ID: 1443534
Sample Name: file.exe
Cookbook: default.jbs
Time: 23:44:10
Date: 17/05/2024
Version: 40.0.0 Tourmaline

Table of Contents

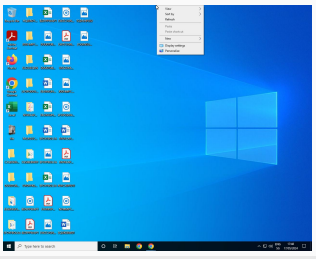
Windows Analysis Report

file.exe

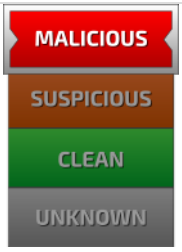
Overview

General Information

Sample name:	file.exe
Analysis ID:	1443534
MD5:	3d0973984654…
SHA1:	2247e38b1f525..
SHA256:	70aaa6e67944…
Tags:	exe
Infos:	



Detection



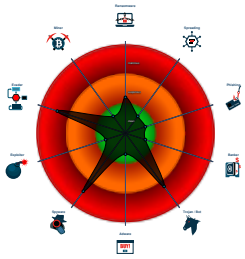
Clipboard Hijacker, RisePro Stealer

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

Signatures

- Antivirus detection for dropped file
- Detected unpacking (changes PE se…
- Malicious sample detected (through…
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Yara detected Clipboard Hijacker
- Yara detected RisePro Stealer
- Machine Learning detection for sam…
- Overwrites code with unconditional j…
- PE file contains section with specia…
- Tries to detect virtualization through…
- Tries to harvest and steal browser in…

Classification



Process Tree

- **System is w10x64**
- file.exe (PID: 4112 cmdline: "C:\Users\user\Desktop\file.exe" MD5: 3D09739846543F4962F2B432DA671C29)
  - schtasks.exe (PID: 3692 cmdline: schtasks /create /f /RU "user" /tr "C:\ProgramData\MSIUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26\MSIUpdaterV2.exe" /tn "MSIUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26 HR" /sc HOURLY /rl HIGHEST MD5: 48C2FE20575769DE916F48EF0676A965)
    - conhost.exe (PID: 5068 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - schtasks.exe (PID: 6668 cmdline: schtasks /create /f /RU "user" /tr "C:\ProgramData\MSIUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26\MSIUpdaterV2.exe" /tn "MSIUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26 LG" /sc ONLOGON /rl HIGHEST MD5: 48C2FE20575769DE916F48EF0676A965)
    - conhost.exe (PID: 4500 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
  - llmcrdwzLnNKYB4T0Vnw.exe (PID: 7056 cmdline: "C:\Users\user\AppData\Local\Temp\span1UB98D2D2zeo\llmcrdwzLnNKYB4T0Vnw.exe" MD5: AF6E384DFABDAD52D43CF8429AD8779C)
    - schtasks.exe (PID: 5728 cmdline: /C /create /F /sc minute /mo 1 /tn "Telemetry Logging" /tr "C:\Users\user\AppData\Roaming\Microsoft\Protect\oobeldr.exe" MD5: 48C2FE20575769DE916F48EF0676A965)
      - conhost.exe (PID: 4748 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
- MSIUpdaterV2.exe (PID: 6504 cmdline: C:\ProgramData\MSIUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26\MSIUpdaterV2.exe MD5: AF6E384DFABDAD52D43CF8429AD8779C)
  - schtasks.exe (PID: 6968 cmdline: /C /create /F /sc minute /mo 1 /tn "Telemetry Logging" /tr "C:\Users\user\AppData\Roaming\Microsoft\Protect\oobeldr.exe" MD5: 48C2FE20575769DE916F48EF0676A965)
    - conhost.exe (PID: 6756 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
- MSIUpdaterV2.exe (PID: 1628 cmdline: C:\ProgramData\MSIUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26\MSIUpdaterV2.exe MD5: AF6E384DFABDAD52D43CF8429AD8779C)
- oobeldr.exe (PID: 7044 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Protect\oobeldr.exe MD5: AF6E384DFABDAD52D43CF8429AD8779C)
  - schtasks.exe (PID: 2504 cmdline: /C /create /F /sc minute /mo 1 /tn "Telemetry Logging" /tr "C:\Users\user\AppData\Roaming\Microsoft\Protect\oobeldr.exe" MD5: 48C2FE20575769DE916F48EF0676A965)
    - conhost.exe (PID: 4320 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 0D698AF330FD17BEE3BF90011D49251D)
- AdobeUpdaterV2.exe (PID: 6436 cmdline: "C:\Users\user\AppData\Local\AdobeUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26\AdobeUpdaterV2.exe" MD5: AF6E384DFABDAD52D43CF8429AD8779C)
- AdobeUpdaterV2.exe (PID: 4332 cmdline: "C:\Users\user\AppData\Local\AdobeUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26\AdobeUpdaterV2.exe" MD5: AF6E384DFABDAD52D43CF8429AD8779C)
- EdgeMS2.exe (PID: 2860 cmdline: "C:\Users\user\AppData\Local\Temp\EdgeMS2_45c48cce2e2d7fbdea1afc51c7c6ad26\EdgeMS2.exe" MD5: AF6E384DFABDAD52D43CF8429AD8779C)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\dZGGvSkztfgYu5jqSY21Wne.zip	JoeSecurity_RisePro Stealer	Yara detected RisePro Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000011.00000002.2298062400.0000000000401000.00000020.00000001.01000000.0000000B.sdmp	Windows_Trojan_Clipbanker_f9f9e79d	unknown	unknown	• 0x4c6:$a1: 7E 7E 0F B7 04 77 83 F8 41 74 69 83 F8 42 74 64 83 F8 43 74 5F 83
00000011.00000002.2298062400.0000000000401000.00000020.00000001.01000000.0000000B.sdmp	Windows_Trojan_Clipbanker_787b130b	unknown	unknown	• 0x1354:$mutex_setup: 55 8B EC 83 EC 20 53 56 57 E8 9E EC FF FF 68 30 30 40 00 6A 00 6A 00 FF 15 40 40 40 00 FF 15 2C 40 40 00 3D B7 00 00 00 75 08 6A 00 FF 15 10 30 40 00
00000000.00000002.4445088347.0000000006449000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RisePro Stealer	Yara detected RisePro Stealer	Joe Security	
00000000.00000003.2157362439.00000000061CB000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_RisePro Stealer	Yara detected RisePro Stealer	Joe Security	
00000013.00000002.2460266314.0000000000401000.00000020.00000001.01000000.0000000C.sdmp	Windows_Trojan_Clipbanker_f9f9e79d	unknown	unknown	• 0x4c6:$a1: 7E 7E 0F B7 04 77 83 F8 41 74 69 83 F8 42 74 64 83 F8 43 74 5F 83

Click to see the 13 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.MSIUpdaterV2.exe.400000.0.unpack	JoeSecurity_Clipboard_Hijacker	Yara detected Clipboard Hijacker	Joe Security	
8.2.MSIUpdaterV2.exe.400000.0.unpack	Windows_Trojan_Clipbanker_f9f9e79d	unknown	unknown	• 0x6c6:$a1: 7E 7E 0F B7 04 77 83 F8 41 74 69 83 F8 42 74 64 83 F8 43 74 5F 83
8.2.MSIUpdaterV2.exe.400000.0.unpack	Windows_Trojan_Clipbanker_787b130b	unknown	unknown	• 0x1554:$mutex_setup: 55 8B EC 83 EC 20 53 56 57 E8 9E EC FF FF 68 30 30 40 00 6A 00 6A 00 FF 15 40 40 40 00 FF 15 2C 40 40 00 3D B7 00 00 00 75 08 6A 00 FF 15 10 30 40 00
7.2.MSIUpdaterV2.exe.400000.0.unpack	JoeSecurity_Clipboard_Hijacker	Yara detected Clipboard Hijacker	Joe Security	
7.2.MSIUpdaterV2.exe.400000.0.unpack	Windows_Trojan_Clipbanker_f9f9e79d	unknown	unknown	• 0x6c6:$a1: 7E 7E 0F B7 04 77 83 F8 41 74 69 83 F8 42 74 64 83 F8 43 74 5F 83

Click to see the 16 entries

Sigma Signatures

System Summary

Sigma detected: CurrentVersion Autorun Keys Modification

Sigma detected: Startup Folder File Write

Sigma detected: Suspicious Add Scheduled Task Parent

Sigma detected: Suspicious Schtasks From Env Var Folder

Snort Signatures

ET TROJAN RisePro TCP Heartbeat Packet - Source IP: 192.168.2.5 - Destination IP: 5.42.96.65	
Timestamp:	05/17/24-23:45:00.848746
SID:	2049060
Source Port:	49704
Destination Port:	50500
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (Activity) - Source IP: 192.168.2.5 - Destination IP: 5.42.96.65	
Timestamp:	05/17/24-23:45:05.461512
SID:	2046269
Source Port:	49704
Destination Port:	50500
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP v.0.x (Get_settings) - Source IP: 192.168.2.5 - Destination IP: 5.42.96.65	
Timestamp:	05/17/24-23:45:05.093768
SID:	2046268
Source Port:	49704
Destination Port:	50500
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile - Source IP: 192.168.2.5 - Destination IP: 5.42.96.170	
Timestamp:	05/17/24-23:45:14.161367
SID:	2019714
Source Port:	49707
Destination Port:	80
Protocol:	TCP
Classtype:	Potentially Bad Traffic

ET TROJAN [ANY.RUN] RisePro TCP (External IP) - Source IP: 5.42.96.65 - Destination IP: 192.168.2.5	
Timestamp:	05/17/24-23:45:02.216807
SID:	2046267
Source Port:	50500
Destination Port:	49704
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN [ANY.RUN] RisePro TCP (Token) - Source IP: 5.42.96.65 - Destination IP: 192.168.2.5	
Timestamp:	05/17/24-23:45:01.844974
SID:	2046266
Source Port:	50500
Destination Port:	49704
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

System Summary

Malicious sample detected (through community Yara rule)

PE file contains section with special chars

Data Obfuscation

Detected unpacking (changes PE section rights)

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

Overwrites code with unconditional jumps - possibly settings hooks in foreign process

Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

Stealing of Sensitive Information

Yara detected Clipboard Hijacker

Yara detected RisePro Stealer

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

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

Remote Access Functionality

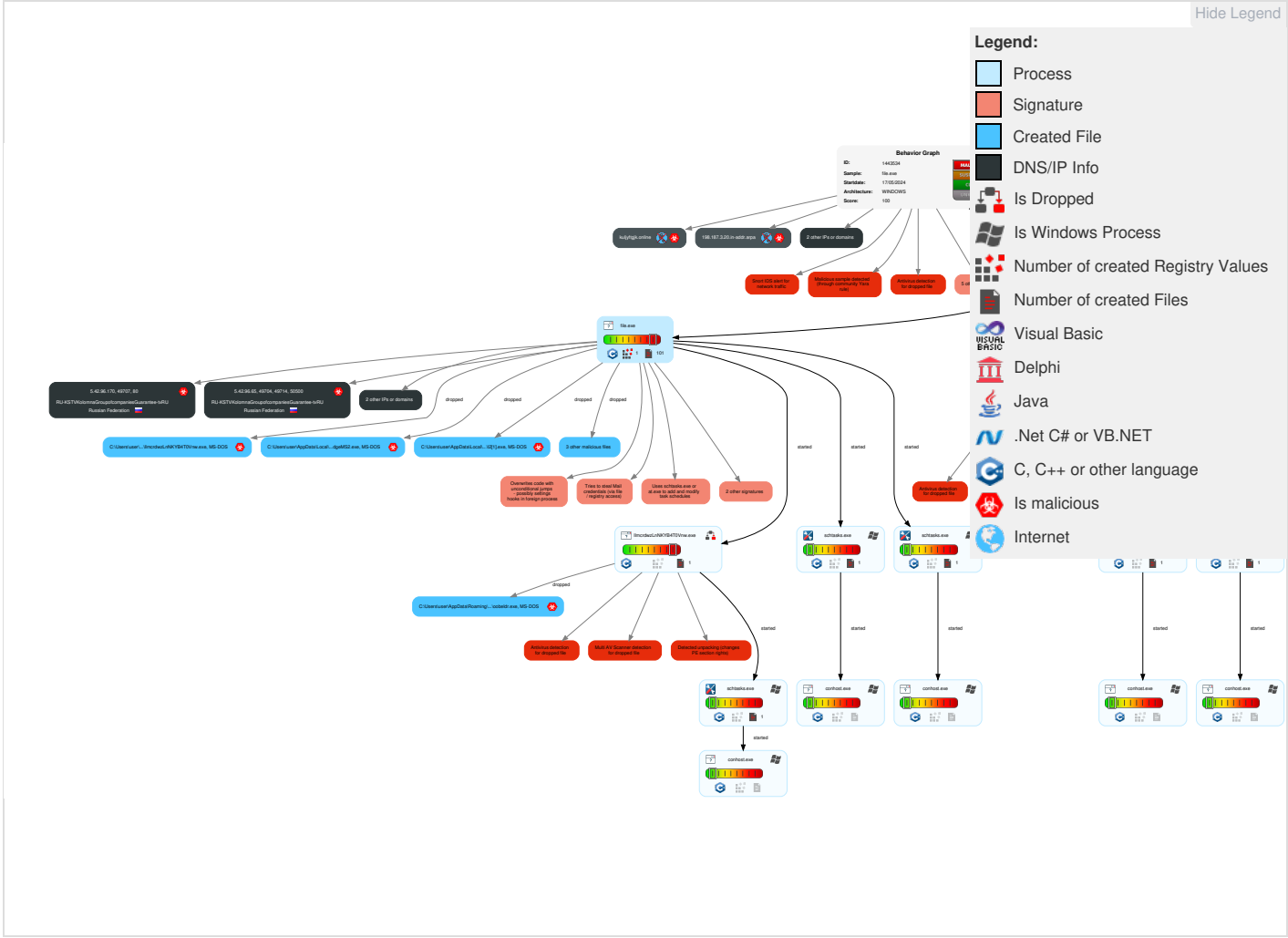
Yara detected RisePro Stealer

Mitre Att&ck Matrix

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Gather Victim Identity Information	Acquire Infrastructure	1 Valid Accounts	2 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	1 2 Ingress Tool Transfer	Exfiltration Over Other Network Medium	Abuse Accessibility Features
Credentials	Domains	Default Accounts	1 Scheduled Task/Job	1 Create Account	1 Valid Accounts	2 Obfuscated Files or Information	1 Credential API Hooking	2 File and Directory Discovery	Remote Desktop Protocol	1 Data from Local System	1 1 Encrypted Channel	Exfiltration Over Bluetooth	Network Denial of Service
Email Addresses	DNS Server	Domain Accounts	At	1 Valid Accounts	1 Access Token Manipulation	1 Software Packing	Security Account Manager	1 4 6 System Information Discovery	SMB/Windows Admin Shares	1 Screen Capture	1 Non-Standard Port	Automated Exfiltration	Data Encrypted for Impact

Reconnai…	Resource Developm…	Initial Access	Execution	Persisten…	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Employee Names	Virtual Private Server	Local Accounts	Cron	1 Scheduled Task/Job	1 1 Process Injection	1 DLL Side-Loading	NTDS	1 Query Registry	Distributed Component Object Model	1 Email Collection	2 Non-Application Layer Protocol	Traffic Duplication	Data Destruction
Gather Victim Network Information	Server	Cloud Accounts	Launchd	2 1 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	1 Masqueradi ng	LSA Secrets	2 2 1 Security Software Discovery	SSH	1 Credential API Hooking	2 3 Application Layer Protocol	Scheduled Transfer	Data Encrypted for Impact
Domain Properties	Botnet	Replication Through Removable Media	Scheduled Task	RC Scripts	2 1 Registry Run Keys / Startup Folder	1 Valid Accounts	Cached Domain Credentials	1 1 Virtualizatio n/Sandbox Evasion	VNC	GUI Input Capture	Multiband Communicat ion	Data Transfer Size Limits	Service Stop
DNS	Web Services	External Remote Services	Systemd Timers	Startup Items	Startup Items	1 Access Token Manipulatio n	DCSync	2 Process Discovery	Windows Remote Managemen t	Web Portal Capture	Commonly Used Port	Exfiltration Over C2 Channel	Inhibit System Recovery
Network Trust Dependenci es	Serverless	Drive-by Compromis e	Container Orchestratio n Job	Scheduled Task/Job	Scheduled Task/Job	1 1 Virtualizatio n/Sandbox Evasion	Proc Filesystem	1 Application Window Discovery	Cloud Services	Credential API Hooking	Application Layer Protocol	Exfiltration Over Alternative Protocol	Defacement
Network Topology	Malvertising	Exploit Public-Facing Application	Command and Scripting Interpreter	At	At	1 1 Process Injection	/etc/passwd and /etc/shadow	1 System Network Configuratio n Discovery	Direct Cloud VM Connections	Data Staged	Web Protocols	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Internal Defacement

