\6644.exe MD5: 19A79DADDFAAC09499E79ADE27E756F8)
    - 6CEC.exe (PID: 4968 cmdline: C:\Users\user\AppData\Local\Temp\6CEC.exe MD5: 28A6112DCB54CE6886F7D9ACB8A15E31)
      - conhost.exe (PID: 408 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - vbc.exe (PID: 5496 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe MD5: B3A917344F5610BEEC562556F11300FA)
    - 816F.exe (PID: 1172 cmdline: C:\Users\user\AppData\Local\Temp\816F.exe MD5: 730A7A6F235525238EE33A2C046C2BA7)
    - 86EE.exe (PID: 4972 cmdline: C:\Users\user\AppData\Local\Temp\86EE.exe MD5: F46063253FF38E6B2452BF4410C5FEC0)
      - 86EE.exe (PID: 5560 cmdline: C:\Users\user\AppData\Local\Temp\86EE.exe MD5: F46063253FF38E6B2452BF4410C5FEC0)
        - 86EE.exe (PID: 5068 cmdline: C:\Users\user\AppData\Local\Temp\86EE.exe MD5: F46063253FF38E6B2452BF4410C5FEC0)
    - 8C00.exe (PID: 5400 cmdline: C:\Users\user\AppData\Local\Temp\8C00.exe MD5: F46063253FF38E6B2452BF4410C5FEC0)
      - 8C00.exe (PID: 5936 cmdline: C:\Users\user\AppData\Local\Temp\8C00.exe MD5: F46063253FF38E6B2452BF4410C5FEC0)
    - explorer.exe (PID: 5612 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
    - explorer.exe (PID: 5928 cmdline: C:\Windows\explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - explorer.exe (PID: 1768 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
    - explorer.exe (PID: 5080 cmdline: C:\Windows\explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - explorer.exe (PID: 3780 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)

- tiddsjj (PID: 3152 cmdline: C:\Users\user\AppData\Roaming\tiddsjj MD5: FFB4CF34B38F126C917E1C1E1D26DF73)
- rovwer.exe (PID: 2560 cmdline: C:\Users\user\AppData\Local\Temp\99e342142d\rovwer.exe MD5: 5E08968D858224A33175069D64DC7F39)
- **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
0000000B.00000002.378510967.0000000000930000.00000040.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_3687686f	unknown	unknown	• 0x30d:$a: 0C 8B 45 F0 89 45 C8 8B 45 C8 8B 40 3C 8B 4D F0 8D 44 01 04 89
00000023.00000000.445464817.0000000003270000.00000040.80000000.00040000.00000000.sdmp	Windows_Trojan_Smokeloader_4e31426e	unknown	unknown	• 0x34:$a: 5B 81 EB 34 10 00 00 6A 30 58 64 8B 00 8B 40 0C 8B 40 1C 8B 40 08 89 85 C0
0000000B.00000002.378663629.0000000000B41000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x7aa8:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B
00000020.00000002.457565511.00000000012D0000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Vidar_1	Yara detected Vidar stealer	Joe Security	
00000013.00000002.535069692.0000000000B01000.00000040.00000020.00020000.00000000.sdmp	Windows_Trojan_RedLineStealer_ed346e4c	unknown	unknown	• 0x6f64:$a: 55 8B EC 8B 45 14 56 57 8B 7D 08 33 F6 89 47 0C 39 75 10 76 15 8B

Click to see the 62 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.tiddsjj.930e67.1.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
12.2.2B4A.exe.2840000.6.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	

Source	Rule	Description	Author	Strings
12.2.2B4A.exe.2840000.6.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
11.3.tiddsjj.950000.0.raw.unpack	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
12.2.2B4A.exe.400000.0.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 40 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18 - Source IP: 192.168.2.3 - Destination IP: 77.232.37.228

Timestamp:	192.168.2.377.232.37.22849729802851815 11/19/22-10:38:14.789628
SID:	2851815
Source Port:	49729
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:	192.168.2.377.232.37.22849733802851815 11/19/22-10:38:20.903452
SID:	2851815
Source Port:	49733
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:	192.168.2.377.232.37.22849725802851815 11/19/22-10:38:10.657737
SID:	2851815
Source Port:	49725
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Single char EXE direct download likely trojan (multiple families) - Source IP: 192.168.2.3 - Destination IP: 89.208.107.216

Timestamp:	192.168.2.389.208.107.21649738802018581 11/19/22-10:38:23.294845
SID:	2018581
Source Port:	49738
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 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

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 Ursnif

Yara detected SmokeLoader

E-Banking Fraud

Yara detected Ursnif

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

.NET source code contains potential unpacker

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

Deletes itself after installation

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

Malware Analysis System Evasion

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

Opens the same file many times (likely Sandbox evasion)

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

Anti Debugging

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion

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

Creates a thread in another existing process (thread injection)

Writes to foreign memory regions

Injects code into the Windows Explorer (explorer.exe)

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

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

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

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

Remote Access Functionality

Yara detected RedLine Stealer

Yara detected Ursnif

Yara detected SmokeLoader

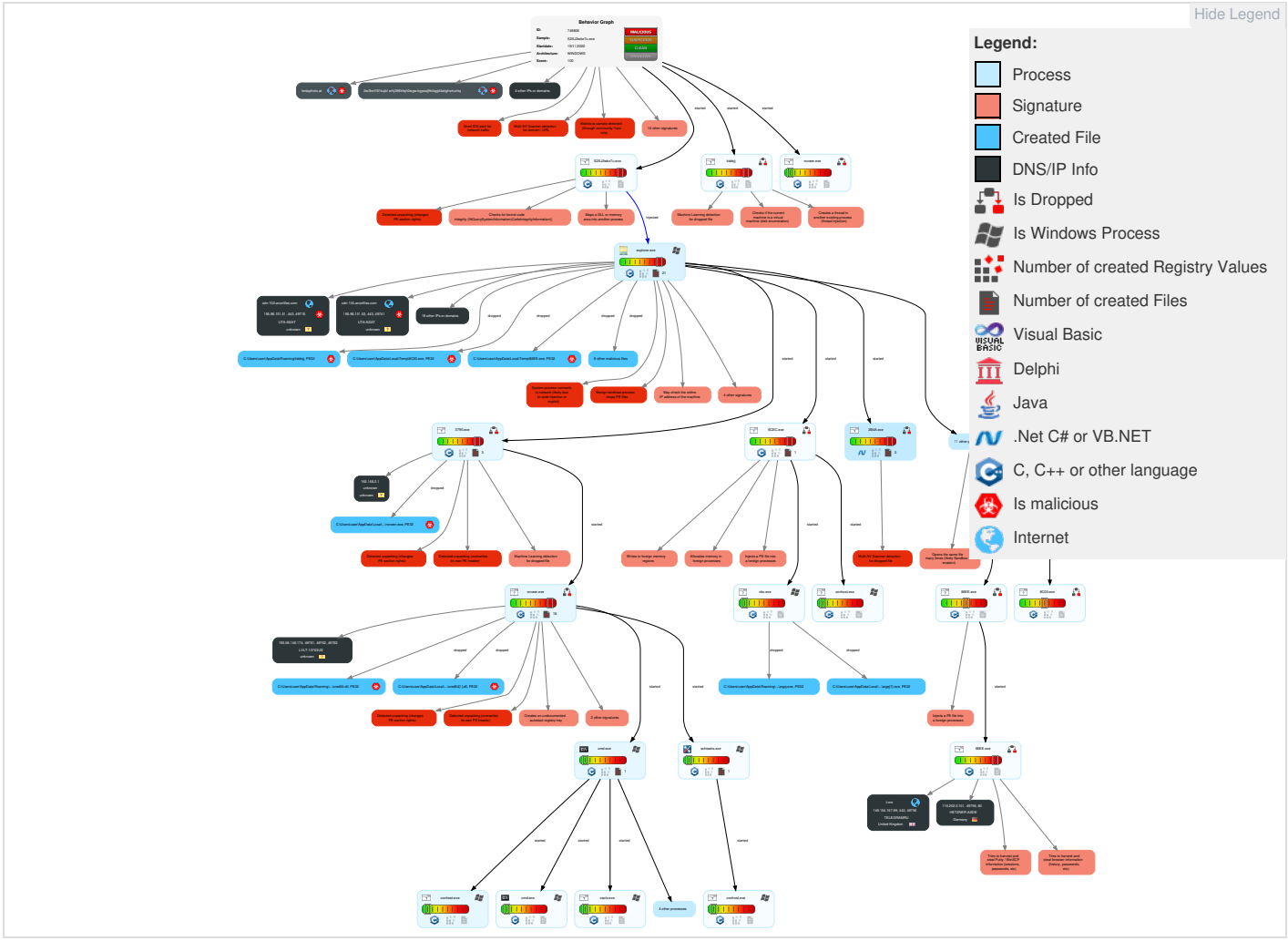
Yara detected Vidar stealer

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
1 Spearphishing Link	2 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 4 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	1 Exploitation for Client Execution	1 Scheduled Task/Job	7 1 2 Process Injection	1 1 Deobfuscate/Decode Files or Information	1 Input Capture	2 File and Directory Discovery	Remote Desktop Protocol	2 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	2 Command and Scripting Interpreter	1 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	3 Obfuscated Files or Information	1 Credentials in Registry	4 4 System Information Discovery	SMB/Windows Admin Shares	1 Input Capture	Automated Exfiltration	5 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 Scheduled Task/Job	1 Services File Permissions Weakness	1 Registry Run Keys / Startup Folder	3 3 Software Packing	NTDS	4 4 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 6 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	1 Services File Permissions Weakness	1 DLL Side-Loading	LSA Secrets	2 3 1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 File Deletion	Cached Domain Credentials	1 3 Process Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 Masquerading	DCSync	1 Application Window 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	2 3 1 Virtualization/Sandbox Evasion	Proc Filesystem	1 Remote System 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)	7 1 2 Process Injection	/etc/passwd and /etc/shadow	1 System Network Configuration 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	Process 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	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