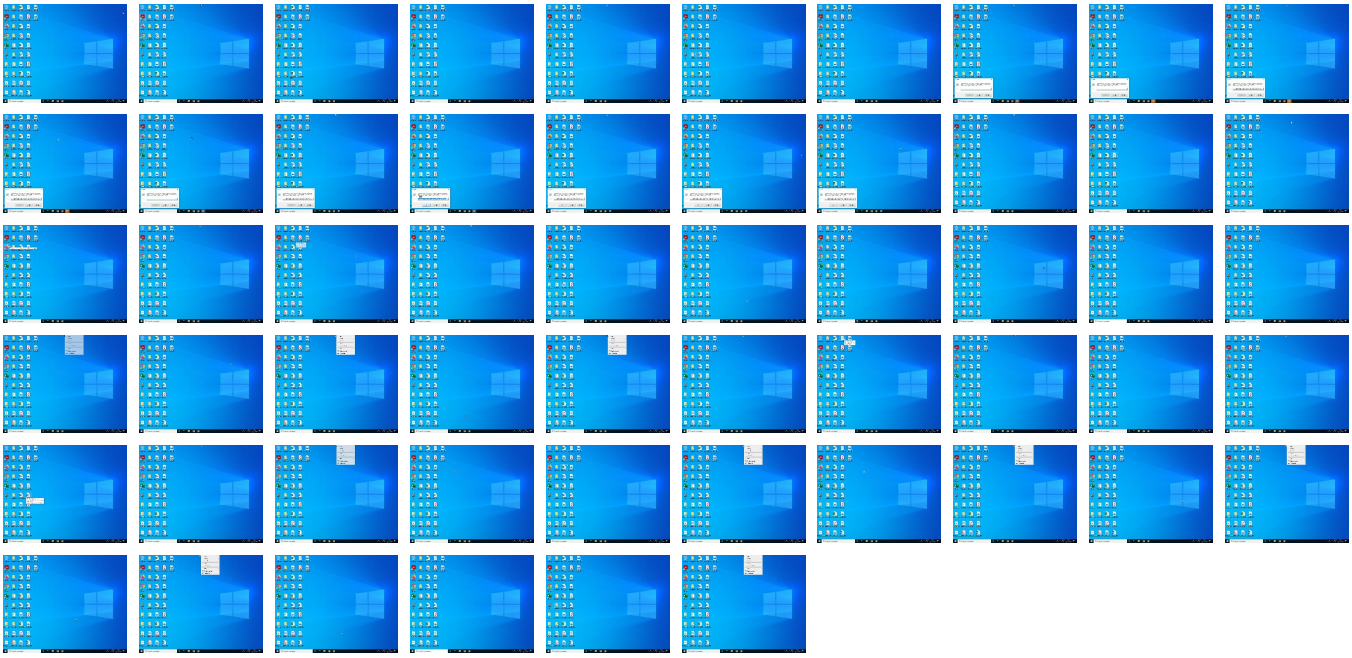
Behavior Graph

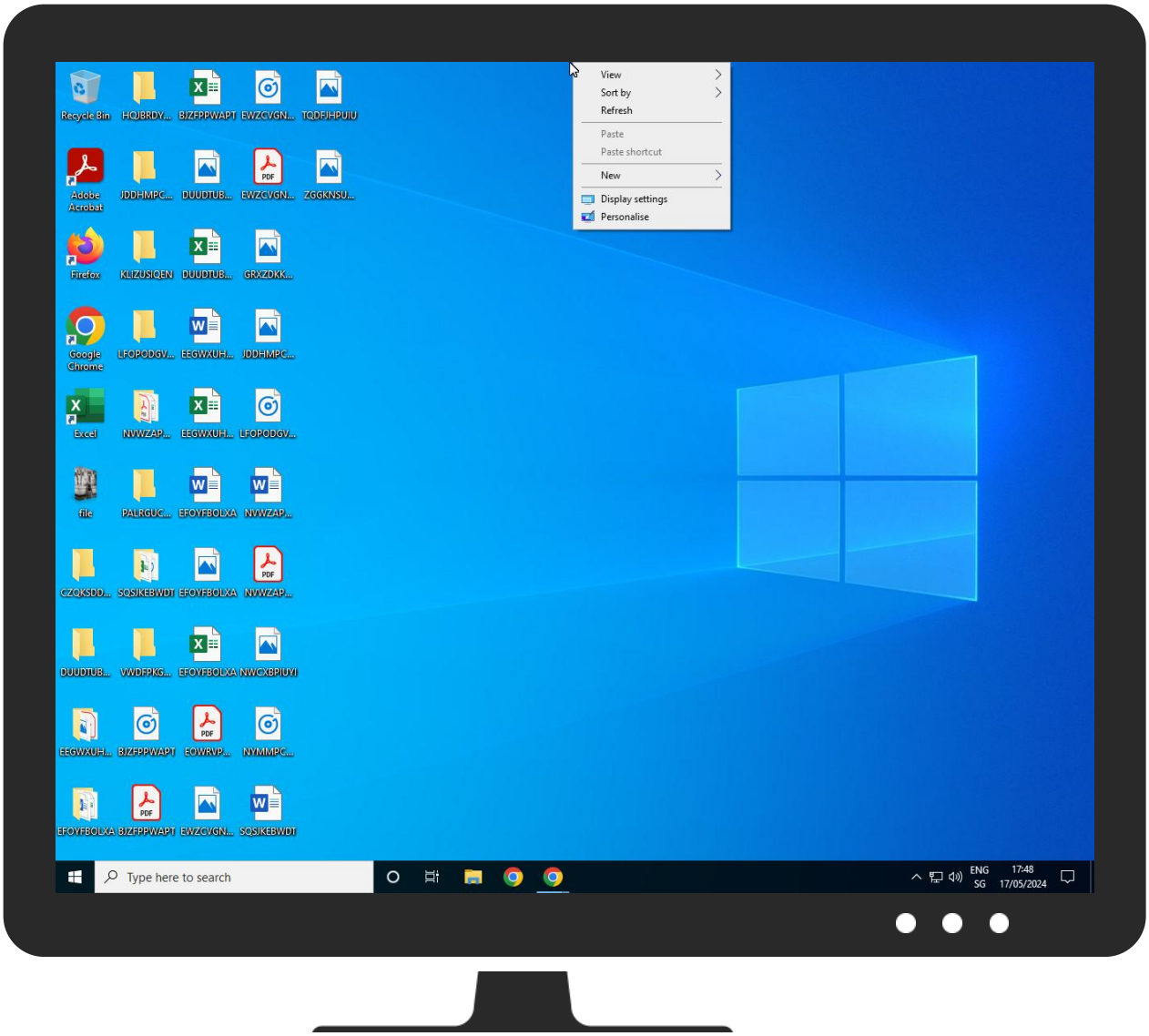


Screenshots

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
file.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\AdobeUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26\AdobeUpdaterV2.exe	100%	Avira	HEUR/AGEN.1304053	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\T9RRWRNL\l2[1].exe	100%	Avira	HEUR/AGEN.1304053	
C:\ProgramData\MSIUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26\MSIUpdaterV2.exe	100%	Avira	HEUR/AGEN.1304053	
C:\Users\user\AppData\Roaming\Microsoft\Protect\oobeldr.exe	100%	Avira	HEUR/AGEN.1304053	
C:\Users\user\AppData\Local\Temp\EdgeMS2_45c48cce2e2d7fbdea1afc51c7c6ad26\EdgeMS2.exe	100%	Avira	HEUR/AGEN.1304053	
C:\Users\user\AppData\Local\Temp\span1UB98D2D2zeo\llmcrdwzLnNKYB4T0Vnw.exe	100%	Avira	HEUR/AGEN.1304053	
C:\ProgramData\MSIUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26\MSIUpdaterV2.exe	83%	ReversingLabs	Win32.Trojan.RedLine	
C:\Users\user\AppData\Local\AdobeUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26\AdobeUpdaterV2.exe	83%	ReversingLabs	Win32.Trojan.RedLine	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\T9RRWRNL\l2[1].exe	83%	ReversingLabs	Win32.Trojan.RedLine	
C:\Users\user\AppData\Local\Temp\EdgeMS2_45c48cce2e2d7fbdea1afc51c7c6ad26\EdgeMS2.exe	83%	ReversingLabs	Win32.Trojan.RedLine	
C:\Users\user\AppData\Local\Temp\span1UB98D2D2zeo\llmcrdwzLnNKYB4T0Vnw.exe	83%	ReversingLabs	Win32.Trojan.RedLine	
C:\Users\user\AppData\Roaming\Microsoft\Protect\oobeldr.exe	83%	ReversingLabs	Win32.Trojan.RedLine	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://https://ipinfo.io/https://www.maxmind.com/en/locate-my-ip-addressWs2_32.dll	0%	URL Reputation	safe	
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	0%	URL Reputation	safe	
http://https://www.ecosia.org/newtab/	0%	URL Reputation	safe	
http://https://ipinfo.io/Mozilla/5.0	0%	URL Reputation	safe	
http://https://support.mozilla.org/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=firefox-br	0%	URL Reputation	safe	
http://https://ac.ecosia.org/autocomplete?q=	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://https://ipinfo.io/	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	0%	URL Reputation	safe	
http://https://ipinfo.io/t	0%	URL Reputation	safe	
http://https://support.mozilla.org/products/firefoxgro.allizom.troppus.GVegJq3nFfBL	0%	URL Reputation	safe	
http://www.winimage.com/zLibDll	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://support.mozilla.org	0%	URL Reputation	safe	
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	0%	URL Reputation	safe	
http://https://duckduckgo.com/ac/?q=	0%	Avira URL Cloud	safe	
http://https://kuljyftgjk.online:80/server/k/l2.exemespace	0%	Avira URL Cloud	safe	
http://https://kuljyftgjk.online:80/server/k/l2.exe	0%	Avira URL Cloud	safe	
http://https://db-ip.com:443/demo/home.php?s=12.205.151.60	0%	Avira URL Cloud	safe	
http://https://ipinfo.io/widget/demo/12.205.151.60	0%	Avira URL Cloud	safe	
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	0%	Avira URL Cloud	safe	
http://https://kuljyftgjk.online:80/	0%	Avira URL Cloud	safe	
http://https://duckduckgo.com/chrome_newtab	0%	Avira URL Cloud	safe	
http://https://db-ip.com/z-	0%	Avira URL Cloud	safe	
http://5.42.96.170/server/k/l2.exe	0%	Avira URL Cloud	safe	
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	0%	Avira URL Cloud	safe	
http://https://t.me/RiseProSUPPORT	0%	Avira URL Cloud	safe	
http://https://t.me/risepro_bot	0%	Avira URL Cloud	safe	
http://5.42.96.170/server/k/l2.exe5	0%	Avira URL Cloud	safe	
http://https://kuljyftgjk.online/server/k/l2.exe5P#.	0%	Avira URL Cloud	safe	
http://https://kuljyftgjk.online/server/k/l2.exedwzLnNKYB4T0Vnw.exe	0%	Avira URL Cloud	safe	
http://https://db-ip.com/demo/home.php?s=12.205.151.60	0%	Avira URL Cloud	safe	
http://https://kuljyftgjk.online:80/I	0%	Avira URL Cloud	safe	
http://5.42.96.170/server/k/l2.exeDTl	0%	Avira URL Cloud	safe	
http://https://kuljyftgjk.online:80/server/k/l2.exe5G	0%	Avira URL Cloud	safe	
http://https://kuljyftgjk.online/server/k/l2.exeo	0%	Avira URL Cloud	safe	
http://https://kuljyftgjk.online/server/k/l2.exexefN	0%	Avira URL Cloud	safe	
http://https://kuljyftgjk.online:80/Mi&/	0%	Avira URL Cloud	safe	
http://https://ipinfo.io:443/widget/demo/12.205.151.60	0%	Avira URL Cloud	safe	
http://https://t.me/risepro_botisepro_bot	0%	Avira URL Cloud	safe	
http://https://kuljyftgjk.online/server/k/l2.exe	0%	Avira URL Cloud	safe	
http://https://kuljyftgjk.online/	0%	Avira URL Cloud	safe	
http://https://kuljyftgjk.online:80/server/k/l2.exeJG	0%	Avira URL Cloud	safe	
http://https://kuljyftgjk.online/Bb	0%	Avira URL Cloud	safe	
http://https://t.me/risepro_bot%(	0%	Avira URL Cloud	safe	
http://https://kuljyftgjk.online/ons	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ipinfo.io	34.117.186.192	true	false		unknown
db-ip.com	172.67.75.166	true	false		unknown
kuljyftgjk.online	unknown	unknown	true		unknown
198.187.3.20.in-addr.arpa	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://5.42.96.170/server/k/l2.exe	true	• Avira URL Cloud: safe	unknown
http://https://ipinfo.io/widget/demo/12.205.151.60	false	• Avira URL Cloud: safe	unknown
http://https://db-ip.com/demo/home.php?s=12.205.151.60	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://kuljyftgjk.online:80/server/k/l2.exe	file.exe, 00000000.00000003.2220430384.000000000647F000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2220783088.0000000006480000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.3698823077.00000000016D3000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000002.4444160556.00000000016D3000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2219971624.000000000647F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/chrome_newtab	file.exe, 00000000.00000003.2121507295.000000006548000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2115771934.0000000006495000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2113965338.0000000006495000.00000004.00000020.00020000.00000000.sdmp, OaQuGlYHO2B0Web Data.0.dr, UdeNZdOQSPDWWeb Data.0.dr, sl01HQPBKH54Web Data.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://kuljyftgjk.online:80/server/k/l2.exemespace	file.exe, 00000000.00000003.2220430384.000000000647F000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2220783088.0000000006480000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2219971624.000000000647F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/ac/?q=	file.exe, 00000000.00000003.2121507295.000000006548000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2115771934.0000000006495000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2113965338.0000000006495000.00000004.00000020.00020000.00000000.sdmp, OaQuGlYHO2B0Web Data.0.dr, UdeNZdOQSPDWWeb Data.0.dr, sl01HQPBKH54Web Data.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://sectigo.com/CPS0	file.exe, 00000000.00000003.2199558318.000000006694F000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2195723746.0000000006946000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2196881348.0000000006945000.00000004.00000020.00020000.00000000.sdmp, MSIUpdaterV2.exe, 00000007.00000003.2217734150.000000000286A000.00000004.00000020.00020000.00000000.sdmp, llmcrdwzLnNKYB4T0Vnw.exe, 00000009.00000003.2209721688.0000000002C1B000.00000004.00000020.00020000.00000000.sdmp, AdobeUpdaterV2.exe.0.dr, l2[1].exe.0.dr, MSIUpdaterV2.exe.0.dr, oobeldr.exe.9.dr, EdgeMS2.exe.0.dr, llmcrdwzLnNKYB4T0Vnw.exe.0.dr	false	• URL Reputation: safe	unknown
http://https://db-ip.com/z-	file.exe, 00000000.00000003.3698823077.00000000016D3000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000002.4444160556.00000000016D3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	file.exe, 00000000.00000003.2121507295.000000006548000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2115771934.0000000006495000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2113965338.0000000006495000.00000004.00000020.00020000.00000000.sdmp, OaQuGlYHO2B0Web Data.0.dr, UdeNZdOQSPDWWeb Data.0.dr, sl01HQPBKH54Web Data.0.dr	false	• Avira URL Cloud: safe	unknown
http://ocsp.sectigo.com0	file.exe, 00000000.00000003.2199558318.000000006694F000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2195723746.0000000006946000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2196881348.0000000006945000.00000004.00000020.00020000.00000000.sdmp, MSIUpdaterV2.exe, 00000007.00000003.2217734150.000000000286A000.00000004.00000020.00020000.00000000.sdmp, llmcrdwzLnNKYB4T0Vnw.exe, 00000009.00000003.2209721688.0000000002C1B000.00000004.00000020.00020000.00000000.sdmp, AdobeUpdaterV2.exe.0.dr, l2[1].exe.0.dr, MSIUpdaterV2.exe.0.dr, oobeldr.exe.9.dr, EdgeMS2.exe.0.dr, llmcrdwzLnNKYB4T0Vnw.exe.0.dr	false	• URL Reputation: safe	unknown