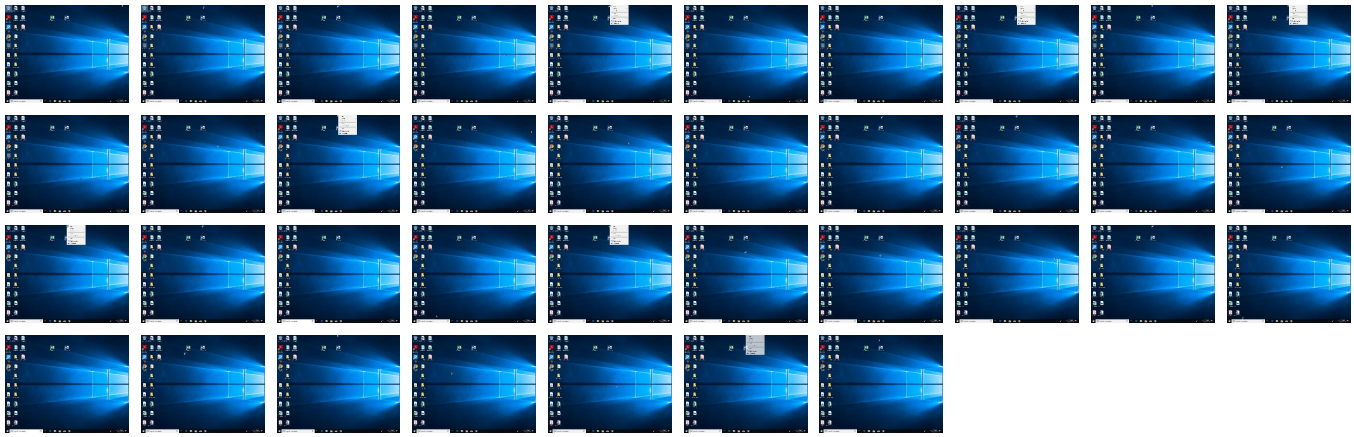
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
S2XJ2wbz7u.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\3790.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\tiddsjj	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\6CEC.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\99e342142d\rovwer.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\453D.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\816F.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\59FE.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\2B4A.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\6644.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\argq[1].exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\argq[1].exe	0%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
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\2B4A.exe	NaN%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\2B4A.exe	73%	ReversingLabs	Win32.Trojan.Raccoon	
C:\Users\user\AppData\Local\Temp\453D.exe	21%	ReversingLabs		
C:\Users\user\AppData\Roaming\PingboardCache\argq.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\PingboardCache\argq.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\a091ec0a6e2227\cred64.dll	88%	ReversingLabs	Win32.Infostealer.Decred	
C:\Users\user\AppData\Roaming\a091ec0a6e2227\cred64.dll	71%	Metadefender		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
21.3.6CEC.exe.6c0000.0.unpack	100%	Avira	TR/Downloader.Gen2		Download File
19.2.6644.exe.950000.2.unpack	100%	Avira	HEUR/AGEN.1245293		Download File
19.3.6644.exe.940000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.3.tiddsjj.950000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.S2XJ2wbz7u.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.tiddsjj.930e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.tiddsjj.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.S2XJ2wbz7u.exe.860e67.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.6644.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen7		Download File
0.3.S2XJ2wbz7u.exe.870000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.6644.exe.930e67.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
cdn-102.anonfiles.com	3%	Virustotal		Browse
raw.githubusercontent.com	1%	Virustotal		Browse
o36fafs3sn6xou.com	15%	Virustotal		Browse
anonfiles.com	4%	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://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://o3b1wk8sfk74tf.com/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/G	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24Response	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/u	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/c	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://o36fafs3sn6xou.com/Mozilla/5.0	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://193.56.146.174/	0%	Avira URL Cloud	safe	
http://svedbergbryanthusnonarithmetical.com/v6/yoae.php?dfkt=6	0%	Avira URL Cloud	safe	
http://193.56.146.174/g84kvj4jck/index.phpIM	0%	Avira URL Cloud	safe	
http://https://raw.githubusercontent.com/decoder1989/Wallet/main/Crypted.exe	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id4Sy(5	0%	Avira URL Cloud	safe	
http://91.213.50.70/Wavafursq.jpeg	100%	Avira URL Cloud	malware	
http://193.56.146.174/g84kvj4jck/index.php)M	0%	Avira URL Cloud	safe	
http://2w3.56.146.174/g84kvj4jck/index.php	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id22Response(5	0%	Avira URL Cloud	safe	
http://svedbergbryanthusnonarithmetical.com/	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id4(5	0%	Avira URL Cloud	safe	
http://116.202.5.101:80	100%	Avira URL Cloud	malware	
http://www.fontbureau.comol	0%	Avira URL Cloud	safe	
http://193.56.146.174/g84kvj4jck/index.php?scr=1kvj4jck/index.php	100%	Avira URL Cloud	malware	
http://193.56.146.174/g84kvj4jck/index.php?scr=1	100%	Avira URL Cloud	malware	
http://193.56.146.174/g84kvj4jck/Plugins/cred64.dllming	100%	Avira URL Cloud	malware	
http://193.56.146.168/mia/solt.exe	100%	Avira URL Cloud	malware	
http://91.213.50.70/Wavafursq.jpeg&BKl:	100%	Avira URL Cloud	malware	
http://tempuri.org/Entity/Id1Response(5	0%	Avira URL Cloud	safe	
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://193.56.146.174/g84kvj4jck/Plugins/cred64.dlltE	100%	Avira URL Cloud	malware	
http://193.56.146.174/U8eZkQ0Y1ZtSx2oLs	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
u.to	195.216.243.155	true	false		high
github.com	140.82.121.4	true	false		high
raw.githubusercontent.com	185.199.108.133	true	true	• 1%, Virustotal, Browse	unknown
t.me	149.154.167.99	true	false		high
cdn.discordapp.com	162.159.133.233	true	false		high
o36fafs3sn6xou.com	77.232.37.228	true	true	• 15%, Virustotal, Browse	unknown
anonfiles.com	45.154.253.151	true	true	• 4%, Virustotal, Browse	unknown
svedbergbryanthusnonarithmetical.com	84.21.172.142	true	false		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	52.217.206.73	true	false		high
youtube-ui.l.google.com	172.217.168.14	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
windowsupdatebg.s.llnwi.net	178.79.225.0	true	false		unknown
cdn-104.anonfiles.com	195.96.151.53	true	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
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	false	• 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://https://www.tiktok.com/@user6068972597711	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://193.56.146.174/	rovwer.exe, 0000000F.00000002.555134587.0000000000B33000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://91.213.50.70/Wavafursq.jpeg	816F.exe, 0000001A.00000002.564423436.000000002508000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Text	2B4A.exe, 0000000C.00000002.593637539.000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/sc/sct	2B4A.exe, 0000000C.00000002.593637539.000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/chrome_newtab	2B4A.exe, 0000000C.00000002.595351111.0000000002AA2000.00000004.00000800.00020000.00000000.sdmp, 86EE.exe, 0000002D.00000003.493239305.00000000275C1000.00000004.00000800.00020000.00000000.sdmp, 84206842141166370440363339.45.dr, 41479232570897308364731578.45.dr	false		high
http://193.56.146.174/g84kvj4jck/index.phpIM	rovwer.exe, 0000000F.00000002.555134587.0000000000B33000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/sc/dk	2B4A.exe, 0000000C.00000002.593637539.000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/ac/?q=	41479232570897308364731578.45.dr	false		high
http://116.202.5.101:80	86EE.exe, 0000002D.00000003.476529249.000000001523000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://tempuri.org/Entity/Id12Response	2B4A.exe, 0000000C.00000002.592021654.000000002901000.00000004.00000800.00020000.00000000.sdmp, 2B4A.exe, 0000000C.00000002.593637539.00000000029CB000.00000004.00000800.00020000.00000000.sdmp, 2B4A.exe, 0000000C.00000002.593366709.000000002996000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://193.56.146.174/g84kvj4jck/Plugins/cred64.dllming	rovwer.exe, 0000000F.00000002.548035575.0000000000AE4000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://www.google.com/intl/en_uk/chrome/https://www.google.com/intl/en_uk/chrome/https://www.google	86EE.exe, 0000002D.00000003.488228184.000000000275BE000.00000004.00000800.00020000.00000000.sdmp, 86EE.exe, 0000002D.00000003.489485701.00000000273BD000.00000004.00000800.00020000.00000000.sdmp, 41578029597719329563787 93.45.dr, 940884334113929105842236 25.45.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://svedbergbryanthusnonarithmetical.com/v6/yoae.php?dfkt=6	vbc.exe, 00000021.00000002.540979642.0000000007542000.00000004.00000800.00020000.00000000.sdmp, vbc.exe, 00000021.00000002.523011791.0000000000998000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://tempuri.org/	2B4A.exe, 0000000C.00000002.592021654.00000000002901000.00000004.00000800.00020000.00000000.sdmp, 2B4A.exe, 0000000C.00000002.593637539.00000000029CB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id2Response	2B4A.exe, 0000000C.00000002.593637539.00000000029CB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	816F.exe, 0000001A.00000002.592418657.00000000007352000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/sc/dk/p_sha1	2B4A.exe, 0000000C.00000002.593637539.00000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id21Response	2B4A.exe, 0000000C.00000002.592021654.00000000002901000.00000004.00000800.00020000.00000000.sdmp, 2B4A.exe, 0000000C.00000002.593366709.0000000002996000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/2005/02/trust/spnego#GSS_Wrap	2B4A.exe, 0000000C.00000002.593637539.00000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.1#SAMLID	2B4A.exe, 0000000C.00000002.593637539.00000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id4Sy(5	2B4A.exe, 0000000C.00000002.593366709.00000000002996000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://support.google.com/chrome/answer/6315198?product=	940884334113929105842236 25.45.dr	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust#BinarySecret	2B4A.exe, 0000000C.00000002.593637539.00000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://193.56.146.174/g84kvj4jck/index.php?scr=1kvj4jck/index.php	rovwer.exe, 0000000F.00000002.555134587.0000000000B33000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://193.56.146.174/g84kvj4jck/index.php)M	rovwer.exe, 0000000F.00000002.555134587.0000000000B33000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/Issue	2B4A.exe, 0000000C.00000002.593637539.00000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.google.com/intl/en_uk/chrome/thank-you.html?statcb=0&installdataindex=empty&defaultbrows	940884334113929105842236 25.45.dr	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Aborted	2B4A.exe, 0000000C.00000002.593637539.00000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/TerminateSequence	2B4A.exe, 0000000C.00000002.592021654.00000000002901000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/fault	2B4A.exe, 0000000C.00000002.593637539.00000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat	2B4A.exe, 0000000C.00000002.593637539.00000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/DPlease	816F.exe, 0000001A.00000002.592418657.00000000007352000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id15Response	2B4A.exe, 0000000C.00000002.592021654.00000000002901000.00000004.00000800.00020000.00000000.sdmp, 2B4A.exe, 0000000C.00000002.593637539.00000000029CB000.00000004.00000800.00020000.00000000.sdmp, 2B4A.exe, 0000000C.00000002.593366709.0000000002996000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	816F.exe, 0000001A.00000002.592418657.00000000007352000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