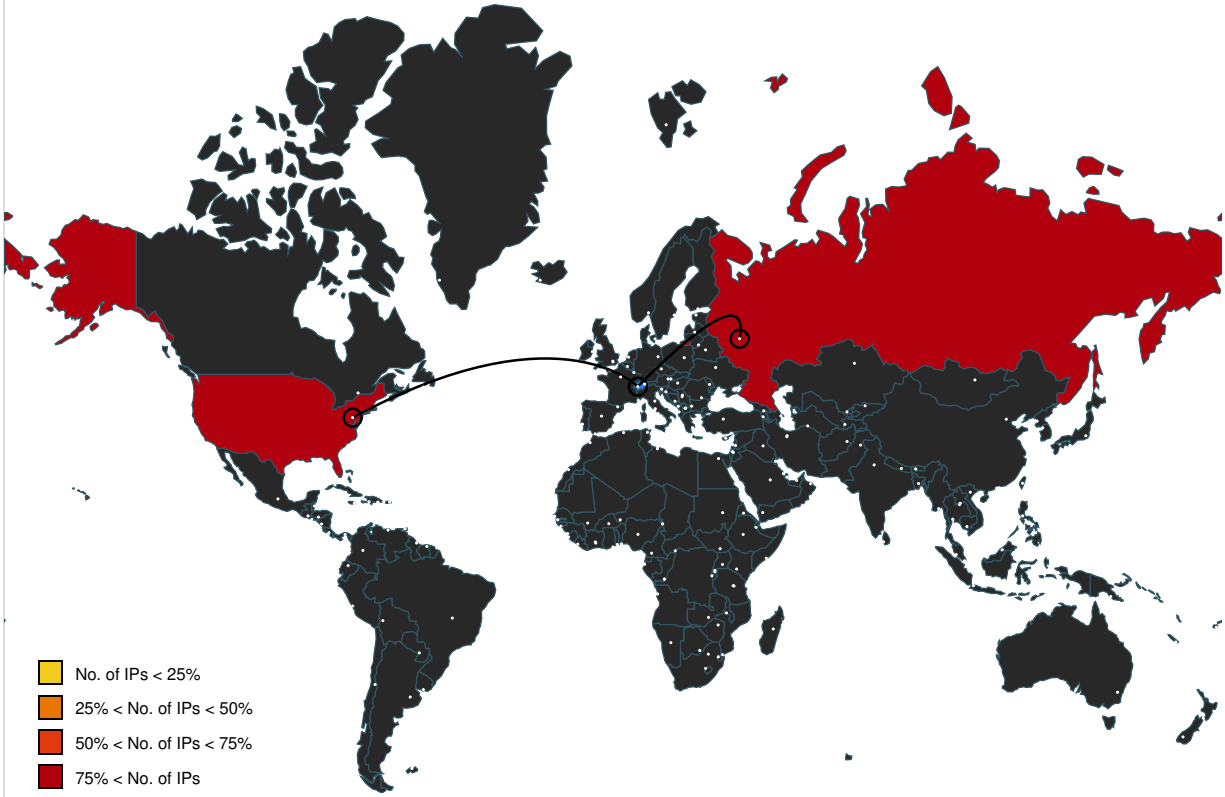
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://db-ip.com:443/demo/home.php?s=12.205.151.60	file.exe, 00000000.00000003.3698823077.00000000016D3000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000002.4444160556.00000000016D3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ipinfo.io/https://www.maxmind.com/en/locate-my-ip-addressWs2_32.dll	file.exe, 00000000.00000002.4442200408.00000000030D000.00000002.00000001.01000000.00000003.sdmp	false	• URL Reputation: safe	unknown
http://https://kuljyftgjk.online:80/	file.exe, 00000000.00000003.2219971624.00000000647F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	file.exe, 00000000.00000003.2121507295.000000006548000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2115771934.0000000006495000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2113965338.0000000006495000.00000004.00000020.00020000.00000000.sdmp, OaQuGlYHO2B0Web Data.0.dr, UdeNZdOQSPDWWeb Data.0.dr, sl01HQPBKH54Web Data.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://kuljyftgjk.online/server/k/l2.exe5P#.	file.exe, 00000000.00000003.2220430384.00000000647F000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2220783088.0000000006480000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2219971624.000000000647F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://t.me/RiseProSUPPORT	file.exe, 00000000.00000002.4445088347.000000006449000.00000004.00000020.00020000.00000000.sdmp, dZGGvSkztfgYu5jqSY21Wne.zip.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://ch.search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas&command=	file.exe, 00000000.00000003.2121507295.000000006548000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2115771934.0000000006495000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2113965338.0000000006495000.00000004.00000020.00020000.00000000.sdmp, OaQuGlYHO2B0Web Data.0.dr, UdeNZdOQSPDWWeb Data.0.dr, sl01HQPBKH54Web Data.0.dr	false	• URL Reputation: safe	unknown
http://https://www.ecosia.org/newtab/	file.exe, 00000000.00000003.2121507295.000000006548000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2115771934.0000000006495000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2113965338.0000000006495000.00000004.00000020.00020000.00000000.sdmp, OaQuGlYHO2B0Web Data.0.dr, UdeNZdOQSPDWWeb Data.0.dr, sl01HQPBKH54Web Data.0.dr	false	• URL Reputation: safe	unknown
http://https://ipinfo.io/Mozilla/5.0	file.exe, 00000000.00000002.4444160556.00000000016C7000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.3698823077.00000000016C7000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://support.mozilla.org/kb/customize-firefox-controls-buttons-and-toolbars?utm_source=firefox-br	D87fZN3R3jFeplaces.sqlite.0.dr	false	• URL Reputation: safe	unknown
http://https://kuljyftgjk.online/server/k/l2.exedwzLnNKYB4T0Vnw.exe	file.exe, 00000000.00000003.2220430384.00000000647F000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2220783088.0000000006480000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000002.4445088347.0000000006480000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2219971624.000000000647F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ac.ecosia.org/autocomplete?q=	file.exe, 00000000.00000003.2121507295.000000006548000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2115771934.0000000006495000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2113965338.0000000006495000.00000004.00000020.00020000.00000000.sdmp, OaQuGlYHO2B0Web Data.0.dr, UdeNZdOQSPDWWeb Data.0.dr, sl01HQPBKH54Web Data.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	file.exe, 00000000.00000003.2199558318.000000000694F000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2195723746.0000000006946000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2196881348.0000000006945000.00000004.00000020.00020000.00000000.sdmp, MSIUpdaterV2.exe, 00000007.00000003.2217734150.000000000286A000.00000004.00000020.00020000.00000000.sdmp, llmcrdwzLnNKYB4T0Vnw.exe, 00000009.00000003.2209721688.0000000002C1B000.00000004.00000020.00020000.00000000.sdmp, AdobeUpdaterV2.exe.0.dr, l2[1].exe.0.dr, MSIUpdaterV2.exe.0.dr, oobeldr.exe.9.dr, EdgeMS2.exe.0.dr, llmcrdwzLnNKYB4T0Vnw.exe.0.dr	false	• URL Reputation: safe	unknown
http://https://t.me/risepro_bot	file.exe, 00000000.00000002.4444160556.0000000016D3000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2142639137.0000000006550000.00000004.00000020.00020000.00000000.sdmp, passwords.txt.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://ipinfo.io/	file.exe, 00000000.00000002.4444160556.0000000016C7000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.3698823077.00000000016D3000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.3698823077.00000000016C7000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000002.4444160556.00000000016D3000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000002.4443887762.0000000001682000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.3698823077.00000000016B9000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000002.4444160556.00000000016B9000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://kuljyftgjk.online:80/l	file.exe, 00000000.00000003.2220430384.000000000647F000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2220783088.0000000006480000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000002.4445088347.0000000006480000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2219971624.000000000647F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://5.42.96.170/server/k/l2.exeDTl	file.exe, 00000000.00000002.4445474316.0000000006530000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	file.exe, 00000000.00000003.2199558318.000000000694F000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2195723746.0000000006946000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2196881348.0000000006945000.00000004.00000020.00020000.00000000.sdmp, MSIUpdaterV2.exe, 00000007.00000003.2217734150.000000000286A000.00000004.00000020.00020000.00000000.sdmp, llmcrdwzLnNKYB4T0Vnw.exe, 00000009.00000003.2209721688.0000000002C1B000.00000004.00000020.00020000.00000000.sdmp, AdobeUpdaterV2.exe.0.dr, l2[1].exe.0.dr, MSIUpdaterV2.exe.0.dr, oobeldr.exe.9.dr, EdgeMS2.exe.0.dr, llmcrdwzLnNKYB4T0Vnw.exe.0.dr	false	• URL Reputation: safe	unknown
http://https://ch.search.yahoo.com/favicon.icohttps://ch.search.yahoo.com/search	file.exe, 00000000.00000003.2121507295.0000000006548000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2115771934.0000000006495000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2113965338.0000000006495000.00000004.00000020.00020000.00000000.sdmp, OaQuGlYHO2B0Web Data.0.dr, UdeNZdOQSPDWWeb Data.0.dr, sl01HQPBKH54Web Data.0.dr	false	• URL Reputation: safe	unknown
http://5.42.96.170/server/k/l2.exe5	file.exe, 00000000.00000003.3698823077.0000000016D3000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000002.4444160556.00000000016D3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ipinfo.io/t	file.exe, 00000000.00000002.4443887762.0000000001682000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://kuljyftgjk.online:80/server/k/l2.exe5G	file.exe, 00000000.00000003.2220430384.000000000647F000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2220783088.0000000006480000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000002.4445088347.0000000006480000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2219971624.000000000647F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://kuljyftgjk.online/server/k/l2.exexefN	file.exe, 00000000.00000003.2220430384.000000000647F000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2219971624.000000000647F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://support.mozilla.org/products/firefoxgro.allizom.troppus.GVegJq3nFfBL	D87fZN3R3jFeplaces.sqlite.0.dr	false	• URL Reputation: safe	unknown
http://https://t.me/risepro_botisepro_bot	file.exe, 00000000.00000003.3698823077.0000000016D3000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000002.4444160556.00000000016D3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://kuljyftgjk.online/server/k/l2.exeo	file.exe, 00000000.00000003.2220430384.000000000647F000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2220783088.0000000006480000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000002.4445088347.0000000006480000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2219971624.000000000647F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.winimage.com/zLibDll	file.exe, 00000000.00000002.4442200408.00000000030D000.00000002.00000001.01000000.00000003.sdmp	false	• URL Reputation: safe	unknown
http://https://ipinfo.io:443/widget/demo/12.205.151.60	file.exe, 00000000.00000002.4444160556.0000000016C7000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.3698823077.00000000016C7000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://support.mozilla.org	D87fZN3R3jFeplaces.sqlite.0.dr	false	• URL Reputation: safe	unknown
http://https://kuljyftgjk.online/server/k/l2.exe	file.exe, 00000000.00000003.2219971624.000000000647F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://kuljyftgjk.online:80/Mi&/	file.exe, 00000000.00000003.2220430384.000000000647F000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2220783088.0000000006480000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000002.4445088347.0000000006480000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2219971624.000000000647F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	file.exe, 00000000.00000003.2121507295.0000000006548000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2115771934.0000000006495000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2113965338.0000000006495000.00000004.00000020.00020000.00000000.sdmp, OaQuGlYHO2B0Web Data.0.dr, UdeNZdOQSPDWWeb Data.0.dr, sl01HQPBKH54Web Data.0.dr	false	• URL Reputation: safe	unknown
http://https://kuljyftgjk.online:80/server/k/l2.exeJG	file.exe, 00000000.00000003.2220430384.000000000647F000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2220783088.0000000006480000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000002.4445088347.0000000006480000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.2219971624.000000000647F000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://kuljyftgjk.online/	file.exe, 00000000.00000002.4444160556.0000000016C7000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.3698823077.00000000016C7000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000002.4445474316.0000000006530000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://kuljyftgjk.online/Bb	file.exe, 00000000.00000002.4445474316.0000000006530000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://t.me/risepro_bot%(	file.exe, 00000000.00000003.3698823077.0000000016D3000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000002.4444160556.00000000016D3000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://kuljyftgjk.online/ons	file.exe, 00000000.00000002.4444160556.0000000016C7000.00000004.00000020.00020000.00000000.sdmp, file.exe, 00000000.00000003.3698823077.00000000016C7000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.117.186.192	ipinfo.io	United States		139070	GOOGLE-AS-APGoogleAsiaPacificPteLtdSG	false
5.42.96.65	unknown	Russian Federation		39493	RU-KSTVKolomnaGroupofcompaniesGuarantee-tvRU	true
172.67.75.166	db-ip.com	United States		13335	CLOUDFLARENETUS	false
5.42.96.170	unknown	Russian Federation		39493	RU-KSTVKolomnaGroupofcompaniesGuarantee-tvRU	true

General Information

Joe Sandbox version:	40.0.0 Tourmaline
Analysis ID:	1443534
Start date and time:	2024-05-17 23:44:10 +02:00
Joe Sandbox product:	CloudBasic
Overall analysis duration:	0h 10m 0s
Hypervisor based Inspection enabled:	false
Report type:	light

Cookbook file name:	default.jbs
Analysis system description:	Windows 10 x64 22H2 with Office Professional Plus 2019, Chrome 117, Firefox 118, Adobe Reader DC 23, Java 8 Update 381, 7zip 23.01
Number of analysed new started processes analysed:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample name:	file.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@24/32@5/4
EGA Information:	• Successful, ratio: 100%
HCA Information:	• Successful, ratio: 73% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Override analysis time to 240000 for current running targets taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe, SIHClient.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ocsp.digicert.com, slscr.update.microsoft.com, ctldl.windowsupdate.com, fe3cr.delivery.mp.microsoft.com
- HTTP raw data packets have been limited to 10 per session. Please view the PCAPs for the complete data.
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- VT rate limit hit for: file.exe

Simulations

Behavior and APIs

Time	Type	Description
17:45:16	API Interceptor	5044664x Sleep call for process: file.exe modified
17:45:53	API Interceptor	1757121x Sleep call for process: oobeldr.exe modified
23:45:15	Task Scheduler	Run new task: MSIUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26 HR path: C:\ProgramData\MSIUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26\MSIUpdaterV2.exe
23:45:16	Task Scheduler	Run new task: MSIUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26 LG path: C:\ProgramData\MSIUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26\MSIUpdaterV2.exe
23:45:16	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run AdobeUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26 C:\Users\user\AppData\Local\AdobeUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26\AdobeUpdaterV2.exe
23:45:18	Task Scheduler	Run new task: Telemetry Logging path: C:\Users\user\AppData\Roaming\Microsoft\Protect\oobeldr.exe
23:45:24	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run AdobeUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26 C:\Users\user\AppData\Local\AdobeUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26\AdobeUpdaterV2.exe
23:45:33	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\EdgeMS2.lnk

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\MSIUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26\MSIUpdaterV2.exe

Process:	C:\Users\user\Desktop\file.exe
File Type:	MS-DOS executable PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows, MZ for MS-DOS
Category:	dropped
Size (bytes):	4563640
Entropy (8bit):	7.906115886926003
Encrypted:	false
SSDEEP:	98304:RpvmMxvdjYr/2BLOizdh/0Rzs24+WhXWXfRqCFh6MacgD5hB:vlVjMuBx0R7RrXpqiUhB
MD5:	AF6E384DFABDAD52D43CF8429AD8779C
SHA1:	C78E8CD8C74AD9D598F591DE5E49F73CE3373791
SHA-256:	F327C2B5AB1D98F0382A35CD78F694D487C74A7290F1FF7BE53F42E23021E599
SHA-512:	B55BA87B275A475E751E13EC9BAC2E7F1A3484057844E210168E2256D73D9B6A7C7C7592845D4A3BF8163CF0D479315418A9F3CB8F2F4832AF88A06867E3DF93
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 83%
Preview:	MZ@.....!..L.!Win32 .EXE...$@...PE..L....M.a.....^.....w.....0....@.....}.....m.F.....w.....w.|.....E..... .....P.w.....MPRESS1.pw.....?.....MPRESS22.....w.....?.....rsrc...|.....w.....?.....@..... .....v2.19w...?. ...o.....G>H.r9aQ..(.....`....=....?....!.Z..&I.....I18..Z!..Y..s...[QX....a....YY...).v.....n.....|)....^f..+.>..84h82g...>*.hb\...E.(.x.....@.8 _.9.4U.m..'.s.....#.....03.....O..]`..S2.@#.....oF~.*.R..Q..q.o.yn...OA@|....g...F....0.j.....s/..H..+ 0C.!....7s..^H,..... ..{.....D.....r.I..,|.....u.6.....E>q..}....g..).U..ME.'.j}.. .....7^...w.....Le.....k.T.`.#%....b..n.F.&-o..../8S.E..{1.E..,....<.c|b.z.Fz.....|..W"p.