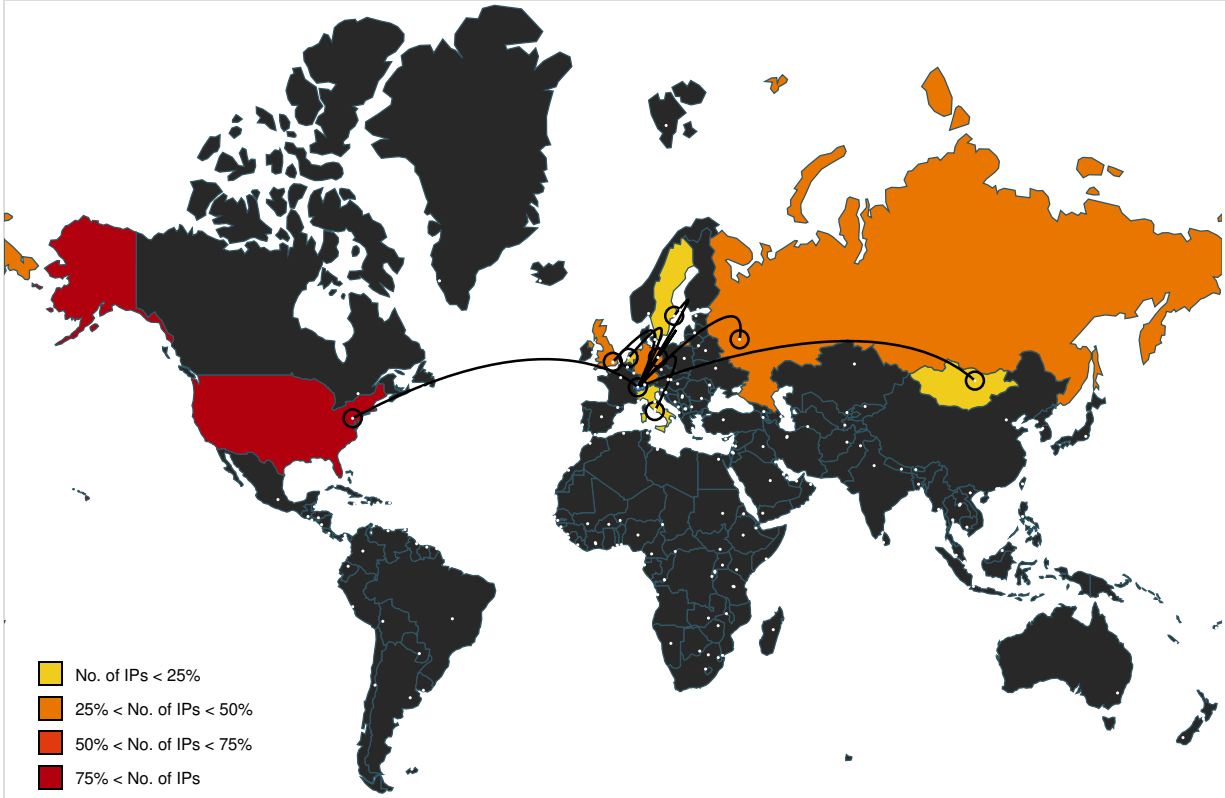
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.google.com/chrome?p=update_error	86EE.exe, 0000002D.00000003.488301104.000000000275CA000.00000004.00000800.00020000.00000000.sdmp, 86EE.exe, 0000002D.00000003.488058790.00000000273BD000.00000004.00000800.00020000.00000000.sdmp, 41578002959771932956378793.45.dr, 940884334113929105842236 25.45.dr	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm8D;	2B4A.exe, 0000000C.00000002.592021654.000000002901000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	2B4A.exe, 0000000C.00000002.593637539.000000029CB000.00000004.00000800.00020000.00000000.sdmp, 816F.exe, 0000001A.00000002.572240339.000000000255C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Renew	2B4A.exe, 0000000C.00000002.593637539.000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wscoor/Register	2B4A.exe, 0000000C.00000002.593637539.000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/trust/SymmetricKey	2B4A.exe, 0000000C.00000002.593637539.000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/Y	816F.exe, 0000001A.00000003.502347136.000000060CB000.00000004.00000800.00020000.00000000.sdmp, 816F.exe, 0000001A.00000003.504941447.00000000060CC000.00000004.00000800.00020000.00000000.sdmp, 816F.exe, 0000001A.00000003.503017067.00000000060D1000.00000004.00000800.00020000.00000000.sdmp, 816F.exe, 0000001A.00000003.503500736.00000000060CC000.00000004.00000800.00020000.00000000.sdmp, 816F.exe, 0000001A.00000003.504087152.00000000060CE000.00000004.00000800.00020000.00000000.sdmp, 816F.exe, 0000001A.00000003.506137806.00000000060CC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.google.com/intl/en_uk/chrome/Google	41578002959771932956378793.45.dr, 940884334113929105842236 25.45.dr	false		high
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000001.00000000.299404500.000000000F270000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000000.286478895.0000000001425000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000001.00000000.276466462.000000000F276000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000001.00000000.307788321.0000000001425000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000001.00000000.257994552.0000000001425000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://api.ip.sb/ip	2B4A.exe, 0000000C.00000002.593637539.000000029CB000.00000004.00000800.00020000.00000000.sdmp, 2B4A.exe, 0000000C.00000003.399248246.0000000000856000.00000004.00000020.00020000.00000000.sdmp, 2B4A.exe, 0000000C.00000002.561654188.000000000227A000.00000004.00000800.00020000.00000000.sdmp, 2B4A.exe, 0000000C.00000002.582776721.0000000002540000.00000004.08000000.00040000.00000000.sdmp, 2B4A.exe, 0000000C.00000002.590764503.0000000002840000.00000004.08000000.00040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://2w3.56.146.174/g84kvj4jck/index.php	rovwer.exe, 0000000F.00000002.558304896.0000000000B71000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://schemas.xmlsoap.org/ws/2005/02/trust/RSTR/SCT/Cancel	2B4A.exe, 0000000C.00000002.593637539.000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	41479232570897308364731578.45.dr	false		high
http://www.jiyu-kobo.co.jp/G	816F.exe, 0000001A.00000003.500229270.000000060CE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/trust/CK/PSHA1	2B4A.exe, 0000000C.00000002.593637539.000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/Entity/Id24Response	2B4A.exe, 0000000C.00000002.592021654.00000000002901000.00000004.00000800.00020000.00000000.sdmp, 2B4A.exe, 0000000C.00000002.593366709.0000000002996000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	2B4A.exe, 0000000C.00000002.595351111.0000000002AA2000.00000004.00000800.00020000.00000000.sdmp, 86EE.exe, 0000002D.00000003.493239305.00000000275C1000.00000004.00000800.00020000.00000000.sdmp, 8420684214116637044036339.45.dr, 41479232570897308364731578.45.dr	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/AckRequested	2B4A.exe, 0000000C.00000002.592021654.00000000002901000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.coml	816F.exe, 0000001A.00000002.592418657.00000000007352000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/tlsnego	2B4A.exe, 0000000C.00000002.593637539.000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://svedbergbryanthusnonarithmetical.com/	vbc.exe, 00000021.00000002.540979642.0000000007542000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://tempuri.org/Entity/Id22Response(5	2B4A.exe, 0000000C.00000002.592021654.00000000002901000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/u	816F.exe, 0000001A.00000003.500229270.000000060CE000.00000004.00000800.00020000.00000000.sdmp, 816F.exe, 0000001A.00000003.497487573.00000000060CE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing	2B4A.exe, 0000000C.00000002.592021654.00000000002901000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id4(5	2B4A.exe, 0000000C.00000002.592021654.00000000002901000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/02/trust/RST/Issue	2B4A.exe, 0000000C.00000002.593637539.000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comol	816F.exe, 0000001A.00000002.591760337.000000060C0000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2004/10/wscoor/CreateCoordinationContextResponse	2B4A.exe, 0000000C.00000002.593637539.000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/c	816F.exe, 0000001A.00000003.494973945.000000060C5000.00000004.00000800.00020000.00000000.sdmp, 816F.exe, 0000001A.00000003.497487573.00000000060CE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://91.213.50.70/Wavafursq.jpeg&BKl:	816F.exe, 0000001A.00000002.541785354.0000000000889000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://tempuri.org/Entity/Id5Response	2B4A.exe, 0000000C.00000002.592021654.00000000002901000.00000004.00000800.00020000.00000000.sdmp, 2B4A.exe, 0000000C.00000002.593637539.000000029CB000.00000004.00000800.00020000.00000000.sdmp, 2B4A.exe, 0000000C.00000002.593366709.0000000002996000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://tempuri.org/Entity/Id1Response(5	2B4A.exe, 0000000C.00000002.593366709.0000000002996000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/dns	2B4A.exe, 0000000C.00000002.592021654.00000000002901000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id10Response	2B4A.exe, 0000000C.00000002.592021654.00000000002901000.00000004.00000800.00020000.00000000.sdmp, 2B4A.exe, 0000000C.00000002.593366709.0000000002996000.00000004.00000800.00020000.00000000.sdmp, 2B4A.exe, 0000000C.00000002.597552021.0000000002B50000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/02/trust/Renew	2B4A.exe, 0000000C.00000002.593637539.000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://tempuri.org/Entity/Id8Response	2B4A.exe, 0000000C.00000002.592021654.000000002901000.00000004.00000800.00020000.00000000.sdmp, 2B4A.exe, 0000000C.00000002.593637539.00000000029CB000.00000004.00000800.00020000.00000000.sdmp, 2B4A.exe, 0000000C.00000002.593366709.000000002996000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://t.me/deadftxhttps://www.tiktok.com/	86EE.exe, 0000001E.00000002.456037519.000000001560000.00000004.00000800.00020000.00000000.sdmp, 8C00.exe, 00000020.00000002.457565511.00000000012D0000.00000004.00000800.00020000.00000000.sdmp, 86EE.exe, 00000022.00000002.463148223.000000000910000.00000004.00000800.00020000.00000000.sdmp, 8C00.exe, 00000029.00000002.464734781.00000000008F0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	816F.exe, 0000001A.00000002.592418657.000000007352000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0#SAMLAssertionID	2B4A.exe, 0000000C.00000002.593637539.000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RST/SCT	2B4A.exe, 0000000C.00000002.593637539.000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2006/02/addressingidentity	2B4A.exe, 0000000C.00000002.593637539.000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/trust/PublicKey	2B4A.exe, 0000000C.00000002.593637539.000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/10/wsat/Rollback	2B4A.exe, 0000000C.00000002.593637539.000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/04/security/trust/RSTR/SCT	2B4A.exe, 0000000C.00000002.593637539.000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/06/addressingex	2B4A.exe, 0000000C.00000002.593637539.000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.typography.netD	816F.exe, 0000001A.00000002.592418657.000000007352000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://193.56.146.174/U8eZkQ0Y1ZtSx2oLs	rovwer.exe, 0000000F.00000002.555134587.0000000000B33000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://o36fafs3sn6xou.com/Mozilla/5.0	explorer.exe, 00000023.00000000.44546481 7.0000000003270000.00000040.80000000.00040000.00000000.sdmp, explorer.exe, 00000028.00000000.448635710.0000000000950000.00000040.80000000.00040000.00000000.sdmp, explorer.exe, 00000028.00000002.522890770.0000000000D20000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000002A.00000000.451638661.00000000005A0000.00000040.80000000.00040000.00000000.sdmp, explorer.exe, 0000002C.00000002.523503696.0000000000810000.00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000002C.00000000.454736835.00000000003E0000.00000040.80000000.00040000.00000000.sdmp	true	• URL Reputation: safe	unknown
http://fontfabrik.com	816F.exe, 0000001A.00000002.592418657.000000007352000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/04/security/trust/Nonce	2B4A.exe, 0000000C.00000002.593637539.000000029CB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/02/rm/CreateSequenceResponse	2B4A.exe, 0000000C.00000002.592021654.000000002901000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/answer/111996?visit_id=637962485686793996-3320600880&p=update_erro	940884334113929105842236 25.45.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://193.56.146.174/g84kvj4jck/Plugins/cred64.dlltE	rovwer.exe, 0000000F.00000002.542120947.0000000000AB0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://www.google.com/intl/en_uk/chrome/	940884334113929105842236 25.45.dr	false		high
http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_REQ1510	2B4A.exe, 0000000C.00000002.593637539.000000000029CB000.00000004.00000800.00020000.00000000.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
195.96.151.53	cdn-104.anonfiles.com	unknown		8437	UTA-ASAT	true
195.96.151.51	cdn-102.anonfiles.com	unknown		8437	UTA-ASAT	true
140.82.121.3	unknown	United States		36459	GITHUBUS	false
140.82.121.4	github.com	United States		36459	GITHUBUS	false
162.159.133.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false
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
89.208.107.216	unknown	Russian Federation		42569	PSKSET-ASRU	true
52.217.206.73	s3-w.us-east-1.amazonaws.com	United States		16509	AMAZON-02US	false
104.192.141.1	bitbucket.org	United States		16509	AMAZON-02US	false
116.202.5.101	unknown	Germany		24940	HETZNER-ASDE	false
148.251.234.93	iplogger.com	Germany		24940	HETZNER-ASDE	false
195.216.243.155	u.to	United Kingdom		57724	DDOS-GUARDRU	false
185.199.108.133	raw.githubusercontent.com	Netherlands		54113	FASTLYUS	true
193.56.146.174	unknown	unknown		10753	LVLT-10753US	false
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
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	749806
Start date and time:	2022-11-19 10:36:06 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	S2XJ2wbz7u.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.troj.spyw.evad.winEXE@67/30@58/22
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 13.5% (good quality ratio 11.6%) • Quality average: 67.1% • Quality standard deviation: 36%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, Conhost.exe, WerFault.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 93.184.220.29, 93.184.221.240
- Excluded domains from analysis (whitelisted): google.com, fs.microsoft.com, cs9.wac.phicdn.net, wu.ec.azureedge.net, ctldl.windowsupdate.com, wu-bg-shim.trafficmanager.net, wu.azureedge.net, ocsp.digicert.com, login.live.com, bg.apr-52dd2-0503.edgecastdns.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, 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 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.