C:\Users\user\AppData\Local\AdobeUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26\AdobeUpdaterV2.exe

Process:	C:\Users\user\Desktop\file.exe
File Type:	MS-DOS executable PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows, MZ for MS-DOS
Category:	dropped
Size (bytes):	4563640
Entropy (8bit):	7.906115886926003
Encrypted:	false
SSDEEP:	98304:RpvmMxvdjYr/2BLOizdh/0Rzs24+WhXWXfRqCFh6MacgD5hB:vlVjMuBx0R7RrXpqiUhB
MD5:	AF6E384DFABDAD52D43CF8429AD8779C
SHA1:	C78E8CD8C74AD9D598F591DE5E49F73CE3373791
SHA-256:	F327C2B5AB1D98F0382A35CD78F694D487C74A7290F1FF7BE53F42E23021E599
SHA-512:	B55BA87B275A475E751E13EC9BAC2E7F1A3484057844E210168E2256D73D9B6A7C7C7592845D4A3BF8163CF0D479315418A9F3CB8F2F4832AF88A06867E3DF93
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 83%
Preview:	MZ@.....!..L.!Win32 .EXE...$@...PE..L....M.a.....^.....w.....0....@.....}.....m.F.....w.....w.|.....E..... .....P.w.....MPRESS1.pw.....?.....MPRESS22.....w.....?.....rsrc...|.....w.....?.....@..... .....v2.19w...?. ...o.....G>H.r9aQ..(.....`....=....?....!.Z..&I.....I18..Z!..Y..s...[QX....a....YY...).v.....n.....|)....^f..+.>..84h82g...>*.hb\...E.(.x.....@.8 _.9.4U.m..'.s.....#.....03.....O..]`..S2.@#.....oF~.*.R..Q..q.o.yn...OA@|....g...F....0.j.....s/..H..+ 0C.!....7s..^H,..... ..{.....D.....r.I..,|.....u.6.....E>q..}....g..).U..ME.'.j}.. .....7^...w.....Le.....k.T.`.#%....b..n.F.&-o..../8S.E..{1.E..,....<.c|b.z.Fz.....|..W"p.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\T9RRWRNL\l2[1].exe

Process:	C:\Users\user\Desktop\file.exe
File Type:	MS-DOS executable PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows, MZ for MS-DOS
Category:	dropped
Size (bytes):	4563640
Entropy (8bit):	7.906115886926003
Encrypted:	false
SSDEEP:	98304:RpvmMxvdjYr/2BLOizdh/0Rzs24+WhXWXfRqCFh6MacgD5hB:vlVjMuBx0R7RrXpqiUhB
MD5:	AF6E384DFABDAD52D43CF8429AD8779C
SHA1:	C78E8CD8C74AD9D598F591DE5E49F73CE3373791
SHA-256:	F327C2B5AB1D98F0382A35CD78F694D487C74A7290F1FF7BE53F42E23021E599
SHA-512:	B55BA87B275A475E751E13EC9BAC2E7F1A3484057844E210168E2256D73D9B6A7C7C7592845D4A3BF8163CF0D479315418A9F3CB8F2F4832AF88A06867E3DF93
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 83%
Preview:	MZ@.....!..L.!Win32 .EXE...$@...PE..L....M.a.....^.....w.....0....@.....}.....m.F.....w.....w.|.....E..... .....P.w.....MPRESS1.pw.....?.....MPRESS22.....w.....?.....rsrc...|.....w.....?.....@..... .....v2.19w...?. ...o.....G>H.r9aQ..(.....`....=....?....!.Z..&I.....I18..Z!..Y..s...[QX....a....YY...).v.....n.....|)....^f..+.>..84h82g...>*.hb\...E.(.x.....@.8 _.9.4U.m..'.s.....#.....03.....O..]`..S2.@#.....oF~.*.R..Q..q.o.yn...OA@|....g...F....0.j.....s/..H..+ 0C.!....7s..^H,..... ..{.....D.....r.I..,|.....u.6.....E>q..}....g..).U..ME.'.j}.. .....7^...w.....Le.....k.T.`.#%....b..n.F.&-o..../8S.E..{1.E..,....<.c|b.z.Fz.....|..W"p.

C:\Users\user\AppData\Local\Temp\EdgeMS2_45c48cce2e2d7fbdea1afc51c7c6ad26\EdgeMS2.exe

Process:	C:\Users\user\Desktop\file.exe
File Type:	MS-DOS executable PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows, MZ for MS-DOS
Category:	dropped
Size (bytes):	4563640
Entropy (8bit):	7.906115886926003
Encrypted:	false
SSDEEP:	98304:RpvmMxvdjYr/2BLOizdh/0Rzs24+WhXWXfRqCFh6MacgD5hB:vlVjMuBx0R7RrXpqiUhB
MD5:	AF6E384DFABDAD52D43CF8429AD8779C
SHA1:	C78E8CD8C74AD9D598F591DE5E49F73CE3373791
SHA-256:	F327C2B5AB1D98F0382A35CD78F694D487C74A7290F1FF7BE53F42E23021E599
SHA-512:	B55BA87B275A475E751E13EC9BAC2E7F1A3484057844E210168E2256D73D9B6A7C7C7592845D4A3BF8163CF0D479315418A9F3CB8F2F4832AF88A06867E3DF93
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 83%
Preview:	MZ@.....!..L.!Win32 .EXE...$@...PE..L....M.a.....^.....w.....0....@.....}.....m.F.....w.....w.|.....E..... .....P.w.....MPRESS1.pw.....?.....MPRESS22.....w.....?.....rsrc...|.....w.....?.....@..... .....v2.19w...?. ...o.....G>H.r9aQ..(.....`....=....?....!.Z..&I.....I18..Z!..Y..s...[QX....a....YY...).v.....n.....|)....^f..+.>..84h82g...>*.hb\...E.(.x.....@.8 _.9.4U.m..'.s.....#.....03.....O..]`..S2.@#.....oF~.*.R..Q..q.o.yn...OA@|....g...F....0.j.....s/..H..+ 0C.!....7s..^H,..... ..{.....D.....r.I..,|.....u.6.....E>q..}....g..).U..ME.'.j}.. .....7^...w.....Le.....k.T.`.#%....b..n.F.&-o..../8S.E..{1.E..,....<.c|b.z.Fz.....|..W"p.

C:\Users\user\AppData\Local\Temp\dZGGvSkztfgYu5jqSY21Wne.zip

Process:	C:\Users\user\Desktop\file.exe
File Type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Category:	dropped
Size (bytes):	697462
Entropy (8bit):	**7.9978720978672815**
Encrypted:	**true**
SSDEEP:	12288:SGiq3xwkqDfTtkdTpKrZgIFxEtmeY3XV1ZiXUoqm:SVsxwR7TOTKr1rEtVY3Biko5
MD5:	09613B60CB6D5DCD89B5B2D39F4345A8
SHA1:	694B5F31527A749E51B3355A25C594C3FEE26308
SHA-256:	30D7CB2080B3FDA7D9814C2967781C92F0FFC05B556DE8E2ACAA5EA627661349
SHA-512:	8A5A9083C9E33CE59A4EBB8027594EF310239BFE6B18E19ED41D189C94FDC5B81C79AB04B921197E577E64DCABBC779C309AFF3414946C0BEEA5DACE4A0CB485
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: C:\Users\user\AppData\Local\Temp\dZGGvSkztfgYu5jqSY21Wne.zip, Author: Joe Security
Preview:	PK.....X.....Cookies\..PK.....X..E.....Cookies\Chrome_Default.txt....P.@.5.....d...`|L2J1l.. .3."_..N.....q..b..=../c.;{.....4F8...0..Y.....Z}Y.g.<w3.f.W(....K .o..l...!*.....y.o;.F..5%.....|0MS.....J.,...../.o...8.H...,M.....;.....I!.z.W....j...e....fE.?.X....6...g...skL.K.85b.U.5.../[/.<.h....C..|...C5"{..i.$...'..W).f.O.i..4.....L..Z..t.Z(}.2.m.?..<....]..... .f..I3?.q..8U.6...8.N.y_#Vb...g.k?.Z1.!.3$.....\.%...PK.....X.....History\..PK.....X..H.A...p...,...History\Firefox_v6zchhhv.default-release.txt.())(.../////.....I../J. /(.,KL..O.,JM...44.4312.06.....)5O74..V.PK.....X}.....information.txt.X]O.J.}.....2H...cw.....Y.....0m.....:Uu....M..c.....p..U.1.....S.1.\f.....X.1...\..M....dLb...x ...d..h.....y..S.../.F..F.$...4K.1kGQ.QD.....ppv.h.4L."..):7....T.Ej..z..2..L...."..7.....k._d.....\|$'Y.....?.?.k<._.....

C:\Users\user\AppData\Local\Temp\span1UB98D2D2zeo\02zdBXl47cvzcookies.sqlite	
Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, user version 12, last written using SQLite version 3042000, page size 32768, writer version 2, read version 2, file counter 3, database pages 3, cookie 0x1, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	98304
Entropy (8bit):	0.08235737944063153
Encrypted:	false
SSDEEP:	12:DQAsfWk73Fmdmc/OPVJXfPNn43etRRfYR5O8atLqxeYaNcDakMG/lO:DQAsff32mNVpP965Ra8KN0MG/lO
MD5:	369B6DD66F1CAD49D0952C40FEB9AD41
SHA1:	D05B2DE29433FB113EC4C558FF33087ED7481DD4
SHA-256:	14150D582B5321D91BDE0841066312AB3E6673CA51C982922BC293B82527220D
SHA-512:	771054845B27274054B6C73776204C235C46E0C742ECF3E2D9B650772BA5D259C8867B2FA92C3A9413D3E1AD35589D8431AC683DF84A53E13CDE361789045928
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....}..}..... ....

C:\Users\user\AppData\Local\Temp\span1UB98D2D2zeo\3b6N2Xdh3CYwplaces.sqlite	
Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, user version 75, last written using SQLite version 3042000, page size 32768, writer version 2, read version 2, file counter 2, database pages 46, cookie 0x26, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	5242880
Entropy (8bit):	0.03859996294213402
Encrypted:	false
SSDEEP:	192:58rJQaXoMXp0VW9FxWHxDSjENbx56p3DisuwAyHI:58r54w0VW3xWdkEFxcp3y/y
MD5:	D2A38A463B7925FE3ABE31ECCCE66ACA
SHA1:	A1824888F9E086439B287DEA497F660F3AA4B397
SHA-256:	474361353F00E89A9ECB246EC4662682392EBAF4F2A4BE9ABB68BBEBE33FA4A0
SHA-512:	62DB46A530D952568EFBFF7796106E860D07754530B724E0392862EF76FDF99043DA9538EC0044323C814DF59802C3BB55454D591362CB9B6E39947D11E981F7
Malicious:	false
Preview:	SQLite format 3.....@ .....&.....K.....j.....-a>.~...|0{dz.z.z"y.y3x.xKw.v.u.uGt.t;sAs.q.p.q.p{o.ohn.nem.n,m9l.k.lPj.j.h.h.g.d.c.c6b.b.a.a>.. ....

C:\Users\user\AppData\Local\Temp\span1UB98D2D2zeo\5PaUKQKCn1cOHistory	
Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 1, database pages 39, cookie 0x20, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	159744
Entropy (8bit):	0.5394293526345721
Encrypted:	false
SSDEEP:	96:AquejzH+bF+UIYysX0lxQzh/tsV0NifLjLqLy0e9S8E:AqtH+bF+UI3iN0RSV0k3qLyj9
MD5:	52701A76A821CDDBC23FB25C3FCA4968
SHA1:	440D4B5A38AF50711C5E6C6BE22D80BC17BF32DE
SHA-256:	D602B4D0B3EB9B51535F6EBA33709DCB881237FA95C5072CB39CECF0E06A0AC4
SHA-512:	2653C8DB9C20207FA7006BC9C63142B7C356FB9DC97F9184D60C75D987DC0848A8159C239E83E2FC9D45C522FEAE8D273CDCD31183DED91B8B587596183FC0 0
Malicious:	false
Preview:	SQLite format 3.....@ .....'..... .....j..... ....

C:\Users\user\AppData\Local\Temp\span1UB98D2D2zeo\D87fZN3R3jFeplaces.sqlite	
Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, user version 75, last written using SQLite version 3042000, page size 32768, writer version 2, read version 2, file counter 2, database pages 46, cookie 0x26, schema 4, UTF-8, version-valid-for 2
Category:	dropped

Size (bytes):	5242880
Entropy (8bit):	0.0385999629421340 2
Encrypted:	false
SSDEEP:	192:58rJQaXoMXp0VW9FxWHxDSjENbx56p3DisuwAyHI:58r54w0VW3xWdkEFxcp3y/y
MD5:	D2A38A463B7925FE3ABE31ECCCE66ACA
SHA1:	A1824888F9E086439B287DEA497F660F3AA4B397
SHA-256:	474361353F00E89A9ECB246EC4662682392EBAF4F2A4BE9ABB68BBEBE33FA4A0
SHA-512:	62DB46A530D952568EFBFF7796106E860D07754530B724E0392862EF76FDF99043DA9538EC0044323C814DF59802C3BB55454D591362CB9B6E39947D11E981F7
Malicious:	false
Preview:	SQLite format 3.....@ .....&.....K.....j.....-a>.~...|0{dz.z.z"y.y3x.xKw.v.u.uGt.t;sAs.q.p.q.p{o.ohn.nem.n,m9l.k.lPj.j.h.h.g.d.c.c6b.b.a.a>.. ....

C:\Users\user\AppData\Local\Temp\span1UB98D2D2zeo\GNGpmTFam5reWeb Data

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.121297215059106
Encrypted:	false
SSDEEP:	384:72qOB1nxCkvSAELyKOMq+8yC8F/YfU5m+OlT:qq+n0E9ELyKOMq+8y9/Ow
MD5:	D87270D0039ED3A5A72E7082EA71E305
SHA1:	0FBACFA8029B11A5379703ABE7B392C4E46F0BD2
SHA-256:	F142782D1E80D89777EFA82C9969E821768DE3E9713FC7C1A4B26D769818AAAA
SHA-512:	18BB9B498C225385698F623DE06F93F9CFF933FE98A6D70271BC6FA4F866A0763054A4683B54684476894D9991F64CAC6C63A021BDFEB8D493310EF2C779638D
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....6.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\span1UB98D2D2zeo\HYMDMNDHbpvCLogin Data

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 25, cookie 0xe, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	51200
Entropy (8bit):	0.8746135976761988
Encrypted:	false
SSDEEP:	96:O8mmwLCn8MouB6wzFlOqUvJKLReZff44EK:O8yLG7IwRWf4
MD5:	9E68EA772705B5EC0C83C2A97BB26324
SHA1:	243128040256A9112CEAC269D56AD6B21061FF80
SHA-256:	17006E475332B22DB7B337F1CBBA285B3D9D0222FD06809AA8658A8F0E9D96EF
SHA-512:	312484208DC1C35F87629520FD6749B9DDB7D224E802D0420211A7535D911EC1FA0115DC32D8D1C2151CF05D5E15BBECC4BCE58955CFFDE2D6D5216E5F8F3E F
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Temp\span1UB98D2D2zeo\KNCS9xAjcy97Login Data

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 20, cookie 0xb, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.8553638852307782
Encrypted:	false
SSDEEP:	48:2x7BA+IIF7CVEq8Ma0D0HOlf/6ykwp1EUwMHZq10bvJKLkw8s8LKvUf9KVyJ7h/f:QNDCn8MouB6wz8iZqmvJKLPeymwil
MD5:	28222628A3465C5F0D4B28F70F97F482
SHA1:	1BAA3DEB7DFD7C9B4CA9FDB540F236C24917DD14
SHA-256:	93A6AF6939B17143531FA4474DFC564FA55359308B910E6F0DCA774D322C9BE4

SHA-512:	C8FB93F658C1A654186FA6AA2039E40791E6B0A1260B223272BB01279A7B574E238B28217DADF3E1850C7083ADFA2FE5DA0CCE6F9BCABD59E1FFD1061B3A88F7
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Temp\span1UB98D2D2zeo\Ln2ferf9cd9cHistory

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 1, database pages 39, cookie 0x20, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	159744
Entropy (8bit):	0.5394293526345721
Encrypted:	false
SSDEEP:	96:AquejzH+bF+UIYysX0IxQzh/tsV0NifLjLqLy0e9S8E:AqtH+bF+UI3iN0RSV0k3qLyj9
MD5:	52701A76A821CDDBC23FB25C3FCA4968
SHA1:	440D4B5A38AF50711C5E6C6BE22D80BC17BF32DE
SHA-256:	D602B4D0B3EB9B51535F6EBA33709DCB881237FA95C5072CB39CECF0E06A0AC4
SHA-512:	2653C8DB9C20207FA7006BC9C63142B7C356FB9DC97F9184D60C75D987DC0848A8159C239E83E2FC9D45C522FEAE8D273CDCD31183DED91B8B587596183FC00
Malicious:	false
Preview:	SQLite format 3.....@ .....'..... .....j..... ....