Simulations

Behavior and APIs

Time	Type	Description
10:37:52	Task Scheduler	Run new task: Firefox Default Browser Agent 56A8988D325A9B46 path: C:\Users\user\AppData\Roaming\tiddsjj
10:38:28	API Interceptor	111x Sleep call for process: rovwer.exe modified

Time	Type	Description
10:38:29	Task Scheduler	Run new task: rovwer.exe path: C:\Users\user\AppData\Local\Temp\99e342142d\rovwer.exe
10:38:39	API Interceptor	185x Sleep call for process: explorer.exe modified
10:39:04	API Interceptor	4x Sleep call for process: vbc.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\41479232570897308364731578

Process:	C:\Users\user\AppData\Local\Temp\86EE.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\41578002959771932956378793

Process:	C:\Users\user\AppData\Local\Temp\86EE.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\428634266555153395578900088

Process:	C:\Users\user\AppData\Local\Temp\86EE.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:\ProgramData\84206842141166370440363339

Process:	C:\Users\user\AppData\Local\Temp\86EE.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\94088433411392910584223625

Process:	C:\Users\user\AppData\Local\Temp\86EE.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\95786452850497366982696300

Process:	C:\Users\user\AppData\Local\Temp\86EE.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:	48:43KzOIIY3HzrkNSs8LKvUf9KnmlG0UX9q4lCm+KLka+yJqhM0ObVEq8Ma0D0HOlx:Sq0NFeymDlGD9qlm+KL2y0Obn8MouO
MD5:	CF7758A2FF4A94A5D589DEBAED38F82E
SHA1:	D3380E70D0CAEB9AD78D14DD970EA480E08232B8
SHA-256:	6CA783B84D01BFCF9AA7185D7857401D336BAD407A182345B97096E1F2502B7F
SHA-512:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804CBF
Malicious:	false
Preview:	SQLite format 3.....@ .....[5..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\wpiq[1].zip

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	1019991
Entropy (8bit):	**7.9981268397514125**
Encrypted:	**true**
SSDEEP:	24576:I8QnhcAisyibvw8QJTTRz+oH7OgXwWpiubynw7ynLbzCQ:Itns7GY1XSsOQfE/7bzCQ
MD5:	9E73FB50D37E37EE8BD19A8E3D2B82CA
SHA1:	3DB1C548E86E4BB7457324A3097B05DA15B7FFC3
SHA-256:	68BA7122EE8D9CE34ED94B6036A171CE38D6D9D9B3A609C2F4DE773F4DD40D5C
SHA-512:	B41209300F018103B0F8A4DE0537F348A3BDFCBC8FEB19E7FEC6634B06C266CC442145FD2D9230F827F273B0D07BB6BBCAB7A0F0E9E1F558E6DD7A076F56805 4
Malicious:	false
Preview:	PK.....e.K...yq1...@.....7zxa.dll...x.....d'.,.b.X%j....5.Q.7.....l.d.B.m%.)mi...$.6.2..b_...R}k[....FK...l"..O...FE.uC...02.9.../.?...=..<.....{...k.g.8N.?]....sr.....)W.0.{v.k.:.E..*..g].... ~..k.....J.__.Q/.'..d.....w.^}...).X.u..7..N.....Y...i.....J.....i.mi30..*Mo.....i...D.GR~@.....}.....X.....E|.w.,...q7.J.0.U...,....<..}O`p.'...L..f.....PT.%..b`s..;.....|I.....<?} %./.06M.....I_.8G^.....g.Fp.y.K.=..3&..$.O..a....V.6..8.]..._W...j:..g....9o._....R.+.2x^3!.<.....kv..S.u.f..L.m.....3....=....d.S....Q...~.....A..`...._f?.We.U6.H..D6...dk...4.Z....Q- .....a...^^...uTr...O:x'.....uh.)..>"...f.S.l.Rb.}f.m..c.0%Yd...x.W...\....u..^....WZ..z.....t+..{.....D....s.ne2....GN.qa.p..7.kD..5.....v.C.....~.k...f]6....P..%#.%.z.$E.!..>....#.. .....g..YH..7U.0..W.).S.....*.*..^"..([.g.)d....iWc...j.w'....F.'s...M."..={.{s<.....}.3..s).|.....\~.T..-k..V~....n.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\argq[1].exe

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	167936
Entropy (8bit):	6.1797557233483955
Encrypted:	false
SSDEEP:	3072:leAGcNNwmlR2GNUbomMYMLnbtoKOmiNL2SJOUOhop:CvNNtWuYcqHmiNLOc
MD5:	75375C22C72F1BEB76BEA39C22A1ED68
SHA1:	E1652B058195DB3F5F754B7AB430652AE04A50B8
SHA-256:	8D9B5190AACE52A1DB1AC73A65EE9999C329157C8E88F61A772433323D6B7A4A
SHA-512:	1B396E78E189185EEFB8C6058AA7E6DFE1B8F2DFF8BABFE4FFBEE93805467BF45760EEA6EFB8D9BB2040D0EAA56841D457B1976DCFE13ED67931ADE01419F55A
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....R.D.3...3...3...,...3...3...3.../...3.....3.../...3.....3..Rich.3..... .....PE..L...P.#B.....xH.....@.....07..P..... .....text..... ..`.rdata...a.....p.....@..@.data....b...P...@....P.....@..... ....

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\2B4A.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	300544
Entropy (8bit):	7.542146445882773
Encrypted:	false
SSDEEP:	3072:fNXZlOquqTc5+9AgXR2numfufipMbiH7Evn7TGq5gXiXRsBmS7F4GYcNLlR3LTcU:fn+uW9AskuYufipGiudsqcNxRsi9
MD5:	2DEE200193091BE2F2321D921750C4ED
SHA1:	4C5B6C7512BE4D4E200C4141DC0E90BCABCE4CA3
SHA-256:	7330807028605EBA5B4ECFACA0390B78CB04E4276D1DE23EB95B407E1244EF12
SHA-512:	4124E9BC1C7C587CE394AD35EC56FD3C6EC4466167DF6E00FFA1D88B09B34FA69072D946337CAD696223D31D85F8662FF9D5452C474D20CCA06D91A8B9C608 D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: NaN%, Browse • Antivirus: ReversingLabs, Detection: 73%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m4.r.g.r.g.r.g. .g.r.g. .g.r.g.xg.r.g.r.gDr.g. .g.r.g. .g.r.g. .g.r.gR ich.r.g.....PE..L...^.ab.....8.....c.....P....@.....3.....:..P.....<.....`.....4..@.... .....text....6.....8..... ..`.data....K...P.....<.....@....rsrc....<.....<...Z.....@..@..... ....

C:\Users\user\AppData\Local\Temp\3790.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	382464
Entropy (8bit):	6.969580968654444
Encrypted:	false
SSDEEP:	6144:O3eRNpLX3EJscap6Hi+RtWce2vjacYJdjpPnFwCLLObfwB:9NtUJsP0jVerxqC3O
MD5:	5E08968D858224A33175069D64DC7F39

SHA1:	8D18D2E867205BA9D0F42DB569C335609FDC1752
SHA-256:	9329CAC20692208A720E6565B51F2492FFAE539FF9B2AD469D6FAC8FDA061C87
SHA-512:	06D08EC2C2352AA7DFCD97F6E3691EFC1AF91CB1409543566D5D4E230D2665DB6F5C820F28D88519D6D888852FAD3B4725E32D36F9ACA3577554D6DCFED161C
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.....H.....@....@.....F.....'..(....pC.xC.....E.....@..... .....text...f ....."..... ..`.data....)B..@...(...&.....@....rsrc...xC...pC..D...N.....@..@.reloc...B....E..D.....@..B..... ....

C:\Users\user\AppData\Local\Temp\453D.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\59FE.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%
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\6644.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%
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\6CEC.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	360448
Entropy (8bit):	7.386873779597766
Encrypted:	false
SSDEEP:	6144:b2GSJmjsOF3L5n8qcXE63miXHB0rtlC0VAin2iuu5hxIpSjgOi6ziFB:CGSUogb5n8q68t/VMu5XQSMGu
MD5:	28A6112DCB54CE6886F7D9ACB8A15E31
SHA1:	432B6AF51096CD77D667F79B2CF89F5DD37FA748
SHA-256:	B35656FEA1C887375414AFA04BDF2DD240541F215D01B4E6B0DACC4BA8ECC73C
SHA-512:	BA86E0832339E33F13BD4F148C7616DE36BBC4A142AB42C7193212A069E5F179E6191368D5AEBFDA74C6AE6DA2606A1E36C2DDF531F38F85EAE589C3462302E0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....}.....Q.....Rich.....PE..L....xc.....B...H.....P.....`....@.....(.....(.....(.....`..@..... .....text....A.....B..... ..`.rdata...H...`...J...F.....@..@.data...8.....@....rsrc...(.....x.....@..@..... ....

C:\Users\user\AppData\Local\Temp\816F.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	228864
Entropy (8bit):	4.207192388303838
Encrypted:	false
SSDEEP:	1536:w6qNKWPdNWepOzb3OdC9E4/hUYcgvqytNIxYcW9yz:uVvWepYb+dmugvntaxw9
MD5:	730A7A6F235525238EE33A2C046C2BA7
SHA1:	DAA1B8E97D23B32B99B4B230DE9608FF1BCD5BF7
SHA-256:	4F24670DB3AA4D4DB6CED0A59AAEA20D9B784C69E181468905DB4D559FB6AFE1
SHA-512:	D97C53CEA4E2FB99BC3DD44E139D3F331251A68F085C980EBA5E8D76D5124195E2FF8958A297CFC9D0500EC90908A45CF6E76603A0040D504B8BF524AE7A9F0E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....vc..... .....@.. .....h.. ..@.....S.....H..... ....H.....text..... ....`.rsrc...H.....@..@.reloc..... .....|.....@..B.....H.....$.....).....0..Y.....(.....% ....TF..... ....Z..... ....Z.... ....%..... ....;.....F..... ....X..... ....?..... ....=.... .....?d... .....=....8{... .....?.... .....=....8....8.... .....?.... .....=....8....8|...8w... .....?>... .....=....8.... .....?.... .....=....80...80...8+

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):	82823
Entropy (8bit):	7.894936066768262
Encrypted:	false
SSDEEP:	1536:CJIA2DzHu++Bp1Xfcj6pnUh0kn9MsMRGnauvp48ePCH5ViZEylibB:r3H1CvPcjCUh1nPauvXegcuek
MD5:	BC42901C6E0D67944F7136A6CF75D87F

SHA1:	79B7FE4111C298B32D52C6A635F176E93FC2562C
SHA-256:	1BA5179353D7E9C3831D1DEEDED3FC01332E5A0BFE21267C5DC941A27E619193
SHA-512:	F4C4897CB90653854649065A15D307A5DB7DF838C04DD7940501CC9D21451AC70269E79C99A72A8853BCD8FA430D90D9826B6332AD35517DA320DD07D674E67
Malicious:	false
Preview:	......JFIF.....`.`.....C.................................. $.' ",#..(7),01444.'9=82<.342...C..........2!.!22222222222222222222222222222222222222222222222222..........".................... ....}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ....?..01KK...lq\....xcS.m..#Hm.....T......<!...wq5...v1.?S.....rHj-.U:...5...........\|..+.......}...<.>...H.......Wo.CK`/l.1./...C...W.....,1....R.0.W....Q..G.Z5..$....i_.S...'..9'.j........ ......;...d..;..F......r..!vV.s......xg.?.w.....q.....X.v?...Gp*.T...6..&.ZJ.i(....R..!....a._.....4."4h.d.J..=.e%.v8.'dy.-}E...G....u...MI...G.?..w...MY.h..|.E{..>...

C:\Users\user\AppData\Local\Temp\86EE.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**
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\8C00.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
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**
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\99e342142d\rovwer.exe

Process:	C:\Users\user\AppData\Local\Temp\3790.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	382464
Entropy (8bit):	6.969580968654444
Encrypted:	false
SSDEEP:	6144:O3eRNpLX3EJscap6Hi+RtWce2vjacYJdjpPnFwCLLObfwB:9NtUJsP0jVerxqC3O
MD5:	5E08968D858224A33175069D64DC7F39
SHA1:	8D18D2E867205BA9D0F42DB569C335609FDC1752
SHA-256:	9329CAC20692208A720E6565B51F2492FFAE539FF9B2AD469D6FAC8FDA061C87
SHA-512:	06D08EC2C2352AA7DFCD97F6E3691EFC1AF91CB1409543566D5D4E230D2665DB6F5C820F28D88519D6D888852FAD3B4725E32D36F9ACA3577554D6DCFED161 C
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.....H.....@....@.....F.....'.(....pC.xC.....E.....@..... .....text...f ....."..... ..`.data....)B..@...(...&.....@....rsrc...xC...pC..D...N.....@..@.reloc...B....E..D.....@..B..... ....

C:\Users\user\AppData\Roaming\PingboardCache\argq.exe

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	167936
Entropy (8bit):	6.1797557233483955
Encrypted:	false
SSDEEP:	3072:IeAGcNNwmlR2GNUbomMYMLnbtoKOmiNL2SJOUOhop:CvNNtWuYcqHmiNLOc
MD5:	75375C22C72F1BEB76BEA39C22A1ED68
SHA1:	E1652B058195DB3F5F754B7AB430652AE04A50B8
SHA-256:	8D9B5190AACE52A1DB1AC73A65EE9999C329157C8E88F61A772433323D6B7A4A
SHA-512:	1B396E78E189185EEFB8C6058AA7E6DFE1B8F2DFF8BABFE4FFBEE93805467BF45760EEA6EFB8D9BB2040D0EAA56841D457B1976DCFE13ED67931ADE01419F55A
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Metadefender, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....R.D.3...3...3...,...3...3...3.../...3.....3.../...3.....3..Rich.3..... .....PE..L...P.#B.....xH.....@.....07..P..... .....text..... ..`.rdata...a.....p.....@..@.data....b...P...@...P.....@..... ....