C:\Users\user\AppData\Local\Temp\span1UB98D2D2zeo\M2i6MTywpfRAHistory

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 1, database pages 38, cookie 0x1f, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	155648
Entropy (8bit):	0.5407252242845243
Encrypted:	false
SSDEEP:	96:OgWyejzH+bDoYysX0IxQzZkHtpVJNlYDLjGQLBE3CeE0kE:OJhH+bDo3iN0Z2TVJkXBBE3yb
MD5:	7B955D976803304F2C0505431A0CF1CF
SHA1:	E29070081B18DA0EF9D98D4389091962E3D37216
SHA-256:	987FB9BFC2A84C4C605DCB339D4935B52A969B24E70D6DEAC8946BA9A2B432DC
SHA-512:	CE2F1709F39683BE4131125BED409103F5EDF1DED545649B186845817C0D69E3D0B832B236F7C4FC09AB7F7BB88E7C9F1E4F7047D1AF56D429752D4D8CBED47A
Malicious:	false
Preview:	SQLite format 3.....@ .....&.....j..... ....

C:\Users\user\AppData\Local\Temp\span1UB98D2D2zeo\OaQuGlYHO2B0Web Data

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 3, database pages 52, cookie 0x21, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	106496
Entropy (8bit):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84
MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\span1UB98D2D2zeo\Pe4W1HgFYxyTHistory	
Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 1, database pages 38, cookie 0x1f, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	155648
Entropy (8bit):	0.5407252242845243
Encrypted:	false
SSDEEP:	96:OgWyejzH+bDoYysX0IxQzZkHtpVJNlYDLjGQLBE3CeE0kE:OJhH+bDo3iN0Z2TVJkXBBE3yb
MD5:	7B955D976803304F2C0505431A0CF1CF
SHA1:	E29070081B18DA0EF9D98D4389091962E3D37216
SHA-256:	987FB9BFC2A84C4C605DCB339D4935B52A969B24E70D6DEAC8946BA9A2B432DC
SHA-512:	CE2F1709F39683BE4131125BED409103F5EDF1DED545649B186845817C0D69E3D0B832B236F7C4FC09AB7F7BB88E7C9F1E4F7047D1AF56D429752D4D8CBED47A
Malicious:	false
Preview:	SQLite format 3.....@ .....&.....j..... ....

C:\Users\user\AppData\Local\Temp\span1UB98D2D2zeo\UdeNZdOQSPDWWeb Data	
Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 3, database pages 52, cookie 0x21, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	106496
Entropy (8bit):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84
MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF
SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....!.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\span1UB98D2D2zeo\VCEccbr_cvO2Cookies	
Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 4, database pages 5, cookie 0x3, schema 4, UTF-8, version-valid-for 4
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.8439810553697228
Encrypted:	false
SSDEEP:	24:TLyAF1kwNbXYFpFNYcw+6UwcQVXH5fBO9p7n52GmCWGf+dyMDCFVE1:TeAFawNLopFgU10XJBOB2Gbf+ba+
MD5:	9D46F142BBCF25D0D495FF1F3A7609D3
SHA1:	629BD8CD800F9D5B078B5779654F7CBFA96D4D4E
SHA-256:	C11B443A512184E82D670BA6F7886E98B03C27CC7A3CEB1D20AD23FCA1DE57DA
SHA-512:	AC90306667AFD38F73F6017543BDBB0B359D79740FA266F587792A94FDD35B54CCE5F6D85D5F6CB7F4344BEDAD9194769ABB3864AAE7D94B4FD6748C31250A02
Malicious:	false
Preview:	SQLite format 3.....@ .....j.....g...$..... ....

C:\Users\user\AppData\Local\Temp\span1UB98D2D2zeo\g85sD372nZcyCookies	
Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, file counter 7, database pages 5, cookie 0x5, schema 4, UTF-8, version-valid-for 7
Category:	dropped
Size (bytes):	20480

Entropy (8bit):	0.6732424250451717
Encrypted:	false
SSDEEP:	24:TLO1nKbXYFpFNYcoqT1kwE6UwpQ9YHVXxZ6HfB:Tq1KLopF+SawLUO1Xj8B
MD5:	CFFF4E2B77FC5A18AB6323AF9BF95339
SHA1:	3AA2C2115A8EB4516049600E8832E9BFFE0C2412
SHA-256:	EC8B67EF7331A87086A6CC085B085A6B7FFFD325E1B3C90BD3B9B1B119F696AE
SHA-512:	0BFDC8D28D09558AA97F4235728AD656FE9F6F2C61DDA2D09B416F89AB60038537B7513B070B907E57032A68B9717F03575DB6778B68386254C8157559A3F1BC
Malicious:	false
Preview:	SQLite format 3.....@ .....j...$.....g.....

C:\Users\user\AppData\Local\Temp\span1UB98D2D2zeo\llmcrdwzLnNKYB4T0Vnw.exe

Process:	C:\Users\user\Desktop\file.exe
File Type:	MS-DOS executable PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows, MZ for MS-DOS
Category:	dropped
Size (bytes):	4563640
Entropy (8bit):	7.906115886926003
Encrypted:	false
SSDEEP:	98304:RpvmMxvdjYr/2BLOizdh/0Rzs24+WhXWXfRqCFh6MacgD5hB:vlVjMuBx0R7RrXpqiUhB
MD5:	AF6E384DFABDAD52D43CF8429AD8779C
SHA1:	C78E8CD8C74AD9D598F591DE5E49F73CE3373791
SHA-256:	F327C2B5AB1D98F0382A35CD78F694D487C74A7290F1FF7BE53F42E23021E599
SHA-512:	B55BA87B275A475E751E13EC9BAC2E7F1A3484057844E210168E2256D73D9B6A7C7C7592845D4A3BF8163CF0D479315418A9F3CB8F2F4832AF88A06867E3DF93
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 83%
Preview:	MZ@.....!..L.!Win32 .EXE...$@...PE..L....M.a.....^.....w.....0....@.....}.....m.F.....w.....w.|.....E.....P.w.....MPRESS1.pw.....?.....MPRESS22.....w.....?.....rsrc...|.....w.....?.....@.....v2.19w...?. ...o.....G>H.r9aQ..(.....`....=....?....!.Z..&I.....I18..Z!..Y..s...[QX....a....YY...).v.....n.....|)....^f..+.>..84h82g...>*.hb\...E.(.x.....@.8 _.9.4U.m..'.s.....#.....03.....O..]`..S2.@#.....oF~.*.R..Q..q.o.yn...OA@|....g....F....0.j.....s/..H..+ 0C.!....7s..^H,..... ..{.....D.....r.I..,|.....u.6.....E>q..}....g..).U..ME.'.j}.. .....7^...w.....Le.....k.T.`.#%....b..n.F.&-o..../8S.E..{1.E..,....<.c|b.z.Fz.....|..W"p.

C:\Users\user\AppData\Local\Temp\span1UB98D2D2zeo\qUesDvUI_ZiWeb Data

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.121297215059106
Encrypted:	false
SSDEEP:	384:72qOB1nxCkvSAELyKOMq+8yC8F/YfU5m+OlT:qq+n0E9ELyKOMq+8y9/Ow
MD5:	D87270D0039ED3A5A72E7082EA71E305
SHA1:	0FBACFA8029B11A5379703ABE7B392C4E46F0BD2
SHA-256:	F142782D1E80D89777EFA82C9969E821768DE3E9713FC7C1A4B26D769818AAAA
SHA-512:	18BB9B498C225385698F623DE06F93F9CFF933FE98A6D70271BC6FA4F866A0763054A4683B54684476894D9991F64CAC6C63A021BDFEB8D493310EF2C779638D
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....6.....j.....W.....

C:\Users\user\AppData\Local\Temp\span1UB98D2D2zeo\sl01HQPBKH54Web Data

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 3, database pages 52, cookie 0x21, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	106496
Entropy (8bit):	1.136413900497188
Encrypted:	false
SSDEEP:	192:ZWTblyVZTnGtgTgabTanQeZVuSVumZa6cV/04:MnlyfnGtxnfVuSVumEHV84
MD5:	429F49156428FD53EB06FC82088FD324
SHA1:	560E48154B4611838CD4E9DF4C14D0F9840F06AF

SHA-256:	9899B501723B97F6943D8FE6ABF06F7FE013B10A17F566BF8EFBF8DCB5C8BFAF
SHA-512:	1D76E844749C4B9566B542ACC49ED07FA844E2AD918393D56C011D430A3676FA5B15B311385F5DA9DD24443ABF06277908618A75664E878F369F68BEBE4CE52F
Malicious:	false
Preview:	SQLite format 3.....@ .....4.....l.....j.....1..... ....

C:\Users\user\AppData\Local\Temp\span1UB98D2D2zeo\tnqSg6erqMxtWeb Data

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 8, database pages 89, cookie 0x36, schema 4, UTF-8, version-valid-for 8
Category:	dropped
Size (bytes):	196608
Entropy (8bit):	1.121297215059106
Encrypted:	false
SSDEEP:	384:72qOB1nxCkvSAELyKOMq+8yC8F/YfU5m+OlT:qq+n0E9ELyKOMq+8y9/Ow
MD5:	D87270D0039ED3A5A72E7082EA71E305
SHA1:	0FBACFA8029B11A5379703ABE7B392C4E46F0BD2
SHA-256:	F142782D1E80D89777EFA82C9969E821768DE3E9713FC7C1A4B26D769818AAAA
SHA-512:	18BB9B498C225385698F623DE06F93F9CFF933FE98A6D70271BC6FA4F866A0763054A4683B54684476894D9991F64CAC6C63A021BDFEB8D493310EF2C779638D
Malicious:	false
Preview:	SQLite format 3.....@ .....Y.....6.....j.....W..... ....

C:\Users\user\AppData\Local\Temp\span1UB98D2D2zeo\yDHoBcv6VALYLogin Data For Account

Process:	C:\Users\user\Desktop\file.exe
File Type:	SQLite 3.x database, last written using SQLite version 3042000, page size 2048, file counter 1, database pages 20, cookie 0xb, schema 4, UTF-8, version-valid-for 1
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.8553638852307782
Encrypted:	false
SSDEEP:	48:2x7BA+IIF7CVEq8Ma0D0HOlf/6ykwp1EUwMHZq10bvJKLkw8s8LKvUf9KVyJ7h/f:QNDCn8MouB6wz8iZqmvJKLPeymwil
MD5:	28222628A3465C5F0D4B28F70F97F482
SHA1:	1BAA3DEB7DFD7C9B4CA9FDB540F236C24917DD14
SHA-256:	93A6AF6939B17143531FA4474DFC564FA55359308B910E6F0DCA774D322C9BE4
SHA-512:	C8FB93F658C1A654186FA6AA2039E40791E6B0A1260B223272BB01279A7B574E238B28217DADF3E1850C7083ADFA2FE5DA0CCE6F9BCABD59E1FFD1061B3A88F7
Malicious:	false
Preview:	SQLite format 3.....@ .....j..... ....

C:\Users\user\AppData\Local\Temp\trixy1UB98D2D2zeo\Cookies\Chrome_Default.txt

Process:	C:\Users\user\Desktop\file.exe
File Type:	ASCII text, with very long lines (369), with CRLF line terminators
Category:	dropped
Size (bytes):	530
Entropy (8bit):	5.999391385907715
Encrypted:	false
SSDEEP:	12:copYxSlufq7gCx7Fbyr4rOSlTfJJADr6HDsZQZ7gC6:KauS79Gr4iSllJALQZ7c
MD5:	06ED2CD304730F55A5C7001509E128BE
SHA1:	49651485B2CE3D239172BD52BF5A265AB3EB8E18
SHA-256:	66851B5AA77B3DEE71B842F53D4E30F664F5A08F9754B9E87B323871981516A4
SHA-512:	0163A8537DE695D34865EEB9C872F15A1827644D8797344A2D36E776F174E5901E77AA560488B0D7D7359B3648614F818B85A7D51F59CCDF2831B5715F5A9334
Malicious:	false
Preview:	.google.com.FALSE./.TRUE.1699018815.1P_JAR.ENC893*_djEwmUj/dRHWNmfhbTB/w+u3HcpAF49UGcxvovgmz9ye9OQyJO9KCFHkRm8=_Spn23kok+Q5pGfoIFZdfhpScu2LLLElOWGEpK4fGivY=*...google.com.TRUE./.TRUE.1712238015.NID.ENC893*_djEwFCqquAx+Q1mLxpuZeEBJZSgzAt4Ngo/HHXcYPxMGlNXG0MJzCe/y7m5VzpUyfsA6ingOdNobTvWP/YbKYpzg64nmGlCjRU9RpPIjDAuAxGlp5MTMUaOP4iC8aSCuijjqDE5gAdZQ5Jgb0/uEAZ4ssWGDsxXJbqpGbi04viYfPDhBfQ9XKXznqtHW/weYlNZJlGlKZBsCWoEIKfuL56VHKaBt04gLO/XK1/P3nHsp6pSc1x1uk1RRK7hSYUjCY5G/hcpBBjFv74dICDI=_Spn23kok+Q5pGfoIFZdfhpScu2LLLElOWGEpK4fGivY=*..

C:\Users\user\AppData\Local\Temp\trixy1UB98D2D2zeo\History\Firefox_v6zchhhv.default-release.txt

Process:	C:\Users\user\Desktop\file.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	112
Entropy (8bit):	4.9113057226932435
Encrypted:	false
SSDEEP:	3:N8DSLvlJiMgTE2WdkQVjDSLvlJiMhKVX3L2WdkQVQ:2OLciodFOLciA8dq
MD5:	0CE7E561D96623E70DD177304D3B56DA
SHA1:	27B4131817E71657AED90C086E01E7E925BF641E
SHA-256:	E0B2F92CFB58B7D5EDFBB1FDF3E81194D4E55A90706986C389BDF21D2AD2325D
SHA-512:	48154E76523305BBB7ED39FEAD22CB4DD6FDD568259DC8D0E70ABA4A21030DAF6D1274E0DC5D7F10DFCF7B3B61BD2401FFB4768F301AEF04F142AF23EF335A B5
Malicious:	false
Preview:	http://https://www.mozilla.org/privacy/firefox/.1696426831..https://www.mozilla.org/en-US/privacy/firefox/.1696426831..