C:\Users\user\AppData\Roaming\PingboardCache\wpiq.zip

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	1019991
Entropy (8bit):	**7.9981268397514125**
Encrypted:	**true**
SSDEEP:	24576:l8QnhcAisyibvw8QJTTRz+oH7OgXwWpiubynw7ynLbzCQ:ltns7GY1XSsOQfE/7bzCQ
MD5:	9E73FB50D37E37EE8BD19A8E3D2B82CA
SHA1:	3DB1C548E86E4BB7457324A3097B05DA15B7FFC3
SHA-256:	68BA7122EE8D9CE34ED94B6036A171CE38D6D9D9B3A609C2F4DE773F4DD40D5C
SHA-512:	B41209300F018103B0F8A4DE0537F348A3BDFCBC8FEB19E7FEC6634B06C266CC442145FD2D9230F827F273B0D07BB6BBCAB7A0F0E9E1F558E6DD7A076F56809 4
Malicious:	false
Preview:	PK.....e.K...yq1...@.....7zxa.dll...x.....d'.,.b.X%j....5.Q.7.....l.d.B.m%.)mi...$.6.2..b_...R}k[....FK...l"..O...FE.uC...02.9.../.?...=..<.....{...k.g.8N.?]....sr.....)W.0.{v.k.:.E..*..g].... ~..k.....J.__.Q/.'..d.....w.^}...).X.u..7..N.....Y...i.....J.....i.mi30..*Mo.....i...D.GR~@.....}.....X.....E|.w.,...q7.J.0.U...,...<..}O`p.'...L..f.....PT.%..b`s..;.....|I.....<?} %./.06M.....I_.8G^.....g.Fp.y.K.=..3&..$.O..a....V.6..8.]..._W...j:..g....9o._....R.+.2x^3!.<.....kv..S.u.f..L.m.....3....=....d.S....Q...~.....A..`...._f?.We.U6.H..D6...dk...4.Z....Q- .....a...^^...uTr...O:x'.....uh.)..>"...f.S.I.Rb.}f.m..c.0%Yd...x.W...\....u..^....WZ..z.....t+..{.....D....s.ne2....GN.qa.p..7.kD..5.....v.C.....~.k...f]6....P..%#.%.z.$E.!..>....#.. .....g..YH..7U.0..W.).S.....*.*..^"..([.g.)d....iWc...j.w'....F.'s...M."..={.{s<.....}.3..s).|.....\~.T..-k..V~....n.....

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:Yx7pOYzBekK3tilNwyP7XSSJds3zhrjPcnqULv4G9: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\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\fgrijii

Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	160970
Entropy (8bit):	**7.998743190535304**
Encrypted:	**true**
SSDEEP:	3072:JxAURrrQurKPLuV+kPEpzS4yYpCbAlovl5z/uZtuyRMv:JxAUgLmPZtbLmz/stK
MD5:	100024D016C74F25F89DCFE50C3B3A2F
SHA1:	23166B8D0D71B01C19B7730F2019E25A103162CA
SHA-256:	60623FFF9AAEB75C60C93F4D4E71680B868E1D05117695DA75AF0C73360A1C6F
SHA-512:	9B27BA829BE35ECA8FA57FC3170F7D0A6DB476A41900E7DD6621CB5AF5BF0787BEC2EA1F5332C8B5A9F49ECA644D92CD292733CF72303C51770D41D755B690F
Malicious:	false
Preview:	.}C...x...h..?...IF.>.....5...s.Q.....Hf...]&.f.....#....=L4..c.....B..p.....w...t.....~..x*yg.m..k...Y[+...R3.O.,5.....U..s.d._V.i.JV..s<..dVs..s.9.hV.d..;4..z....T.~.qf.1..x.....p.)..V,]..^..CTX....l\6.!.....2....d.#S..*S(~...-.....h.B..[....qK...UkcT....y.D....Y..)...../F....f>).....6%..!.]...Z....c..;R...f.wCm..W...Y.....1.q;lo.#.2...f..F.>.R..7..H!.^H...<.J...K.&._...b. c.&.*|~.$-.1Kf.R.Gmu....?.'c.I..C....A..C.....}.A.~{.I..%...._v...E..:h%.)W\|.. .*gFq.y.@.;~..=.Na..E..G..m..%.;=..j..o+..J...%...6..>'.UHTX.....u].w.O.9..z..`..@1.>.....)+..sk. ....H.w.."..E....&O.....a..E}.Q...O.[....GT.'+.wf.!.oy^....C.y...[..}.>.27...LA.. .~....H...b..e..4^..*..b....m...R0.....c.....\..t..7M.{..C..I.@..Q..a6.z..S...I^k....j../8..J.}.D.. ..`s..[.P..... <.....K...f...) .....9=.....&... ..T...I[...T.K..o.{%.A.?\WL.#.....j.F...*.8.I.O...?.F..^..~7..L.g..)..W...[..G.b.....".^.h.....i.....+Z.x7..E.B....".c.:$

C:\Users\user\AppData\Roaming\tiddsjj

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	343552
Entropy (8bit):	6.790900644113691
Encrypted:	false
SSDEEP:	6144:mzE3TFjX0rs2VfUQbgjpPnFwCLLObfwB:jFGNmxqC3O
MD5:	FFB4CF34B38F126C917E1C1E1D26DF73
SHA1:	36E558FDB10418AA971AEA3F02D6BA1F4D566ED2
SHA-256:	4A47FDBB09DD09EA813C0475D32F693CBBDED09B3753DEF43179F91E1A8F8A55
SHA-512:	E7BA484B42AF0B4FDE10736D7ABD6374145D3808961BEA2A55A2E41C9E5B3C549590E914489E0DC505C5C53C1D1B7071D42892B4458956E5CD4DECBBF1BDE765
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...oU'a.....".....D.....H.....@....@.....pE.....>d.....'..(.....B.xC..... E.....@..... .....text...f .....".....`.data....A..@.....&.....@....rsrc...xC....B..D.....@..@.reloc..*B... E..D.....@..B..... .....

C:\Users\user\AppData\Roaming\tiddsjj: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

\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):	6.790900644113691
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:	S2XJ2wbz7u.exe
File size:	343552
MD5:	ffb4cf34b38f126c917e1c1e1d26df73
SHA1:	36e558fdb10418aa971aea3f02d6ba1f4d566ed2
SHA256:	4a47fdbb09dd09ea813c0475d32f693cbbded09b3753def43179f91e1a8f8a55
SHA512:	e7ba484b42af0b4fde10736d7abd6374145d3808961bea2a55a2e41c9e5b3c549590e914489e0dc505c5c53c1d1b7071d42892b4458956e5cd4decbbf1bde765
SSDEEP:	6144:mzE3TFjX0rs2VfUQbgjpPnFwCLLObfwB:jFGNmxqC3O
TLSH:	3974CF3472B0D4B2F575C670C429CAA5AABCEC213524C9033316FBBF6E30A9D566E275
File Content 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...oU'a.....

File Icon

Icon Hash:	acfca6b6b69486e2

Static PE Info

General

Entrypoint:	0x4048a5
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:	0x6127556F [Thu Aug 26 08:48:47 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:	938ae2aaaa8ec1fc2d05063ef7a2e3c5

Entrypoint Preview
Instruction
call 00007FEF60A9B8F3h
jmp 00007FEF60A96E4Dh
push 00000008h
push 00412368h
call 00007FEF60A977BAh
mov ecx, dword ptr [ebp+08h]
test ecx, ecx
je 00007FEF60A96FFCh
cmp dword ptr [ecx], E06D7363h
jne 00007FEF60A96FF4h
mov eax, dword ptr [ecx+1Ch]
test eax, eax
je 00007FEF60A96FEDh
mov eax, dword ptr [eax+04h]
test eax, eax
je 00007FEF60A96FE6h
and dword ptr [ebp-04h], 00000000h
push eax
push dword ptr [ecx+18h]
call 00007FEF60A9BA7Ch
mov dword ptr [ebp-04h], FFFFFFFEh
call 00007FEF60A977C9h
ret
xor eax, eax
cmp byte ptr [ebp+0Ch], al
setne al
ret
mov esp, dword ptr [ebp-18h]
call 00007FEF60A9B9BAh
int3
call 00007FEF60A97F97h
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 [0042CEB0h], 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

Instruction
and dword ptr [ebp-00000328h], 00000000h
push ebx
push 0000004Ch
lea eax, dword ptr [ebp-00000324h]
push 00000000h
push eax
call 00007FEF60A9BDA2h
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	0x12784	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x42d000	0x24378	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x452000	0xba0	.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	0x2cb8	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	0x12066	0x12200	False	0.5797279094827587	data	6.691650867340855	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x14000	0x418fc8	0x19000	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x42d000	0x24378	0x24400	False	0.6327653556034483	data	6.386559817005297	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x452000	0x422a	0x4400	False	0.150390625	data	1.731638841465645	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
AFX_DIALOG_LAYOUT	0x44f138	0x2	data	Setsuana	South Africa
AFX_DIALOG_LAYOUT	0x44f120	0x2	data	Setsuana	South Africa
AFX_DIALOG_LAYOUT	0x44f110	0xe	data	Setsuana	South Africa
AFX_DIALOG_LAYOUT	0x44f100	0xe	data	Setsuana	South Africa

Name	RVA	Size	Type	Language	Country
AFX_DIALOG_LAYOUT	0x44f128	0xe	data	Setsuana	South Africa
GIFOGIDICUBOTOVUKEFORAVOLIDESEF	0x44cab0	0x629	ASCII text, with very long lines (1577), with no line terminators	Setsuana	South Africa
KIFIYUMITUYIZUREL	0x44c2d8	0x7d1	ASCII text, with very long lines (2001), with no line terminators	Setsuana	South Africa
YELALASEYUGUBAHOP	0x44d0e0	0x1f9c	ASCII text, with very long lines (8092), with no line terminators	Setsuana	South Africa
RT_CURSOR	0x44f140	0x330	Device independent bitmap graphic, 48 x 96 x 1, image size 0	Setsuana	South Africa
RT_CURSOR	0x44f470	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 0	Setsuana	South Africa
RT_CURSOR	0x44f5c8	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Setsuana	South Africa
RT_CURSOR	0x450470	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Setsuana	South Africa
RT_ICON	0x42dd50	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Setsuana	South Africa
RT_ICON	0x42ebf8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Setsuana	South Africa
RT_ICON	0x42f4a0	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Setsuana	South Africa
RT_ICON	0x42fa08	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x431fb0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x433058	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x4339e0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x433eb0	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Setsuana	South Africa
RT_ICON	0x434d58	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Setsuana	South Africa
RT_ICON	0x435600	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x437ba8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x438c50	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x439108	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Setsuana	South Africa
RT_ICON	0x439fb0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Setsuana	South Africa
RT_ICON	0x43a858	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Setsuana	South Africa
RT_ICON	0x43adc0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x43d368	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x43e410	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x43ed98	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x43f268	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	Setsuana	South Africa
RT_ICON	0x440110	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	Setsuana	South Africa
RT_ICON	0x4409b8	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	Setsuana	South Africa
RT_ICON	0x441080	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	Setsuana	South Africa
RT_ICON	0x4415e8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	Setsuana	South Africa
RT_ICON	0x443b90	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	Setsuana	South Africa
RT_ICON	0x444c38	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	Setsuana	South Africa
RT_ICON	0x4455c0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	Setsuana	South Africa
RT_ICON	0x445aa0	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0	Setsuana	South Africa