C:\Users\user\AppData\Local\Temp\trixy1UB98D2D2zeo\information.txt

Process:	C:\Users\user\Desktop\file.exe
File Type:	ASCII text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	6549
Entropy (8bit):	5.6055337767834965
Encrypted:	false
SSDEEP:	96:xzDyJ2mRkoc2KBhA6tsxODsZ8svxhjANUbg3x:xfYyoX6tsxPZ8skB
MD5:	F949146D8F44A5E3B39FFA8B299C2CE4
SHA1:	7764E054E6A828328274D08D593F17D996027466
SHA-256:	34F3899A8081AA366C82D37E25B800E63D675DB221E3BB375D785C3BDE64B2D3
SHA-512:	1E2843ECFFEF386A1BC2A08619A2256A2D639E20C886D5A7349D11EC38C10FDA574010740EC909FACA4EB938FEE666CB37B2AF9DDB7EBA7C5C89DE8BD3369 423
Malicious:	false
Preview:	Build: default..Version: 2.0....Date: Fri May 17 17:45:09 2024.MachineID: 9e146be9-c76a-4720-bcdb-53011b87bd06..GUID: {a33c7340-61ca-11ee-8c18-806e6f6 e6963}..HWID: 3d7cb3c48b150bab83c70d51fda6606f....Path: C:\Users\user\Desktop\file.exe..Work Dir: C:\Users\user\AppData\Local\Temp\trixy1UB98D2D2zeo....IP: 12.205.151.60..Location: US, San Francisco..ZIP (Autofills): -..Windows: Windows 10 Pro [x64]..Computer Name: 855271 [WORKGROUP]..User Name: user..Display Resolution: 1280x1024..Display Language: en-CH..Keyboard Languages: English (United Kingdom) / English (United Kingdom)..Local Time: 17/5/2024 17:45:9..TimeZon e: UTC-5....[Hardware]..Processor: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz..CPU Count: 4..RAM: 8191 MB..VideoCard #0: Microsoft Basic Display Adapter....[Process es]..System [4]..Registry [92]..smss.exe [332]..csrss.exe [420]..wininit.exe [496]..csrss.exe [504]..winlogon.exe [564]..services.exe [632]..lsass.exe [640]..svchost.exe [752]..fontdrvhost.exe [780]..fontdrvhost.ex

C:\Users\user\AppData\Local\Temp\trixy1UB98D2D2zeo\passwords.txt

Process:	C:\Users\user\Desktop\file.exe
File Type:	Unicode text, UTF-8 text, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	4897
Entropy (8bit):	2.518316437186352
Encrypted:	false
SSDEEP:	48:4MMMMMMMMMMdMMMM1MMMMMMMM1MMMMMMMM1MMMMMMMM1MMMMMMMMMdMMMMMMMM3:q
MD5:	B3E9D0E1B8207AA74CB8812BAAF52EAE
SHA1:	A2DCE0FB6B0BBC955A1E72EF3D87CADCC6E3CC6B
SHA-256:	4993311FC913771ACB526BB5EF73682EDA69CD31AC14D25502E7BDA578FFA37C
SHA-512:	B17ADF4AA80CADC581A09C72800DA22F62E5FB32953123F2C513D2E88753C430CC996E82AAE7190C8CB3340FCF2D9E0D759D99D909D2461369275FBE5C68C2 A
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\trixy1UB98D2D2zeo\screenshot.png

Process:	C:\Users\user\Desktop\file.exe
File Type:	PNG image data, 1280 x 1024, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	711746

Entropy (8bit):	7.924358481947605
Encrypted:	false
SSDEEP:	12288:LN5Ik7hE5TUlevY31R2XSefNY396zjUvZKyn7tg1czUxd8B+x5ruugEnlV1MCvXu:Yk78Uj1RySeC0zjoKy7e1Z/8ofcEjm
MD5:	576DFC1AEDDC22FF1B5B2ED158DCDEFD
SHA1:	3BF1C8AC4E8541BB33DB2F6672DF544F5C32B4D4
SHA-256:	9731A447D10DC67279FC1D5DA41A48637E4FE5C685FDC95EAF090EA0B6BEA50F
SHA-512:	7AB6B3136DFF3CFA505266649352247BBBE3303D2DE02453D695693EA1FB5015F9925669BC555A15F66033484F613EAD769560AD60A9546C31C74781D9BEA7D3
Malicious:	false
Preview:	.PNG.....IHDR.....C....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^..w.mG.....ms.....c...~.VuU..UUt.V.{o.....$.....$.,.@.S.E...9...d...../.....1#..;...7f.....<9.'...N....^'?5..I.....3.....Nx|..7"S..|_.....:~..q....-.WI!.....y1.....0|...Jo.C.b....H.G.}G0u.....X..h.....w...b.....S.....].|...J...L.TE..w.....X...{.A.=w.d.."....w.=...w..1...'.....A.Z~0+..>7.o..H.TL.....g..L.%.....M.Y..|_..z.wG...1S..Na....^{.....:Gc..1.....k,|..z.-...%..2..w.knJ.W.....t..3X..S...../.X...c....{e....\?...L..%.7,}E.g..2...X....u.....|..i..y...MK^~M..X.....].-....9g.?.}.u..6M.uM..yu..qU.._..|o9.. .v...9gEn...y.....nW.9.K.>..,....hk...=.N.....0^.{....B..+...}.O+.....#..=.....].k..../L.zY.....|.|...v...-.....u3.....+.g].?..]//..-.%.S.s.o...s...;....S;\RX..yLN.s.Kv..P....!.}..v...m/)..;....osq7.s.a..y_..b-.....vy}n5^.m....d.|..'.<A.y`n..;.1..{.....E%...%.\].

C:\Users\user\AppData\Roaming\Microsoft\Protect\oobeldr.exe

Process:	C:\Users\user\AppData\Local\Temp\span1UB98D2D2zeo\llmcrdwzLnNKYB4T0Vnw.exe
File Type:	MS-DOS executable PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows, MZ for MS-DOS
Category:	dropped
Size (bytes):	4563640
Entropy (8bit):	7.906115886926003
Encrypted:	false
SSDEEP:	98304:RpvmMxvdjYr/2BLOizdh/0Rzs24+WhXWXfRqCFh6MacgD5hB:vlVjMuBx0R7RrXpqiUhB
MD5:	AF6E384DFABDAD52D43CF8429AD8779C
SHA1:	C78E8CD8C74AD9D598F591DE5E49F73CE3373791
SHA-256:	F327C2B5AB1D98F0382A35CD78F694D487C74A7290F1FF7BE53F42E23021E599
SHA-512:	B55BA87B275A475E751E13EC9BAC2E7F1A3484057844E210168E2256D73D9B6A7C7C7592845D4A3BF8163CF0D479315418A9F3CB8F2F4832AF88A06867E3DF93
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 83%
Preview:	MZ@.....!..L.!Win32 .EXE...$@...PE..L....M.a.....^.....w.....0....@.....}.....m.F.....w.....w.|.....E.....P.w.....MPRESS1.pw.....?.....MPRESS22.....w.....?.....rsrc...|.....w.....?.....@.....v2.19w...?. ...o.....G>H.r9aQ..(.....`....=....?....!.Z..&I.....I18..Z!..Y..s...[QX....a....YY...).v.....n.....|)....^f..+.>..84h82g...>*.hb\...E.(.x.....@.8_.9.4U.m..'.s.....#.....03.....O..]`..S2.@#.....oF~.*.R..Q..q.o.yn...OA@|....g...F....0.j.....s/..H..+ 0C.!....7s..^H,..... ..{.....D.....r.I..|.....u.6.....E>q..}....g..).U..ME.'.j}.....7^...w.....Le.....k.T.`.#%....b..n.F.&-o..../8S.E..{1.E..,....<.c|b.z.Fz.....|..W"p.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\EdgeMS2.lnk

Process:	C:\Users\user\Desktop\file.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Description string, Has Relative path, Archive, ctime=Fri May 17 20:45:15 2024, mtime=Fri May 17 20:45:15 2024, atime=Fri May 17 20:45:15 2024, length=4563640, window=hide
Category:	dropped
Size (bytes):	1330
Entropy (8bit):	4.862977598680543
Encrypted:	false
SSDEEP:	24:8KHfmf8HVMQROgKb6xA9lE9d7lwXAIB1yNdFd2aSnqygm:8KHuErRy6xIExwwIB1yVryg
MD5:	C519A29483EE8E20AA66C2CBC23EA91F
SHA1:	245FD3D3F14D96CF46380E7DB0018727F62E16D7
SHA-256:	0399769E4CD0930D72CED5E76A98ACB37116D28F75A3FF8C27D385DFA9774B12
SHA-512:	CA8EF450FD17E6CEF7F1D28727ED90A36FD60F0E263E022F48B4017AC6AE80D14EE23E14A16D4525BB491BEBB47EA48D9121ADD350684578C9E39CAA19F62335
Malicious:	false
Preview:	L.....F.... ...c.....c.....E.....X.:..DG..Yr?.D..U..k0.&...&..... M.....p....$.....t...CFSF..1.....DWSl..AppData...t.Y^...H.g.3..(.....gVA.G..k...@.....DWSl.X.....B.....Bdg.A.p.p.D.a.t.a...B.P.1.....X....Local.<.....DWSl.X.....V.....S4N.L.o.c.a.l.....N.1.....X....Temp..:.....DWSl.X.....\.....T.e.m.p.....1.....X....EDGEMS~1.....X...X..... .E.d.g.e.M.S.2._.4.5.c.4.8.c.c.e.2.e.2.d.7.f.b.d.e.a.1.a.f.c.5.1.c.7.c.6.a.d.2.6.....b.2...E..X.. .EdgeMS2.exe.H.....X...X.....c.q.E.d.g.e.M.S.2...e.x.e.....-.....C:\Users\user\AppData\Local\Temp\EdgeMS2_45c48cce2e2d7fbdea1afc51c7c6ad26\EdgeMS2.exe....E.d.g.e.M.S.2.Q.....\.....\.....\.....\.....\.....\.L.o.c.a.l.\.T.e.m.p.\.E.d.g.e.M.S.2._.4.5.c.4.8.c.c.e.2.e.2.d.7.f.b.d.e.a.1.a.f.c.5.1.c.7.c.6.a.d.2.6.\.E.d.g.e.M.S.2...e.x.e.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.973325521474956

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:	file.exe
File size:	8'778'752 bytes
MD5:	3d09739846543f4962f2b432da671c29
SHA1:	2247e38b1f5257df93db091328488c652f6bea0a
SHA256:	70aaa6e67944e919f8c7bbdf71b6b09deed41f51166bc1dc15fc6f66efc1b014
SHA512:	f762d0c8d9ce9a8a7189af007ec9b6e4ff863005f982d107b2b276281152f64386425b7fbe8ceda2b96ab9d7f827eb99358e3920ec79c9f5a063b87aa7e7bf5d
SSDEEP:	196608:EMnAaGWGFMEFFP8/1IK56wtjoRvH8FPuAfs/4:ZnAafG5w/1I4TtsRvqur
TLSH:	F796336331651185D1EAC93E9A377E9533F2523F464184FCB4A97FC22AE25F5E203A83
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...jR;f.....'.....? X.....@.....p.....@.....

File Icon

Icon Hash:	07e3b7d7b794c087

Static PE Info

General

Entrypoint:	0xc7583f
Entrypoint Section:	.vmpY[.
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, TERMINAL_SERVER_AWARE
Time Stamp:	0x663B526A [Wed May 8 10:22:34 2024 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	d784b50e0634f83cc71436d4fb111768

Entrypoint Preview

Instruction
push D6FCCA80h
call 00007F2B8D8299F1h
inc ecx
jmp 00007F2B8D27FB97h
stc
xor edx, 1F142980h
stc
xor ebx, edx
cmp di, 1557h
stc
add ebp, edx
jmp 00007F2B8D3AC82Dh
je 00007F2B8D366777h
mov bl, cl
sub bl, 00000030h
jmp 00007F2B8D36D01Ch
dec edx

Instruction
cmp esp, 40C2572Eh
xor ebx, edx
add edi, edx
jmp 00007F2B8D30919Ah
jmp 00007F2B8D229C49h
inc ecx
dec ebx
push ebp
inc esp
xor dword ptr [esp], ebx
inc eax
xchg ch, ch
inc eax
shl ch, FFFFFFA1h
bt bp, sp
pop ebp
stc
inc ebp
test cl, ah
dec ebp
arpl bx, bx
inc esp
test bl, dl
jmp 00007F2B8D29711Ah
or esi, ebx
lodsb
test dword ptr [eax-0879947Ah], 8E05EDA3h
neg dword ptr [edx+eax+52F795DBh]
mov ah, 54h
sahf
or dword ptr [eax+08CC3DDEh], esp
dec esi
sbb byte ptr [esi+08h], ah
int1

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xed6cf8	0x190	.vmpY[.
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xf76000	0x26ee8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xf75000	0x5c8	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xd25c80	0x20	.vmpY[.
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xf73760	0x40	.vmpY[.
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x75a000	0x290	.vmpY[.
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x7b1880	0x40	.vmpY[.
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics

Name	Virtual Address	Virtual Size	Raw Size	MD5	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x15bae8	0x0	d41d8cd98f00b204e9800998ecf8427e	False	0	empty	0.0	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x15d000	0x27e32	0x0	d41d8cd98f00b204e9800998ecf8427e	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x185000	0x4930	0x0	d41d8cd98f00b204e9800998ecf8427e	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.vmp#+	0x18a000	0x121e7a	0x0	d41d8cd98f00b204e9800998ecf8427e	False	0	empty	0.0	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.vmp#+	0x2ac000	0x580	0x0	d41d8cd98f00b204e9800998ecf8427e	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.vmp#+	0x2ad000	0x1427e0	0x0	d41d8cd98f00b204e9800998ecf8427e	False	0	empty	0.0	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.vmpY[.	0x3f0000	0x34b3e7	0x0	d41d8cd98f00b204e9800998ecf8427e	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.vmpY[.	0x73c000	0x838010	0x838200	bdacb5ec0292c102fa3f2bae395ef848	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.reloc	0xf75000	0x5c8	0x600	2025a475ee6a4cf5d3bdd2e9ccf3e193	False	0.5325520833333334	data	4.322933984772373	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xf76000	0x26ee8	0x26800	dd048426ffb4368f719a01897ce94a50	False	0.6937715604707793	data	6.736445338106505	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
AFX_DIALOG_LAYOUT	0xf9c6bc	0x2	data	Korean	North Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c6bc	0x2	data	Korean	South Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c6c0	0x2	data	Korean	North Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c6c0	0x2	data	Korean	South Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c6c4	0x2	data	Korean	North Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c6c4	0x2	data	Korean	South Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c6c8	0x2	data	Korean	North Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c6c8	0x2	data	Korean	South Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c6cc	0x2	data	Korean	North Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c6cc	0x2	data	Korean	South Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c6d0	0x2	data	Korean	North Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c6d0	0x2	data	Korean	South Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c6d4	0x2	data			5.0
AFX_DIALOG_LAYOUT	0xf9c6d8	0x2	data	Korean	North Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c6d8	0x2	data	Korean	South Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c6dc	0x2	data			5.0
AFX_DIALOG_LAYOUT	0xf9c6e0	0x2	data	Korean	North Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c6e0	0x2	data	Korean	South Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c6e4	0x2	data			5.0
AFX_DIALOG_LAYOUT	0xf9c6e8	0x2	data	Korean	North Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c6e8	0x2	data	Korean	South Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c6ec	0x2	data			5.0