Name	RVA	Size	Type	Language	Country
RT_ICON	0x446948	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0	Setsuana	South Africa
RT_ICON	0x4471f0	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0	Setsuana	South Africa
RT_ICON	0x4478b8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0	Setsuana	South Africa
RT_ICON	0x447e20	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x44a3c8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x44b470	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0	Setsuana	South Africa
RT_ICON	0x44bdf8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0	Setsuana	South Africa
RT_STRING	0x450f30	0x442	data	Setsuana	South Africa
RT_ACCELERATOR	0x44f080	0x40	data	Setsuana	South Africa
RT_GROUP_CURSOR	0x44f5a0	0x22	data	Setsuana	South Africa
RT_GROUP_CURSOR	0x450d18	0x22	data	Setsuana	South Africa
RT_GROUP_ICON	0x433e48	0x68	data	Setsuana	South Africa
RT_GROUP_ICON	0x4390b8	0x4c	data	Setsuana	South Africa
RT_GROUP_ICON	0x43f200	0x68	data	Setsuana	South Africa
RT_GROUP_ICON	0x445a28	0x76	data	Setsuana	South Africa
RT_GROUP_ICON	0x44c260	0x76	data	Setsuana	South Africa
RT_VERSION	0x450d40	0x1f0	MS Windows COFF PowerPC object file	Setsuana	South Africa
None	0x44f0d0	0xa	data	Setsuana	South Africa
None	0x44f0c0	0xa	data	Setsuana	South Africa
None	0x44f0e0	0xa	data	Setsuana	South Africa
None	0x44f0f0	0xa	data	Setsuana	South Africa

Imports

DLL	Import
KERNEL32.dll	GetComputerNameA, SetProcessAffinityMask, WriteConsoleOutputCharacterA, OpenJobObjectA, GetCommState, AddConsoleAliasW, CreateHardLinkA, GetSystemDefaultLCID, GetModuleHandleW, GetConsoleAliasesA, WaitNamedPipeW, LoadLibraryW, CopyFileW, GetFileAttributesA, GetFileAttributesW, WriteConsoleW, GetVolumePathNameA, GetPrivateProfileIntW, FillConsoleOutputCharacterW, GetLastError, GetProcAddress, VirtualAlloc, EnumSystemCodePagesW, 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, GetTickCount, 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
192.168.2.377.232.37.228 49729802851815 11/19/22-10:38:14.789628	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49729	80	192.168.2.3	77.232.37.228
192.168.2.377.232.37.228 49733802851815 11/19/22-10:38:20.903452	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49733	80	192.168.2.3	77.232.37.228
192.168.2.377.232.37.228 49725802851815 11/19/22-10:38:10.657737	TCP	2851815	ETPRO TROJAN Sharik/Smokeloader CnC Beacon 18	49725	80	192.168.2.3	77.232.37.228
192.168.2.389.208.107.21 649738802018581 11/19/22-10:38:23.294845	TCP	2018581	ET TROJAN Single char EXE direct download likely trojan (multiple families)	49738	80	192.168.2.3	89.208.107.216

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2022 10:37:51.845873117 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:51.908421040 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:51.908559084 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:51.908721924 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:51.908723116 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:51.971393108 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:51.979885101 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:51.979959011 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:51.980001926 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:51.980045080 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:51.980077028 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:51.980113983 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:51.980151892 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:51.980194092 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:51.980237961 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:51.980257034 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:51.980298996 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:51.980341911 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:51.980359077 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:51.980402946 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:51.980447054 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:52.042936087 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.043060064 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.043106079 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.043148041 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.043189049 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.043230057 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.043272972 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.043304920 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:52.043359041 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.043401003 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.043442965 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.043495893 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.043507099 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:52.043550014 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.043571949 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:52.043612003 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.043638945 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:52.043677092 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.043720007 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.043765068 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:52.043782949 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.043843985 CET	80	49702	77.232.37.228	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2022 10:37:52.043864012 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:52.043910980 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.043976068 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.044011116 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:52.044044018 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.044106007 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:52.106694937 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.106735945 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.106751919 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.106765032 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.106777906 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.106794119 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.106828928 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.106846094 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.106869936 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.106910944 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:52.106930017 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:52.106949091 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.106971025 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.106988907 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.106998920 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:52.107016087 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.107033014 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.107044935 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:52.107058048 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.107075930 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.107085943 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:52.107103109 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.107119083 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:52.107126951 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.107144117 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.107160091 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.107171059 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:52.107186079 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.107206106 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.107212067 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:52.107228994 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.107244968 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:52.107253075 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.107265949 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.107283115 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.107295990 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.107309103 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.107316971 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:52.107333899 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.107342005 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:52.107357979 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.107377052 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.107382059 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:52.107399940 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.107408047 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:52.107424974 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.107441902 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.107454062 CET	49702	80	192.168.2.3	77.232.37.228
Nov 19, 2022 10:37:52.107465982 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.107482910 CET	80	49702	77.232.37.228	192.168.2.3
Nov 19, 2022 10:37:52.107491970 CET	49702	80	192.168.2.3	77.232.37.228