Name	RVA	Size	Type	Language	Country	ZLIB Complexity
AFX_DIALOG_LAYOUT	0xf9c6f0	0x2	data	Korean	North Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c6f0	0x2	data	Korean	South Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c6f4	0x2	data			5.0
AFX_DIALOG_LAYOUT	0xf9c6f8	0x2	data	Korean	North Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c6f8	0x2	data	Korean	South Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c6fc	0x2	data			5.0
AFX_DIALOG_LAYOUT	0xf9c700	0x2	data	Korean	North Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c700	0x2	data	Korean	South Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c704	0x2	data			5.0
AFX_DIALOG_LAYOUT	0xf9c708	0x2	data	Korean	North Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c708	0x2	data	Korean	South Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c70c	0x2	data			5.0
AFX_DIALOG_LAYOUT	0xf9c710	0x2	data	Korean	North Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c710	0x2	data	Korean	South Korea	5.0
AFX_DIALOG_LAYOUT	0xf9c714	0x7a	data			0.09836065573770492
AFX_DIALOG_LAYOUT	0xf9c790	0x7a	data	Korean	North Korea	0.10714285714285714
AFX_DIALOG_LAYOUT	0xf9c790	0x7a	data	Korean	South Korea	0.10714285714285714
AFX_DIALOG_LAYOUT	0xf9c80c	0x2	empty			0
AFX_DIALOG_LAYOUT	0xf9c810	0x2	empty	Korean	North Korea	0
AFX_DIALOG_LAYOUT	0xf9c810	0x2	empty	Korean	South Korea	0
AFX_DIALOG_LAYOUT	0xf9c814	0x2	empty			0
AFX_DIALOG_LAYOUT	0xf9c818	0x2	empty	Korean	North Korea	0
AFX_DIALOG_LAYOUT	0xf9c818	0x2	empty	Korean	South Korea	0
AFX_DIALOG_LAYOUT	0xf9c81c	0x2	empty			0
AFX_DIALOG_LAYOUT	0xf9c820	0x2	empty	Korean	North Korea	0
AFX_DIALOG_LAYOUT	0xf9c820	0x2	empty	Korean	South Korea	0
AFX_DIALOG_LAYOUT	0xf9c824	0x2	empty			0
AFX_DIALOG_LAYOUT	0xf9c828	0x2	empty	Korean	North Korea	0
AFX_DIALOG_LAYOUT	0xf9c828	0x2	empty	Korean	South Korea	0
AFX_DIALOG_LAYOUT	0xf9c82c	0x5a	empty			0
AFX_DIALOG_LAYOUT	0xf9c888	0x5a	empty	Korean	North Korea	0
AFX_DIALOG_LAYOUT	0xf9c888	0x5a	empty	Korean	South Korea	0
AFX_DIALOG_LAYOUT	0xf9c8e4	0x2	empty			0
AFX_DIALOG_LAYOUT	0xf9c8e8	0x2	empty	Korean	North Korea	0
AFX_DIALOG_LAYOUT	0xf9c8e8	0x2	empty	Korean	South Korea	0
RT_ICON	0xf768b4	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024			0.774822695035461
RT_ICON	0xf76d1c	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216			0.5385892116182572
RT_ICON	0xf792c4	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 65536			0.4255441854962735
RT_ICON	0xf89aec	0x11965	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced			0.999250385218707
RT_MENU	0xf9c8ec	0x2f4	empty			0
RT_MENU	0xf9cbe0	0x308	empty	Korean	North Korea	0
RT_MENU	0xf9cbe0	0x308	empty	Korean	South Korea	0
RT_GROUP_ICON	0xf9b454	0x3e	data			0.8225806451612904
RT_VERSION	0xf9b494	0x3ec	data			0.3615537848605578
RT_MANIFEST	0xf9b880	0xe3b	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators			0.38594564919022784

Imports

DLL	Import
KERNEL32.dll	GetVersionExA
USER32.dll	wsprintfA
GDI32.dll	CreateCompatibleBitmap
ADVAPI32.dll	RegQueryValueExA
SHELL32.dll	ShellExecuteA
ole32.dll	CoInitialize
WS2_32.dll	WSAStartup

DLL	Import
CRYPT32.dll	CryptUnprotectData
SHLWAPI.dll	PathFindExtensionA
gdiplus.dll	GdipGetImageEncoders
SETUPAPI.dll	SetupDiEnumDeviceInfo
ntdll.dll	RtlUnicodeStringToAnsiString
RstrtMgr.DLL	RmStartSession
KERNEL32.dll	HeapAlloc, HeapFree, ExitProcess, GetModuleHandleA, LoadLibraryA, GetProcAddress
WTSAPI32.dll	WTSSendMessageW
KERNEL32.dll	VirtualQuery, GetSystemTimeAsFileTime, GetModuleHandleA, CreateEventA, GetModuleFileNameW, LoadLibraryA, TerminateProcess, GetCurrentProcess, CreateToolhelp32Snapshot, Thread32First, GetCurrentProcessId, GetCurrentThreadId, OpenThread, Thread32Next, CloseHandle, SuspendThread, ResumeThread, WriteProcessMemory, GetSystemInfo, VirtualAlloc, VirtualProtect, VirtualFree, GetProcessAffinityMask, SetProcessAffinityMask, GetCurrentThread, SetThreadAffinityMask, Sleep, FreeLibrary, GetTickCount, SystemTimeToFileTime, FileTimeToSystemTime, GlobalFree, LocalAlloc, LocalFree, GetProcAddress, ExitProcess, EnterCriticalSection, LeaveCriticalSection, InitializeCriticalSection, DeleteCriticalSection, GetModuleHandleW, LoadResource, MultiByteToWideChar, FindResourceExW, FindResourceExA, WideCharToMultiByte, GetThreadLocale, GetUserDefaultLCID, GetSystemDefaultLCID, EnumResourceNamesA, EnumResourceNamesW, EnumResourceLanguagesA, EnumResourceLanguagesW, EnumResourceTypesA, EnumResourceTypesW, CreateFileW, LoadLibraryW, GetLastError, FlushFileBuffers, CreateFileA, WriteConsoleW, GetConsoleOutputCP, WriteConsoleA, GetCommandLineA, RaiseException, RtlUnwind, HeapFree, GetCPInfo, InterlockedIncrement, InterlockedDecrement, GetACP, GetOEMCP, IsValidCodePage, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, SetLastError, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, HeapAlloc, LCMapStringA, LCMapStringW, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, HeapCreate, HeapDestroy, QueryPerformanceCounter, HeapReAlloc, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, HeapSize, WriteFile, SetFilePointer, GetConsoleCP, GetConsoleMode, InitializeCriticalSectionAndSpinCount, SetStdHandle
USER32.dll	GetProcessWindowStation, GetUserObjectInformationW, CharUpperBuffW, MessageBoxW
KERNEL32.dll	LocalAlloc, LocalFree, GetModuleFileNameW, GetProcessAffinityMask, SetProcessAffinityMask, SetThreadAffinityMask, Sleep, ExitProcess, FreeLibrary, LoadLibraryA, GetModuleHandleA, GetProcAddress
USER32.dll	GetProcessWindowStation, GetUserObjectInformationW

Possible Origin

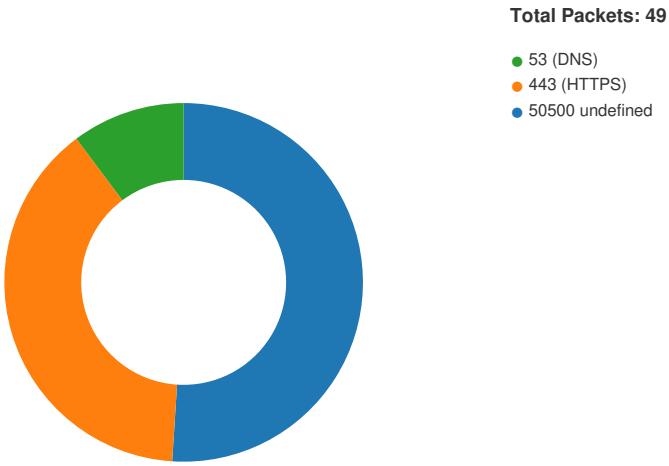
Language of compilation system	Country where language is spoken	Map
Korean	North Korea	
Korean	South Korea	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/17/24-23:45:00.848746	TCP	2049060	ET TROJAN RisePro TCP Heartbeat Packet	49704	50500	192.168.2.5	5.42.96.65
05/17/24-23:45:05.461512	TCP	2046269	ET TROJAN [ANY.RUN] RisePro TCP (Activity)	49704	50500	192.168.2.5	5.42.96.65
05/17/24-23:45:05.093768	TCP	2046268	ET TROJAN [ANY.RUN] RisePro TCP v.0.x (Get_settings)	49704	50500	192.168.2.5	5.42.96.65
05/17/24-23:45:14.161367	TCP	2019714	ET CURRENT_EVENTS Terse alphanumeric executable downloader high likelihood of being hostile	49707	80	192.168.2.5	5.42.96.170
05/17/24-23:45:02.216807	TCP	2046267	ET TROJAN [ANY.RUN] RisePro TCP (External IP)	50500	49704	5.42.96.65	192.168.2.5
05/17/24-23:45:01.844974	TCP	2046266	ET TROJAN [ANY.RUN] RisePro TCP (Token)	50500	49704	5.42.96.65	192.168.2.5

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 17, 2024 23:45:00.823570013 CEST	49704	50500	192.168.2.5	5.42.96.65
May 17, 2024 23:45:00.830173969 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:00.830306053 CEST	49704	50500	192.168.2.5	5.42.96.65
May 17, 2024 23:45:00.848746061 CEST	49704	50500	192.168.2.5	5.42.96.65
May 17, 2024 23:45:00.888148069 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:01.844974041 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:01.898729086 CEST	49704	50500	192.168.2.5	5.42.96.65
May 17, 2024 23:45:02.212306023 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:02.212758064 CEST	49704	50500	192.168.2.5	5.42.96.65
May 17, 2024 23:45:02.216774940 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:02.216806889 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:02.216887951 CEST	49704	50500	192.168.2.5	5.42.96.65
May 17, 2024 23:45:02.442466974 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:02.442562103 CEST	49704	50500	192.168.2.5	5.42.96.65
May 17, 2024 23:45:02.447838068 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:02.505626917 CEST	49705	443	192.168.2.5	34.117.186.192
May 17, 2024 23:45:02.505665064 CEST	443	49705	34.117.186.192	192.168.2.5
May 17, 2024 23:45:02.505752087 CEST	49705	443	192.168.2.5	34.117.186.192
May 17, 2024 23:45:02.507396936 CEST	49705	443	192.168.2.5	34.117.186.192
May 17, 2024 23:45:02.507406950 CEST	443	49705	34.117.186.192	192.168.2.5
May 17, 2024 23:45:03.331181049 CEST	443	49705	34.117.186.192	192.168.2.5
May 17, 2024 23:45:03.331459045 CEST	49705	443	192.168.2.5	34.117.186.192
May 17, 2024 23:45:03.335395098 CEST	49705	443	192.168.2.5	34.117.186.192
May 17, 2024 23:45:03.335402012 CEST	443	49705	34.117.186.192	192.168.2.5
May 17, 2024 23:45:03.335609913 CEST	443	49705	34.117.186.192	192.168.2.5
May 17, 2024 23:45:03.383002043 CEST	49705	443	192.168.2.5	34.117.186.192
May 17, 2024 23:45:03.397473097 CEST	49705	443	192.168.2.5	34.117.186.192
May 17, 2024 23:45:03.444129944 CEST	443	49705	34.117.186.192	192.168.2.5
May 17, 2024 23:45:03.670281887 CEST	443	49705	34.117.186.192	192.168.2.5
May 17, 2024 23:45:03.670437098 CEST	443	49705	34.117.186.192	192.168.2.5
May 17, 2024 23:45:03.670505047 CEST	49705	443	192.168.2.5	34.117.186.192
May 17, 2024 23:45:03.673120022 CEST	49705	443	192.168.2.5	34.117.186.192
May 17, 2024 23:45:03.673135042 CEST	443	49705	34.117.186.192	192.168.2.5
May 17, 2024 23:45:03.673151970 CEST	49705	443	192.168.2.5	34.117.186.192
May 17, 2024 23:45:03.673157930 CEST	443	49705	34.117.186.192	192.168.2.5
May 17, 2024 23:45:03.771847963 CEST	49706	443	192.168.2.5	172.67.75.166
May 17, 2024 23:45:03.771873951 CEST	443	49706	172.67.75.166	192.168.2.5
May 17, 2024 23:45:03.771949053 CEST	49706	443	192.168.2.5	172.67.75.166
May 17, 2024 23:45:03.772314072 CEST	49706	443	192.168.2.5	172.67.75.166
May 17, 2024 23:45:03.772325039 CEST	443	49706	172.67.75.166	192.168.2.5
May 17, 2024 23:45:04.619467020 CEST	443	49706	172.67.75.166	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 17, 2024 23:45:04.619560957 CEST	49706	443	192.168.2.5	172.67.75.166
May 17, 2024 23:45:04.622503042 CEST	49706	443	192.168.2.5	172.67.75.166
May 17, 2024 23:45:04.622514963 CEST	443	49706	172.67.75.166	192.168.2.5
May 17, 2024 23:45:04.622746944 CEST	443	49706	172.67.75.166	192.168.2.5
May 17, 2024 23:45:04.624036074 CEST	49706	443	192.168.2.5	172.67.75.166
May 17, 2024 23:45:04.664135933 CEST	443	49706	172.67.75.166	192.168.2.5
May 17, 2024 23:45:05.081523895 CEST	443	49706	172.67.75.166	192.168.2.5
May 17, 2024 23:45:05.081813097 CEST	443	49706	172.67.75.166	192.168.2.5
May 17, 2024 23:45:05.081913948 CEST	49706	443	192.168.2.5	172.67.75.166
May 17, 2024 23:45:05.087728977 CEST	49706	443	192.168.2.5	172.67.75.166
May 17, 2024 23:45:05.087744951 CEST	443	49706	172.67.75.166	192.168.2.5
May 17, 2024 23:45:05.087759018 CEST	49706	443	192.168.2.5	172.67.75.166
May 17, 2024 23:45:05.087764025 CEST	443	49706	172.67.75.166	192.168.2.5
May 17, 2024 23:45:05.093767881 CEST	49704	50500	192.168.2.5	5.42.96.65
May 17, 2024 23:45:05.177021027 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:05.461512089 CEST	49704	50500	192.168.2.5	5.42.96.65
May 17, 2024 23:45:05.466664076 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:05.517889977 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:05.570538998 CEST	49704	50500	192.168.2.5	5.42.96.65
May 17, 2024 23:45:05.649158001 CEST	49704	50500	192.168.2.5	5.42.96.65
May 17, 2024 23:45:05.656826019 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:05.834423065 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:05.883008003 CEST	49704	50500	192.168.2.5	5.42.96.65
May 17, 2024 23:45:06.044207096 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:06.086308002 CEST	49704	50500	192.168.2.5	5.42.96.65
May 17, 2024 23:45:06.086450100 CEST	49704	50500	192.168.2.5	5.42.96.65
May 17, 2024 23:45:06.096681118 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:06.450611115 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:06.452780008 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:06.452914953 CEST	49704	50500	192.168.2.5	5.42.96.65
May 17, 2024 23:45:06.457537889 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:06.462457895 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:06.462470055 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:06.462507963 CEST	49704	50500	192.168.2.5	5.42.96.65
May 17, 2024 23:45:06.508004904 CEST	49704	50500	192.168.2.5	5.42.96.65
May 17, 2024 23:45:06.604279041 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:06.633135080 CEST	49704	50500	192.168.2.5	5.42.96.65
May 17, 2024 23:45:06.638257980 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:07.002048969 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:07.054877043 CEST	49704	50500	192.168.2.5	5.42.96.65
May 17, 2024 23:45:07.070698023 CEST	49704	50500	192.168.2.5	5.42.96.65
May 17, 2024 23:45:07.112792015 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:07.485585928 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:07.539239883 CEST	49704	50500	192.168.2.5	5.42.96.65
May 17, 2024 23:45:11.537136078 CEST	49704	50500	192.168.2.5	5.42.96.65
May 17, 2024 23:45:11.542507887 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:11.544882059 CEST	49704	50500	192.168.2.5	5.42.96.65
May 17, 2024 23:45:11.549984932 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:11.550066948 CEST	49704	50500	192.168.2.5	5.42.96.65
May 17, 2024 23:45:11.554996967 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:11.555010080 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:11.555022001 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:11.555033922 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:11.555046082 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:11.555057049 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:11.555068016 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:11.555073977 CEST	49704	50500	192.168.2.5	5.42.96.65
May 17, 2024 23:45:11.555079937 CEST	50500	49704	5.42.96.65	192.168.2.5
May 17, 2024 23:45:11.555093050 CEST	50500	49704	5.42.96.65	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 17, 2024 23:45:02.493062973 CEST	60266	53	192.168.2.5	1.1.1.1
May 17, 2024 23:45:02.500276089 CEST	53	60266	1.1.1.1	192.168.2.5
May 17, 2024 23:45:03.675697088 CEST	60901	53	192.168.2.5	1.1.1.1
May 17, 2024 23:45:03.770749092 CEST	53	60901	1.1.1.1	192.168.2.5
May 17, 2024 23:45:17.505036116 CEST	55501	53	192.168.2.5	1.1.1.1
May 17, 2024 23:45:17.515978098 CEST	53	55501	1.1.1.1	192.168.2.5
May 17, 2024 23:45:31.140155077 CEST	63858	53	192.168.2.5	1.1.1.1
May 17, 2024 23:45:31.150041103 CEST	53	63858	1.1.1.1	192.168.2.5
May 17, 2024 23:45:32.140742064 CEST	53	52447	162.159.36.2	192.168.2.5
May 17, 2024 23:45:32.950365067 CEST	51773	53	192.168.2.5	1.1.1.1
May 17, 2024 23:45:32.998289108 CEST	53	51773	1.1.1.1	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 17, 2024 23:45:02.493062973 CEST	192.168.2.5	1.1.1.1	0xac3f	Standard query (0)	ipinfo.io	A (IP address)	IN (0x0001)	false
May 17, 2024 23:45:03.675697088 CEST	192.168.2.5	1.1.1.1	0xf651	Standard query (0)	db-ip.com	A (IP address)	IN (0x0001)	false
May 17, 2024 23:45:17.505036116 CEST	192.168.2.5	1.1.1.1	0x6fe6	Standard query (0)	kuljyftgjk.online	A (IP address)	IN (0x0001)	false
May 17, 2024 23:45:31.140155077 CEST	192.168.2.5	1.1.1.1	0x6f3b	Standard query (0)	kuljyftgjk.online	A (IP address)	IN (0x0001)	false
May 17, 2024 23:45:32.950365067 CEST	192.168.2.5	1.1.1.1	0xfa2	Standard query (0)	198.187.3.20.in-addr.arpa	PTR (Pointer record)	IN (0x0001)	false

DNS Answers

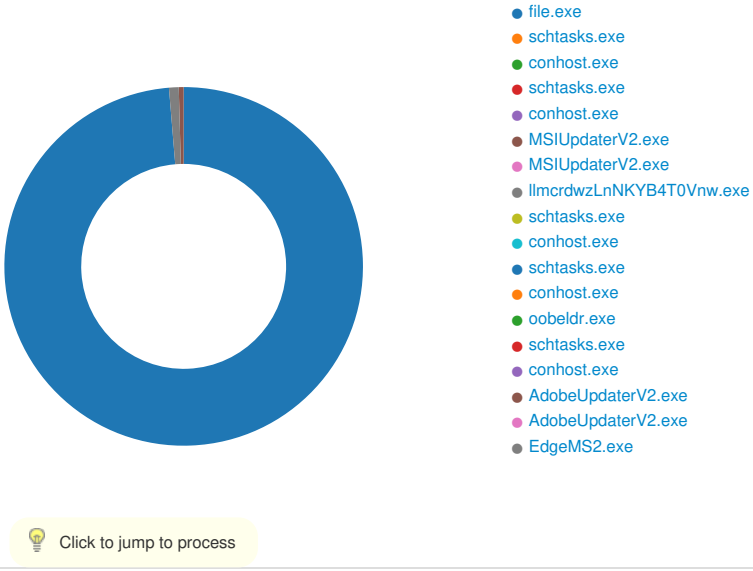
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
May 17, 2024 23:45:02.500276089 CEST	1.1.1.1	192.168.2.5	0xac3f	No error (0)	ipinfo.io		34.117.186.192	A (IP address)	IN (0x0001)	false
May 17, 2024 23:45:03.770749092 CEST	1.1.1.1	192.168.2.5	0xf651	No error (0)	db-ip.com		172.67.75.166	A (IP address)	IN (0x0001)	false
May 17, 2024 23:45:03.770749092 CEST	1.1.1.1	192.168.2.5	0xf651	No error (0)	db-ip.com		104.26.5.15	A (IP address)	IN (0x0001)	false
May 17, 2024 23:45:03.770749092 CEST	1.1.1.1	192.168.2.5	0xf651	No error (0)	db-ip.com		104.26.4.15	A (IP address)	IN (0x0001)	false
May 17, 2024 23:45:17.515978098 CEST	1.1.1.1	192.168.2.5	0x6fe6	Name error (3)	kuljyftgjk.online	none	none	A (IP address)	IN (0x0001)	false
May 17, 2024 23:45:31.150041103 CEST	1.1.1.1	192.168.2.5	0x6f3b	Name error (3)	kuljyftgjk.online	none	none	A (IP address)	IN (0x0001)	false
May 17, 2024 23:45:32.998289108 CEST	1.1.1.1	192.168.2.5	0xfa2	Name error (3)	198.187.3.20.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)	false

HTTP Request Dependency Graph

- https:
  - ipinfo.io
- db-ip.com
- 5.42.96.170

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: **4112**, Parent PID: **1028**

General

Target ID:	0
Start time:	17:44:54
Start date:	17/05/2024
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\file.exe"
Imagebase:	0x1b0000
File size:	8'778'752 bytes
MD5 hash:	3D09739846543F4962F2B432DA671C29
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: 00000000.00000002.4445088347.0000000006449000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_RiseProStealer, Description: Yara detected RisePro Stealer, Source: 00000000.00000003.2157362439.00000000061CB000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low
Has exited:	false

File Activities

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	AdobeUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26	unicode	C:\Users\user\AppData\Local\AdobeUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26\AdobeUpdaterV2.exe	success or wait	1	23C5F8	RegSetValueExA

Analysis Process: schtasks.exe PID: **3692**, Parent PID: **4112**

General	
Target ID:	3
Start time:	17:45:15
Start date:	17/05/2024
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /create /f /RU "user" /tr "C:\ProgramData\MSIUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26\MSIUpdaterV2.exe" /tn "MSIUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26 HR" /sc HOURLY /rl HIGHEST
Imagebase:	0x7ff6d64d0000
File size:	187'904 bytes
MD5 hash:	48C2FE20575769DE916F48EF0676A965
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

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: 5068, Parent PID: 3692

General	
Target ID:	4
Start time:	17:45:15
Start date:	17/05/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6d64d0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: schtasks.exe PID: 6668, Parent PID: 4112

General	
Target ID:	5
Start time:	17:45:15
Start date:	17/05/2024
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /create /f /RU "user" /tr "C:\ProgramData\MSIUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26\MSIUpdaterV2.exe" /tn "MSIUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26 LG" /sc ONLOGON /rl HIGHEST
Imagebase:	0x1c0000
File size:	187'904 bytes
MD5 hash:	48C2FE20575769DE916F48EF0676A965
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Has exited:	true

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: 4500, Parent PID: 6668

General

Target ID:	6
Start time:	17:45:15
Start date:	17/05/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6d64d0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: MSIUpdaterV2.exe PID: 6504, Parent PID: 1068

General

Target ID:	7
Start time:	17:45:15
Start date:	17/05/2024
Path:	C:\ProgramData\MSIUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26\MSIUpdaterV2.exe
Wow64 process (32bit):	true
Commandline:	C:\ProgramData\MSIUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26\MSIUpdaterV2.exe
Imagebase:	0x400000
File size:	4'563'640 bytes
MD5 hash:	AF6E384DFABDAD52D43CF8429AD8779C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Clipbanker_f9f9e79d, Description: unknown, Source: 00000007.00000002.2220685526.0000000000401000.00000020.00000001.01000000.00000006.sdmp, Author: unknown • Rule: Windows_Trojan_Clipbanker_787b130b, Description: unknown, Source: 00000007.00000002.2220685526.0000000000401000.00000020.00000001.01000000.00000006.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 83%, ReversingLabs
Reputation:	moderate
Has exited:	true

File Activities

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Protect\oobeldr.exe	0	524288	4d 5a 40 00 01 00 00 00 02 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 57 69 6e 33 32 20 2e 45 58 45 2e 0d 0a 24 40 00 00 00 50 45 00 00 4c 01 03 00 fd 4d fd 61 00 00 00 00 00 00 00 00 fd 00 02 03 0b 01 0e 1d 00 18 00 00 00 5e 19 00 00 00 00 00 00 77 00 00 10 00 00 00 30 00 00 00 00 40 00 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 7d 00 00 02 00 00 6d 1a 46 00 02 00 00 fd 00 00 10 00 00 fd 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 fd 77 00 fd 00 00 00 00 fd 77 00 7c fd 05 00 00 00 00 00 00 00 00 00 00 fd 45 00 fd 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!Win32 .EXE.$@PELMa^w0@}m Fww|E	success or wait	9	401325	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: MSIUpdaterV2.exe PID: **1628**, Parent PID: **1068**

General

Target ID:	8
Start time:	17:45:16
Start date:	17/05/2024
Path:	C:\ProgramData\MSIUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26\MSIUpdaterV2.exe
Wow64 process (32bit):	true
Commandline:	C:\ProgramData\MSIUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26\MSIUpdaterV2.exe
Imagebase:	0x400000
File size:	4'563'640 bytes
MD5 hash:	AF6E384DFABDAD52D43CF8429AD8779C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Clipbanker_f9f9e79d, Description: unknown, Source: 00000008.00000002.2218340799.0000000000401000.00000020.00000001.01000000.00000006.sdmp, Author: unknown • Rule: Windows_Trojan_Clipbanker_787b130b, Description: unknown, Source: 00000008.00000002.2218340799.0000000000401000.00000020.00000001.01000000.00000006.sdmp, Author: unknown
Reputation:	moderate
Has exited:	true

Analysis Process: llmcrdwzLnNKYB4T0Vnw.exe PID: **7056**, Parent PID: **4112**

General

Target ID:	9
Start time:	17:45:16
Start date:	17/05/2024
Path:	C:\Users\user\AppData\Local\Temp\span1UB98D2D2zeo\llmcrdwzLnNKYB4T0Vnw.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\span1UB98D2D2zeo\llmcrdwzLnNKYB4T0Vnw.exe"
Imagebase:	0x400000
File size:	4'563'640 bytes

MD5 hash:	AF6E384DFABDAD52D43CF8429AD8779C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Clipbanker_f9f9e79d, Description: unknown, Source: 00000009.00000002.2211800433.0000000000401000.00000020.00000001.01000000.00000008.sdmp, Author: unknown • Rule: Windows_Trojan_Clipbanker_787b130b, Description: unknown, Source: 00000009.00000002.2211800433.0000000000401000.00000020.00000001.01000000.00000008.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 83%, ReversingLabs
Reputation:	moderate
Has exited:	true

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Protect\oobeldr.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	401325	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Protect\oobeldr.exe	0	524288	4d 5a 40 00 01 00 00 00 02 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 0a 00 00 00 00 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 57 69 6e 33 32 20 2e 45 58 45 2e 0d 0a 24 40 00 00 00 50 45 00 00 4c 01 03 00 fd 4d fd 61 00 00 00 00 00 00 00 00 fd 00 02 03 0b 01 0e 1d 00 18 00 00 00 5e 19 00 00 00 00 00 00 77 00 00 10 00 00 00 30 00 00 00 00 40 00 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 fd 7d 00 00 02 00 00 6d 1a 46 00 02 00 00 fd 00 00 10 00 00 fd 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 fd 77 00 fd 00 00 00 00 fd 77 00 7c fd 05 00 00 00 00 00 00 00 00 00 00 fd 45 00 fd 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!Win32 .EXE.$@PELMa^w0@}m Fww|E	success or wait	9	401325	CopyFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: schtasks.exe PID: **5728**, Parent PID: **7056**

General

Target ID:	10
Start time:	17:45:16
Start date:	17/05/2024
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	/C /create /F /sc minute /mo 1 /tn "Telemetry Logging" /tr "C:\Users\user\AppData\Roaming\Microsoft\Protect\oobeldr.exe"

Imagebase:	0x1c0000
File size:	187'904 bytes
MD5 hash:	48C2FE20575769DE916F48EF0676A965
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

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: **4748**, Parent PID: **5728**

General

Target ID:	11
Start time:	17:45:16
Start date:	17/05/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6d64d0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: schtasks.exe PID: **6968**, Parent PID: **6504**

General

Target ID:	12
Start time:	17:45:17
Start date:	17/05/2024
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	/C /create /F /sc minute /mo 1 /tn "Telemetry Logging" /tr "C:\Users\user\AppData\Roaming\Microsoft\Protect\oobeldr.exe"
Imagebase:	0x1c0000
File size:	187'904 bytes
MD5 hash:	48C2FE20575769DE916F48EF0676A965
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

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: **6756**, Parent PID: **6968**

General	
Target ID:	13
Start time:	17:45:17
Start date:	17/05/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6d64d0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high
Has exited:	true

Analysis Process: oobeldr.exe PID: **7044**, Parent PID: **1068**

General	
Target ID:	14
Start time:	17:45:18
Start date:	17/05/2024
Path:	C:\Users\user\AppData\Roaming\Microsoft\Protect\oobeldr.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Protect\oobeldr.exe
Imagebase:	0x400000
File size:	4'563'640 bytes
MD5 hash:	AF6E384DFABDAD52D43CF8429AD8779C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Clipbanker_f9f9e79d, Description: unknown, Source: 0000000E.00000002.4441908172.0000000000401000.00000020.00000001.01000000.0000000A.sdmp, Author: unknown • Rule: Windows_Trojan_Clipbanker_787b130b, Description: unknown, Source: 0000000E.00000002.4441908172.0000000000401000.00000020.00000001.01000000.0000000A.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 83%, ReversingLabs
Reputation:	moderate
Has exited:	false

Analysis Process: schtasks.exe PID: **2504**, Parent PID: **7044**

General	
Target ID:	15
Start time:	17:45:18
Start date:	17/05/2024
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	/C /create /F /sc minute /mo 1 /tn "Telemetry Logging" /tr "C:\Users\user\AppData\Roaming\Microsoft\Protect\oobeldr.exe"
Imagebase:	0x1c0000
File size:	187'904 bytes
MD5 hash:	48C2FE20575769DE916F48EF0676A965
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

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: **4320**, Parent PID: **2504**

General

Target ID:	16
Start time:	17:45:19
Start date:	17/05/2024
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6d64d0000
File size:	862'208 bytes
MD5 hash:	0D698AF330FD17BEE3BF90011D49251D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Has exited:	true

Analysis Process: AdobeUpdaterV2.exe PID: **6436**, Parent PID: **1028**

General

Target ID:	17
Start time:	17:45:24
Start date:	17/05/2024
Path:	C:\Users\user\AppData\Local\AdobeUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26\AdobeUpdaterV2.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\AdobeUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26\AdobeUpdaterV2.exe"
Imagebase:	0x400000
File size:	4'563'640 bytes
MD5 hash:	AF6E384DFABDAD52D43CF8429AD8779C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Clipbanker_f9f9e79d, Description: unknown, Source: 00000011.00000002.2298062400.0000000000401000.00000020.00000001.01000000.0000000B.sdmp, Author: unknown • Rule: Windows_Trojan_Clipbanker_787b130b, Description: unknown, Source: 00000011.00000002.2298062400.0000000000401000.00000020.00000001.01000000.0000000B.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 83%, ReversingLabs
Has exited:	true

Analysis Process: AdobeUpdaterV2.exe PID: **4332**, Parent PID: **1028**

General

Target ID:	18
Start time:	17:45:33
Start date:	17/05/2024
Path:	C:\Users\user\AppData\Local\AdobeUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26\AdobeUpdaterV2.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\AdobeUpdaterV2_45c48cce2e2d7fbdea1afc51c7c6ad26\AdobeUpdaterV2.exe"
Imagebase:	0x400000
File size:	4'563'640 bytes
MD5 hash:	AF6E384DFABDAD52D43CF8429AD8779C

Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Clipbanker_f9f9e79d, Description: unknown, Source: 00000012.00000002.2379291934.0000000000401000.00000020.00000001.01000000.0000000B.sdmp, Author: unknown • Rule: Windows_Trojan_Clipbanker_787b130b, Description: unknown, Source: 00000012.00000002.2379291934.0000000000401000.00000020.00000001.01000000.0000000B.sdmp, Author: unknown
Has exited:	true

Analysis Process: EdgeMS2.exe PID: **2860**, Parent PID: **1028**

General

Target ID:	19
Start time:	17:45:41
Start date:	17/05/2024
Path:	C:\Users\user\AppData\Local\Temp\EdgeMS2_45c48cce2e2d7fbdea1afc51c7c6ad26\EdgeMS2.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\EdgeMS2_45c48cce2e2d7fbdea1afc51c7c6ad26\EdgeMS2.exe"
Imagebase:	0x400000
File size:	4'563'640 bytes
MD5 hash:	AF6E384DFABDAD52D43CF8429AD8779C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Clipbanker_f9f9e79d, Description: unknown, Source: 00000013.00000002.2460266314.0000000000401000.00000020.00000001.01000000.0000000C.sdmp, Author: unknown • Rule: Windows_Trojan_Clipbanker_787b130b, Description: unknown, Source: 00000013.00000002.2460266314.0000000000401000.00000020.00000001.01000000.0000000C.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 83%, ReversingLabs
Has exited:	true

Disassembly

No disassembly