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 19, 2022 10:37:51.433576107 CET	192.168.2.3	8.8.8.8	0xde57	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:37:52.290333033 CET	192.168.2.3	8.8.8.8	0x6ed	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:37:52.727514982 CET	192.168.2.3	8.8.8.8	0xb42c	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:37:53.275449991 CET	192.168.2.3	8.8.8.8	0x3f2a	Standard query (0)	srshf.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:37:54.221432924 CET	192.168.2.3	8.8.8.8	0xb96b	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:37:54.780044079 CET	192.168.2.3	8.8.8.8	0xb58b	Standard query (0)	iplogger.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:37:54.952774048 CET	192.168.2.3	8.8.8.8	0xadca	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:37:55.115462065 CET	192.168.2.3	8.8.8.8	0xe594	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:37:55.278120995 CET	192.168.2.3	8.8.8.8	0x8e00	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:37:55.443361044 CET	192.168.2.3	8.8.8.8	0xd493	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:37:55.848453999 CET	192.168.2.3	8.8.8.8	0x20c4	Standard query (0)	1ecosolution.it	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:03.417083025 CET	192.168.2.3	8.8.8.8	0x8bf5	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:03.578258038 CET	192.168.2.3	8.8.8.8	0xf694	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:04.012542009 CET	192.168.2.3	8.8.8.8	0xb8a2	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:04.179675102 CET	192.168.2.3	8.8.8.8	0x921c	Standard query (0)	cdn-102.anonfiles.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:04.402832031 CET	192.168.2.3	8.8.8.8	0xb4b4	Standard query (0)	anonfiles.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:04.594675064 CET	192.168.2.3	8.8.8.8	0xd613	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:04.767508030 CET	192.168.2.3	8.8.8.8	0x3427	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:04.926534891 CET	192.168.2.3	8.8.8.8	0xf816	Standard query (0)	bitbucket.org	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:05.481759071 CET	192.168.2.3	8.8.8.8	0xdbc8	Standard query (0)	bbuseruploads.s3.amazonaws.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:09.012053967 CET	192.168.2.3	8.8.8.8	0x5215	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:09.198158979 CET	192.168.2.3	8.8.8.8	0xf417	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:10.570333958 CET	192.168.2.3	8.8.8.8	0x1f89	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:10.754020929 CET	192.168.2.3	8.8.8.8	0x9505	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:10.966792107 CET	192.168.2.3	8.8.8.8	0x729c	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:11.164679050 CET	192.168.2.3	8.8.8.8	0x18e2	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:14.707420111 CET	192.168.2.3	8.8.8.8	0xf502	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:14.869998932 CET	192.168.2.3	8.8.8.8	0xc662	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:15.042428970 CET	192.168.2.3	8.8.8.8	0x79af	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:15.238451004 CET	192.168.2.3	8.8.8.8	0x4cf3	Standard query (0)	hoteldostyk.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:20.819649935 CET	192.168.2.3	8.8.8.8	0x17f0	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:21.034486055 CET	192.168.2.3	8.8.8.8	0x3ce7	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:21.249598980 CET	192.168.2.3	8.8.8.8	0x7709	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 19, 2022 10:38:22.885689974 CET	192.168.2.3	8.8.8.8	0x88fc	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:23.094655037 CET	192.168.2.3	8.8.8.8	0xe063	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:25.949970007 CET	192.168.2.3	8.8.8.8	0x6f70	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:27.010088921 CET	192.168.2.3	8.8.8.8	0x8425	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:27.258568048 CET	192.168.2.3	8.8.8.8	0x5b74	Standard query (0)	cdn-104.anonfiles.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:27.536580086 CET	192.168.2.3	8.8.8.8	0xe85a	Standard query (0)	anonfiles.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:27.761984110 CET	192.168.2.3	8.8.8.8	0x7097	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:28.066414118 CET	192.168.2.3	8.8.8.8	0x699e	Standard query (0)	u.to	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:28.602567911 CET	192.168.2.3	8.8.8.8	0x8382	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:29.239953995 CET	192.168.2.3	8.8.8.8	0xf8cc	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:29.435972929 CET	192.168.2.3	8.8.8.8	0xa3aa	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:29.613445044 CET	192.168.2.3	8.8.8.8	0x140	Standard query (0)	github.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:29.890120029 CET	192.168.2.3	8.8.8.8	0x10c6	Standard query (0)	raw.githubusercontent.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:30.736552000 CET	192.168.2.3	8.8.8.8	0x350b	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:30.898178101 CET	192.168.2.3	8.8.8.8	0x4ee1	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:31.088722944 CET	192.168.2.3	8.8.8.8	0xe6ab	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:31.256349087 CET	192.168.2.3	8.8.8.8	0x15a9	Standard query (0)	github.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:31.377008915 CET	192.168.2.3	8.8.8.8	0xa5d6	Standard query (0)	raw.githubusercontent.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:32.301501989 CET	192.168.2.3	8.8.8.8	0xdb7a	Standard query (0)	o36fafs3sn6xou.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:40.929582119 CET	192.168.2.3	8.8.8.8	0xc0c4	Standard query (0)	t.me	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:39:04.991622925 CET	192.168.2.3	8.8.8.8	0x8afc	Standard query (0)	svedbergbryanthusnonarithmetical.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:39:05.429963112 CET	192.168.2.3	8.8.8.8	0x8218	Standard query (0)	www.youtube.com	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:39:06.277318954 CET	192.168.2.3	8.8.8.8	0x6334	Standard query (0)	2w3ke1f81kujb1erhj396kfejh2wgw.kgpoaj9k4sgjd4aitghsrtuxhq	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:39:12.060153961 CET	192.168.2.3	8.8.8.8	0xde8f	Standard query (0)	t.me	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:39:14.078975916 CET	192.168.2.3	8.8.8.8	0xe667	Standard query (0)	lentaphoto.at	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 10:36:51.095769882 CET	8.8.8.8	192.168.2.3	0xeec5	No error (0)	windowsupdatebg.s.llnwi.net		178.79.225.0	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:36:51.095769882 CET	8.8.8.8	192.168.2.3	0xeec5	No error (0)	windowsupdatebg.s.llnwi.net		95.140.230.192	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:37:51.842966080 CET	8.8.8.8	192.168.2.3	0xde57	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:37:52.583683014 CET	8.8.8.8	192.168.2.3	0x6ed	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 10:37:53.134239912 CET	8.8.8.8	192.168.2.3	0xb42c	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:37:53.431488991 CET	8.8.8.8	192.168.2.3	0x3f2a	No error (0)	srshf.com		108.167.141.212	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:37:54.634073973 CET	8.8.8.8	192.168.2.3	0xb96b	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:37:54.805392027 CET	8.8.8.8	192.168.2.3	0xb58b	No error (0)	iplogger.com		148.251.234.93	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:37:54.972848892 CET	8.8.8.8	192.168.2.3	0xadca	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:37:55.133872986 CET	8.8.8.8	192.168.2.3	0xe594	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:37:55.295975924 CET	8.8.8.8	192.168.2.3	0x8e00	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:37:55.703301907 CET	8.8.8.8	192.168.2.3	0xd493	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:37:55.883002043 CET	8.8.8.8	192.168.2.3	0x20c4	No error (0)	1ecosolution.it		46.252.148.24	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:03.435493946 CET	8.8.8.8	192.168.2.3	0x8bf5	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:03.871123075 CET	8.8.8.8	192.168.2.3	0xf694	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:04.030489922 CET	8.8.8.8	192.168.2.3	0xb8a2	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:04.214128971 CET	8.8.8.8	192.168.2.3	0x921c	No error (0)	cdn-102.anonfiles.com		195.96.151.51	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:04.422077894 CET	8.8.8.8	192.168.2.3	0xb4b4	No error (0)	anonfiles.com		45.154.253.151	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:04.422077894 CET	8.8.8.8	192.168.2.3	0xb4b4	No error (0)	anonfiles.com		45.154.253.152	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:04.422077894 CET	8.8.8.8	192.168.2.3	0xb4b4	No error (0)	anonfiles.com		45.154.253.150	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:04.615020037 CET	8.8.8.8	192.168.2.3	0xd613	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:04.785401106 CET	8.8.8.8	192.168.2.3	0x3427	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:04.950486898 CET	8.8.8.8	192.168.2.3	0xf816	No error (0)	bitbucket.org		104.192.141.1	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:05.499828100 CET	8.8.8.8	192.168.2.3	0xdbc8	No error (0)	bbuseruploads.s3.amazonaws.com	s3-1-w.amazonaws.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 19, 2022 10:38:05.499828100 CET	8.8.8.8	192.168.2.3	0xdbc8	No error (0)	s3-1-w.amazonaws.com	s3-w.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 19, 2022 10:38:05.499828100 CET	8.8.8.8	192.168.2.3	0xdbc8	No error (0)	s3-w.us-east-1.amazonaws.com		52.217.206.73	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:05.499828100 CET	8.8.8.8	192.168.2.3	0xdbc8	No error (0)	s3-w.us-east-1.amazonaws.com		3.5.16.107	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:05.499828100 CET	8.8.8.8	192.168.2.3	0xdbc8	No error (0)	s3-w.us-east-1.amazonaws.com		52.216.24.52	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:05.499828100 CET	8.8.8.8	192.168.2.3	0xdbc8	No error (0)	s3-w.us-east-1.amazonaws.com		52.217.13.228	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 10:38:05.499828100 CET	8.8.8.8	192.168.2.3	0xdbc8	No error (0)	s3-w.us-east-1.amazonaws.com		3.5.3.100	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:05.499828100 CET	8.8.8.8	192.168.2.3	0xdbc8	No error (0)	s3-w.us-east-1.amazonaws.com		54.231.137.17	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:05.499828100 CET	8.8.8.8	192.168.2.3	0xdbc8	No error (0)	s3-w.us-east-1.amazonaws.com		52.216.214.81	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:05.499828100 CET	8.8.8.8	192.168.2.3	0xdbc8	No error (0)	s3-w.us-east-1.amazonaws.com		52.216.88.171	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:09.030143976 CET	8.8.8.8	192.168.2.3	0x5215	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:09.215954065 CET	8.8.8.8	192.168.2.3	0xf417	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:10.590337038 CET	8.8.8.8	192.168.2.3	0x1f89	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:10.773845911 CET	8.8.8.8	192.168.2.3	0x9505	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:10.987179995 CET	8.8.8.8	192.168.2.3	0x729c	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:11.184869051 CET	8.8.8.8	192.168.2.3	0x18e2	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:14.725869894 CET	8.8.8.8	192.168.2.3	0xf502	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:14.890060902 CET	8.8.8.8	192.168.2.3	0xc662	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:15.060513020 CET	8.8.8.8	192.168.2.3	0x79af	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:15.701762915 CET	8.8.8.8	192.168.2.3	0x4cf3	No error (0)	hoteldostyk.com		43.231.112.109	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:20.839776039 CET	8.8.8.8	192.168.2.3	0x17f0	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:21.054763079 CET	8.8.8.8	192.168.2.3	0x3ce7	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:21.270658016 CET	8.8.8.8	192.168.2.3	0x7709	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:22.904759884 CET	8.8.8.8	192.168.2.3	0x88fc	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:23.112772942 CET	8.8.8.8	192.168.2.3	0xe063	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:25.967694998 CET	8.8.8.8	192.168.2.3	0x6f70	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:27.029911995 CET	8.8.8.8	192.168.2.3	0x8425	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:27.286843061 CET	8.8.8.8	192.168.2.3	0x5b74	No error (0)	cdn-104.anonfiles.com		195.96.151.53	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:27.554032087 CET	8.8.8.8	192.168.2.3	0xe85a	No error (0)	anonfiles.com		45.154.253.151	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:27.554032087 CET	8.8.8.8	192.168.2.3	0xe85a	No error (0)	anonfiles.com		45.154.253.152	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:27.554032087 CET	8.8.8.8	192.168.2.3	0xe85a	No error (0)	anonfiles.com		45.154.253.150	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 10:38:27.779742002 CET	8.8.8.8	192.168.2.3	0x7097	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:28.087229967 CET	8.8.8.8	192.168.2.3	0x699e	No error (0)	u.to		195.216.243.155	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:28.625432014 CET	8.8.8.8	192.168.2.3	0x8382	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:28.625432014 CET	8.8.8.8	192.168.2.3	0x8382	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:28.625432014 CET	8.8.8.8	192.168.2.3	0x8382	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:28.625432014 CET	8.8.8.8	192.168.2.3	0x8382	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:28.625432014 CET	8.8.8.8	192.168.2.3	0x8382	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:29.258445978 CET	8.8.8.8	192.168.2.3	0xf8cc	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:29.455861092 CET	8.8.8.8	192.168.2.3	0xa3aa	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:29.644002914 CET	8.8.8.8	192.168.2.3	0x140	No error (0)	github.com		140.82.121.4	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:29.907610893 CET	8.8.8.8	192.168.2.3	0x10c6	No error (0)	raw.githubusercontent.com		185.199.108.133	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:29.907610893 CET	8.8.8.8	192.168.2.3	0x10c6	No error (0)	raw.githubusercontent.com		185.199.109.133	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:29.907610893 CET	8.8.8.8	192.168.2.3	0x10c6	No error (0)	raw.githubusercontent.com		185.199.110.133	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:29.907610893 CET	8.8.8.8	192.168.2.3	0x10c6	No error (0)	raw.githubusercontent.com		185.199.111.133	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:30.754844904 CET	8.8.8.8	192.168.2.3	0x350b	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:30.916239977 CET	8.8.8.8	192.168.2.3	0x4ee1	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:31.107050896 CET	8.8.8.8	192.168.2.3	0xe6ab	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:31.276186943 CET	8.8.8.8	192.168.2.3	0x15a9	No error (0)	github.com		140.82.121.3	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:31.396316051 CET	8.8.8.8	192.168.2.3	0xa5d6	No error (0)	raw.githubusercontent.com		185.199.108.133	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:31.396316051 CET	8.8.8.8	192.168.2.3	0xa5d6	No error (0)	raw.githubusercontent.com		185.199.109.133	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:31.396316051 CET	8.8.8.8	192.168.2.3	0xa5d6	No error (0)	raw.githubusercontent.com		185.199.110.133	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:31.396316051 CET	8.8.8.8	192.168.2.3	0xa5d6	No error (0)	raw.githubusercontent.com		185.199.111.133	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:32.319535017 CET	8.8.8.8	192.168.2.3	0xdb7a	No error (0)	o36fafs3sn6xou.com		77.232.37.228	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:38:40.947027922 CET	8.8.8.8	192.168.2.3	0xc0c4	No error (0)	t.me		149.154.167.99	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 10:39:05.010046005 CET	8.8.8.8	192.168.2.3	0x8afc	No error (0)	svedbergbryanthusnonarithmetical.com		84.21.172.142	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:39:05.447870016 CET	8.8.8.8	192.168.2.3	0x8218	No error (0)	www.youtube.com	youtube-ui.l.google.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 19, 2022 10:39:05.447870016 CET	8.8.8.8	192.168.2.3	0x8218	No error (0)	youtube-ui.l.google.com		172.217.168.14	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:39:05.447870016 CET	8.8.8.8	192.168.2.3	0x8218	No error (0)	youtube-ui.l.google.com		172.217.168.46	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:39:05.447870016 CET	8.8.8.8	192.168.2.3	0x8218	No error (0)	youtube-ui.l.google.com		172.217.168.78	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:39:05.447870016 CET	8.8.8.8	192.168.2.3	0x8218	No error (0)	youtube-ui.l.google.com		142.250.203.110	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:39:05.447870016 CET	8.8.8.8	192.168.2.3	0x8218	No error (0)	youtube-ui.l.google.com		216.58.215.238	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:39:06.295533895 CET	8.8.8.8	192.168.2.3	0x6334	Name error (3)	2w3ke1f81kujb1erhj396kfejh2wgw.kgpoaj9k4sgjd4aitghsrtuxhq	none	none	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:39:12.079382896 CET	8.8.8.8	192.168.2.3	0xde8f	No error (0)	t.me		149.154.167.99	A (IP address)	IN (0x0001)	false
Nov 19, 2022 10:39:14.447832108 CET	8.8.8.8	192.168.2.3	0xe667	Server failure (2)	lentaphoto.at	none	none	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

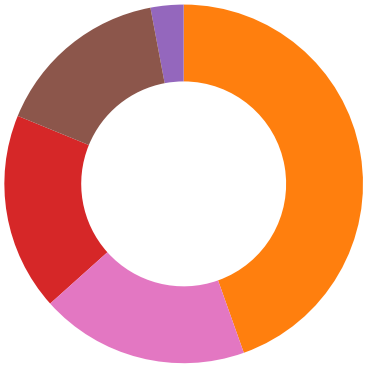
- srshf.com
- iplogger.com
- cdn-102.anonfiles.com
- anonfiles.com
- bitbucket.org
- bbuseruploads.s3.amazonaws.com
- transfer.sh
- hoteldostyk.com
- cdn-104.anonfiles.com
- u.to
- cdn.discordapp.com
- github.com
- raw.githubusercontent.com
- t.me
- debvplifcf.com

- o36fafs3sn6xou.com
- kpswfp.com
- sdins.com
- auypktwjk.net
- ebvtwkfux.com
- hqmym.org
- datryh.net
- ajpfnqvlq.net
- sxihacbmgi.com
- upkkyf.com
- hgusiwjl.com
- ulciihlbw.org
- bjtfrvl.com
- vvydl.com
- jtmdotimkr.org
- 193.56.146.168
- gsqxoged.net
- ahgwjjm.org
- efngjyqy.org
- ukkwrl.org
- ebaxoe.net
- eqghptenl.com
- ptpfdpcirh.net
- etebl.net
- aexqt.org
- aehnv.net
- 89.208.107.216
- fbybhia.org
- fhkewyoq.net
- mqfbhqf.com

- acxiqgb.org
- xawdohy.net
- uvlvsvw.com
- jorxt.net
- syohyc.net
- cbmlqnw.com
- 116.202.5.101
- 193.56.146.174

Statistics

Behavior



- S2XJ2wbz7u.exe
- explorer.exe
- tiddsjj
- 2B4A.exe
- 3790.exe
- 453D.exe
- rovwer.exe
- 59FE.exe
- 6644.exe
- schtasks.exe
- 6CEC.exe
- conhost.exe
- cmd.exe
- conhost.exe
- conhost.exe
- 816F.exe
- cmd.exe
- rovwer.exe
- cacls.exe
- 86EE.exe
- cacls.exe
- 8C00.exe
- vbc.exe
- 86EE.exe
- explorer.exe
- cmd.exe
- cacls.exe
- explorer.exe
- 8C00.exe
- explorer.exe
- cacls.exe
- explorer.exe
- 86EE.exe
- explorer.exe

Click to jump to process

System Behavior

Analysis Process: S2XJ2wbz7u.exe PID: **6020**, Parent PID: **3452**

General

Target ID:	0
Start time:	10:36:56
Start date:	19/11/2022
Path:	C:\Users\user\Desktop\S2XJ2wbz7u.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\S2XJ2wbz7u.exe
Imagebase:	0x400000
File size:	343552 bytes
MD5 hash:	FFB4CF34B38F126C917E1C1E1D26DF73
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: 00000000.00000003.246440191.0000000000870000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.327477801.000000000D61000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.327477801.000000000D61000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.326943587.0000000000860000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000000.00000002.327296717.00000000009C0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000000.00000002.327296717.00000000009C0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000000.00000002.327031304.0000000000891000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: explorer.exe PID: **3452**, Parent PID: **6020**

General

Target ID:	1
Start time:	10:37:05
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: 00000001.00000000.308924439.0000000003321000.00000020.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 00000001.00000000.308924439.0000000003321000.00000020.80000000.00040000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

Analysis Process: tiddsjj PID: **3152**, Parent PID: **1080**

General

Target ID:	11
Start time:	10:37:52
Start date:	19/11/2022
Path:	C:\Users\user\AppData\Roaming\tiddsjj
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\tiddsjj
Imagebase:	0x400000
File size:	343552 bytes
MD5 hash:	FFB4CF34B38F126C917E1C1E1D26DF73

Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 0000000B.00000002.378510967.0000000000930000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000B.00000002.378663629.0000000000B41000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000B.00000002.378864135.0000000002611000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000000B.00000002.378864135.0000000002611000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000B.00000003.366967601.0000000000950000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000000B.00000002.378578278.00000000009E0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000000B.00000002.378578278.00000000009E0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: 2B4A.exe PID: **5260**, Parent PID: **3452**

General

Target ID:	12
Start time:	10:38:07
Start date:	19/11/2022
Path:	C:\Users\user\AppData\Local\Temp\2B4A.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\2B4A.exe
Imagebase:	0x400000
File size:	300544 bytes
MD5 hash:	2DEE200193091BE2F2321D921750C4ED
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: 0000000C.00000003.399248246.0000000000856000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000C.00000002.593637539.00000000029CB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000C.00000003.397792222.0000000000780000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 0000000C.00000003.397792222.0000000000780000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000C.00000002.561654188.000000000227A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000C.00000002.582776721.0000000002540000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 0000000C.00000002.582776721.0000000002540000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000C.00000002.526298773.0000000000740000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 0000000C.00000002.526298773.0000000000740000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000C.00000002.517740314.0000000000400000.00000040.00000001.01000000.00000009.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 0000000C.00000002.517740314.0000000000400000.00000040.00000001.01000000.00000009.sdmp, Author: ditekSHen • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000C.00000002.590764503.0000000002840000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_RedLine, Description: Detects RedLine infostealer, Source: 0000000C.00000002.590764503.0000000002840000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000C.00000002.540373176.00000000007D6000.00000040.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: NaN%, Metadefender, Browse • Detection: 73%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3CCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3CCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C211B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C211B4F	ReadFile

Analysis Process: 3790.exe PID: **2336**, Parent PID: **3452**

General

Target ID:	13
Start time:	10:38:10
Start date:	19/11/2022
Path:	C:\Users\user\AppData\Local\Temp\3790.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\3790.exe
Imagebase:	0x400000
File size:	382464 bytes
MD5 hash:	5E08968D858224A33175069D64DC7F39
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 0000000D.00000002.415736878.0000000000870000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000D.00000002.419975883.0000000000A61000.00000040.00000020.00020000.00000000.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
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 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 ef fd 61 00 00 00 00 00 00 00 00 fd 00 02	MZ@!L!This program cannot be run in DOS mode.$P1x1x1xc1xc!1xc1x1xy1xc1xc1xc1xRich1xPELa	success or wait	3	40B78F	CopyFileA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: 453D.exe PID: **4024**, Parent PID: **3452**

General

Target ID:	14
Start time:	10:38:13
Start date:	19/11/2022
Path:	C:\Users\user\AppData\Local\Temp\453D.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\453D.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: 0000000E.00000002.557498334.0000000000774000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 21%, ReversingLabs
Reputation:	low

Analysis Process: rovwer.exe PID: **4764**, Parent PID: **2336**

General

Target ID:	15
Start time:	10:38:16
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:	382464 bytes
MD5 hash:	5E08968D858224A33175069D64DC7F39
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: 0000000F.00000002.556830130.0000000000B4C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey, Description: Yara detected Amadey bot, Source: 0000000F.00000002.542120947.0000000000AB0000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Amadey, Description: Yara detected Amadey bot, Source: 0000000F.00000002.555134587.0000000000B33000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 0000000F.00000002.538954387.0000000000A91000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Amadey_2, Description: Yara detected Amadey\'s stealer DLL, Source: 0000000F.00000002.551885520.0000000000AFF000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 0000000F.00000002.529416121.0000000000980000.00000040.00001000.00020000.00000000.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\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
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	1	41F5C3	DeleteFileW

File Written

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 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	MZP@!L!This program must be run under Win32$7	success or wait	8	408C17	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 3b 5f 5e 5b cb 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 fd 0f 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 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 04 4e 75 fd 5e 5b cd 40 00 fd fd 0f fd fd fd fd fd 4a fd fd fd 0f fd fd fd fd fd 51 52 50 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	20508	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: 59FE.exe PID: **5228**, Parent PID: **3452**

General

Target ID:	16
Start time:	10:38:19
Start date:	19/11/2022
Path:	C:\Users\user\AppData\Local\Temp\59FE.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\59FE.exe
Imagebase:	0x7ff74a220000
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
Reputation:	low

Analysis Process: 6644.exe PID: **1916**, Parent PID: **3452**

General

Target ID:	19
Start time:	10:38:22
Start date:	19/11/2022

Path:	C:\Users\user\AppData\Local\Temp\6644.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\6644.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: Windows_Trojan_RedLineStealer_ed346e4c, Description: unknown, Source: 00000013.00000002.535069692.0000000000B01000.00000040.00000020.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000013.00000002.556838350.0000000001279000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000013.00000002.525358193.0000000000930000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000013.00000002.560249916.0000000001858000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Gozi_fd494041, Description: unknown, Source: 00000013.00000002.560249916.0000000001858000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Gozi_261f5ac5, Description: unknown, Source: 00000013.00000002.560249916.0000000001858000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: schtasks.exe PID: **1396**, Parent PID: **4764**

General

Target ID:	20
Start time:	10:38:23
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:	0xaf0000
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: 6CEC.exe PID: **4968**, Parent PID: **3452**

General

Target ID:	21
Start time:	10:38:23
Start date:	19/11/2022
Path:	C:\Users\user\AppData\Local\Temp\6CEC.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\6CEC.exe
Imagebase:	0x400000
File size:	360448 bytes
MD5 hash:	28A6112DCB54CE6886F7D9ACB8A15E31
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
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

Analysis Process: conhost.exe PID: **2992**, Parent PID: **1396**

General

Target ID:	22
Start time:	10:38:24
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: **5972**, Parent PID: **4764**

General

Target ID:	23
Start time:	10:38:25
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: **408**, Parent PID: **4968**

General

Target ID:	24
Start time:	10:38:26
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: conhost.exe PID: **2436**, Parent PID: **5972**

General

Target ID:	25
Start time:	10:38:27
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: 816F.exe PID: **1172**, Parent PID: **3452**

General

Target ID:	26
Start time:	10:38:28
Start date:	19/11/2022
Path:	C:\Users\user\AppData\Local\Temp\816F.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\816F.exe
Imagebase:	0x190000
File size:	228864 bytes
MD5 hash:	730A7A6F235525238EE33A2C046C2BA7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3CCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3CCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3A5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3003DE	ReadFile
C:\Users\user\AppData\Local\Temp\816F.exe	unknown	4096	success or wait	1	6D38D72F	unknown
C:\Users\user\AppData\Local\Temp\816F.exe	unknown	512	success or wait	1	6D38D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C211B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C211B4F	ReadFile

Analysis Process: cmd.exe PID: **3012**, Parent PID: **5972**

General

Target ID:	27
Start time:	10:38:29
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

Analysis Process: rovwer.exe PID: **2560**, Parent PID: **1080**

General

Target ID:	28
Start time:	10:38:29
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:	382464 bytes
MD5 hash:	5E08968D858224A33175069D64DC7F39
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cacls.exe PID: **4392**, Parent PID: **5972**

General

Target ID:	29
Start time:	10:38:30

Start date:	19/11/2022
Path:	C:\Windows\SysWOW64\cacls.exe
Wow64 process (32bit):	true
Commandline:	CACLS "rovwer.exe" /P "user:N"
Imagebase:	0xc10000
File size:	27648 bytes
MD5 hash:	4CBB1C027DF71C53A8EE4C855FD35B25
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: 86EE.exe PID: **4972**, Parent PID: **3452**

General

Target ID:	30
Start time:	10:38:30
Start date:	19/11/2022
Path:	C:\Users\user\AppData\Local\Temp\86EE.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\86EE.exe
Imagebase:	0x900000
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: 0000001E.00000002.456037519.0000000001560000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: cacls.exe PID: **4984**, Parent PID: **5972**

General

Target ID:	31
Start time:	10:38:31
Start date:	19/11/2022
Path:	C:\Windows\SysWOW64\cacls.exe
Wow64 process (32bit):	true
Commandline:	CACLS "rovwer.exe" /P "user:R" /E
Imagebase:	0xc10000
File size:	27648 bytes
MD5 hash:	4CBB1C027DF71C53A8EE4C855FD35B25
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: 8C00.exe PID: **5400**, Parent PID: **3452**

General

Target ID:	32
Start time:	10:38:31
Start date:	19/11/2022
Path:	C:\Users\user\AppData\Local\Temp\8C00.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\8C00.exe
Imagebase:	0xbf0000
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: 00000020.00000002.457565511.00000000012D0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: vbc.exe PID: **5496**, Parent PID: **4968**

General	
Target ID:	33
Start time:	10:38:32
Start date:	19/11/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\vbc.exe
Imagebase:	0x1280000
File size:	2688096 bytes
MD5 hash:	B3A917344F5610BEEC562556F11300FA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: 86EE.exe PID: **5560**, Parent PID: **4972**

General	
Target ID:	34
Start time:	10:38:32
Start date:	19/11/2022
Path:	C:\Users\user\AppData\Local\Temp\86EE.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\86EE.exe
Imagebase:	0x900000
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: 00000022.00000002.463148223.0000000000910000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: explorer.exe PID: **5612**, Parent PID: **3452**

General	
Target ID:	35
Start time:	10:38:32
Start date:	19/11/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xc20000
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: 00000023.00000000.445464817.0000000003270000.00000040.80000000.00040000.00000000.sdmp, Author: unknown

Analysis Process: cmd.exe PID: **5640**, Parent PID: **5972**

General	
Target ID:	36
Start time:	10:38:32
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

Analysis Process: cacls.exe PID: **5668**, Parent PID: **5972**

General	
Target ID:	37
Start time:	10:38:32
Start date:	19/11/2022
Path:	C:\Windows\SysWOW64\cacls.exe
Wow64 process (32bit):	true
Commandline:	CACLS "..\99e342142d" /P "user:N"
Imagebase:	0xc10000
File size:	27648 bytes
MD5 hash:	4CBB1C027DF71C53A8EE4C855FD35B25
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: **5928**, Parent PID: **3452**

General	
Target ID:	40
Start time:	10:38:34
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: 8C00.exe PID: **5936**, Parent PID: **5400**

General	
Target ID:	41
Start time:	10:38:34

Start date:	19/11/2022
Path:	C:\Users\user\AppData\Local\Temp\8C00.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\8C00.exe
Imagebase:	0xbf0000
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: 00000029.00000002.464734781.00000000008F0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

Analysis Process: explorer.exe PID: 1768, Parent PID: 3452

General

Target ID:	42
Start time:	10:38:35
Start date:	19/11/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xc20000
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: JoeSecurity_SmokeLoader, Description: Yara detected SmokeLoader, Source: 0000002A.00000002.520066119.0000000000591000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_4e31426e, Description: unknown, Source: 0000002A.00000000.451638661.00000000005A0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown

Analysis Process: cacls.exe PID: 3124, Parent PID: 5972

General

Target ID:	43
Start time:	10:38:35
Start date:	19/11/2022
Path:	C:\Windows\SysWOW64\cacls.exe
Wow64 process (32bit):	true
Commandline:	CACLS "..\99e342142d" /P "user:R" /E
Imagebase:	0xc10000
File size:	27648 bytes
MD5 hash:	4CBB1C027DF71C53A8EE4C855FD35B25
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: 5080, Parent PID: 3452

General

Target ID:	44
Start time:	10:38:36
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: 0000002C.00000002.520020559.00000000003D1000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security

Analysis Process: 86EE.exe PID: **5068**, Parent PID: **5560**

General	
Target ID:	45
Start time:	10:38:38
Start date:	19/11/2022
Path:	C:\Users\user\AppData\Local\Temp\86EE.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\86EE.exe
Imagebase:	0x900000
File size:	341006 bytes
MD5 hash:	F46063253FF38E6B2452BF4410C5FEC0
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: explorer.exe PID: **3780**, Parent PID: **3452**

General	
Target ID:	46
Start time:	10:38:38
Start date:	19/11/2022
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xc20000
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: 0000002E.00000000.457780298.00000000032C0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown

Disassembly

No disassembly