ID: 830750
Sample Name:
SecuriteInfo.com.Trojan.Garf.Gen.6.31593.18898.exe
Cookbook: default.jbs
Time: 16:58:12
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

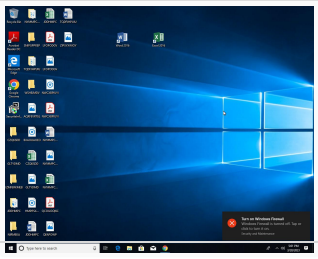
Windows Analysis Report

SecuriteInfo.com.Trojan.Garf.Gen.6.31593.18898.exe

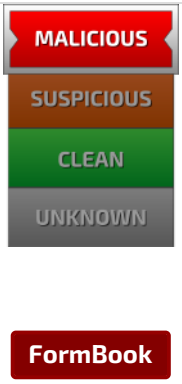
Overview

General Information

Sample Name:	SecuriteInfo.com.Trojan.Garf.Gen.6.31593.18898.exe
Analysis ID:	830750
MD5:	c7714b273571…
SHA1:	c24d9460bee8…
SHA256:	e62c1e809c48…
Tags:	exe Formbook
Infos:	



Detection



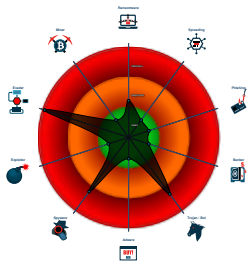
FormBook

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- System process connects to networ…
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Sample uses process hollowing tech…
- Tries to steal Mail credentials (via fi…
- Maps a DLL or memory area into an…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Trojan.Garf.Gen.6.31593.18898.exe (PID: 5020 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Garf.Gen.6.31593.18898.exe MD5: C7714B273571BA64C0B77AFCA236AC6D)
  - vfpbkeeo.exe (PID: 1316 cmdline: "C:\Users\user\AppData\Local\Temp\vfpbkeeo.exe" C:\Users\user\AppData\Local\Temp\bzuxwizqdxf.m MD5: 6D30D26416D626447BA4298A59111F6D)
    - conhost.exe (PID: 1240 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - vfpbkeeo.exe (PID: 1948 cmdline: C:\Users\user\AppData\Local\Temp\vfpbkeeo.exe MD5: 6D30D26416D626447BA4298A59111F6D)
      - explorer.exe (PID: 3528 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - cmd.exe (PID: 916 cmdline: C:\Windows\SysWOW64\cmd.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Formbook, Formbo	FormBook contains a unique crypter RunPE that has unique behavioral patterns subject to detection. It was initially called "Babushka Crypter" by Insidemalware.	• SWEED • Cobalt	http://blog.inquest.net/blog/2018/06/22/a-look-at-formbook-stealer/http://cambuz.blogspot.de/2016/06/form-grabber-2016-cromeffoperathunderbi.htmlhttp://www.vkremez.com/2018/01/lets-learn-dissecting-formbook.htmlhttps://asec.ahnlab.com/en/32149/https://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.formbook

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.567150912.0000000000D10000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000005.00000002.567150912.0000000000D10000.00000040.10000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x1f0e0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xae4f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x182f7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000005.00000002.567150912.0000000000D10000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x180f5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x17b91:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x181f7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1836f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xaa1a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x16ddc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1de87:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ee3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000002.352371790.00000000008C0000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000003.00000002.352371790.00000000008C0000.00000040.10000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x1f0e0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xae4f:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x182f7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83

Click to see the 13 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.vfpbkeeo.exe.400000.0.unpack	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
3.2.vfpbkeeo.exe.400000.0.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x20103:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xbe72:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x1931a:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
3.2.vfpbkeeo.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x19118:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x18bb4:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1921a:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x19392:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xba3d:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x17dff:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1eeaa:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1fe5d:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.vfpbkeeo.exe.400000.0.raw.unpack	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
3.2.vfpbkeeo.exe.400000.0.raw.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x20f03:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xcc72:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x1a11a:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83

Click to see the 1 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 91.195.240.94	
Timestamp:	192.168.2.491.195.240.9449702802031449 03/20/23-17:00:09.343542
SID:	2031449
Source Port:	49702
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 81.17.18.198	
Timestamp:	192.168.2.481.17.18.19849706802031412 03/20/23-17:00:25.955923
SID:	2031412
Source Port:	49706
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 81.17.18.198	
Timestamp:	192.168.2.481.17.18.19849706802031453 03/20/23-17:00:25.955923
SID:	2031453
Source Port:	49706
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 94.176.104.86	
Timestamp:	192.168.2.494.176.104.8649696802031453 03/20/23-16:59:46.201874
SID:	2031453
Source Port:	49696
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 91.195.240.94	
Timestamp:	192.168.2.491.195.240.9449702802031453 03/20/23-17:00:09.343542
SID:	2031453
Source Port:	49702
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 94.176.104.86	
Timestamp:	192.168.2.494.176.104.8649696802031412 03/20/23-16:59:46.201874
SID:	2031412
Source Port:	49696
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 91.195.240.94	
Timestamp:	192.168.2.491.195.240.9449702802031412 03/20/23-17:00:09.343542
SID:	2031412
Source Port:	49702
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 94.176.104.86	
Timestamp:	192.168.2.494.176.104.8649696802031449 03/20/23-16:59:46.201874
SID:	2031449
Source Port:	49696
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.4 - Destination IP: 81.17.18.198	
Timestamp:	192.168.2.481.17.18.19849706802031449 03/20/23-17:00:25.955923
SID:	2031449
Source Port:	49706
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

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

Snort IDS alert for network traffic

Performs DNS queries to domains with low reputation

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (changes PE section rights)

Malware Analysis System Evasion

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

HIPS / PFW / Operating System Protection Evasion

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information

Yara detected FormBook

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

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

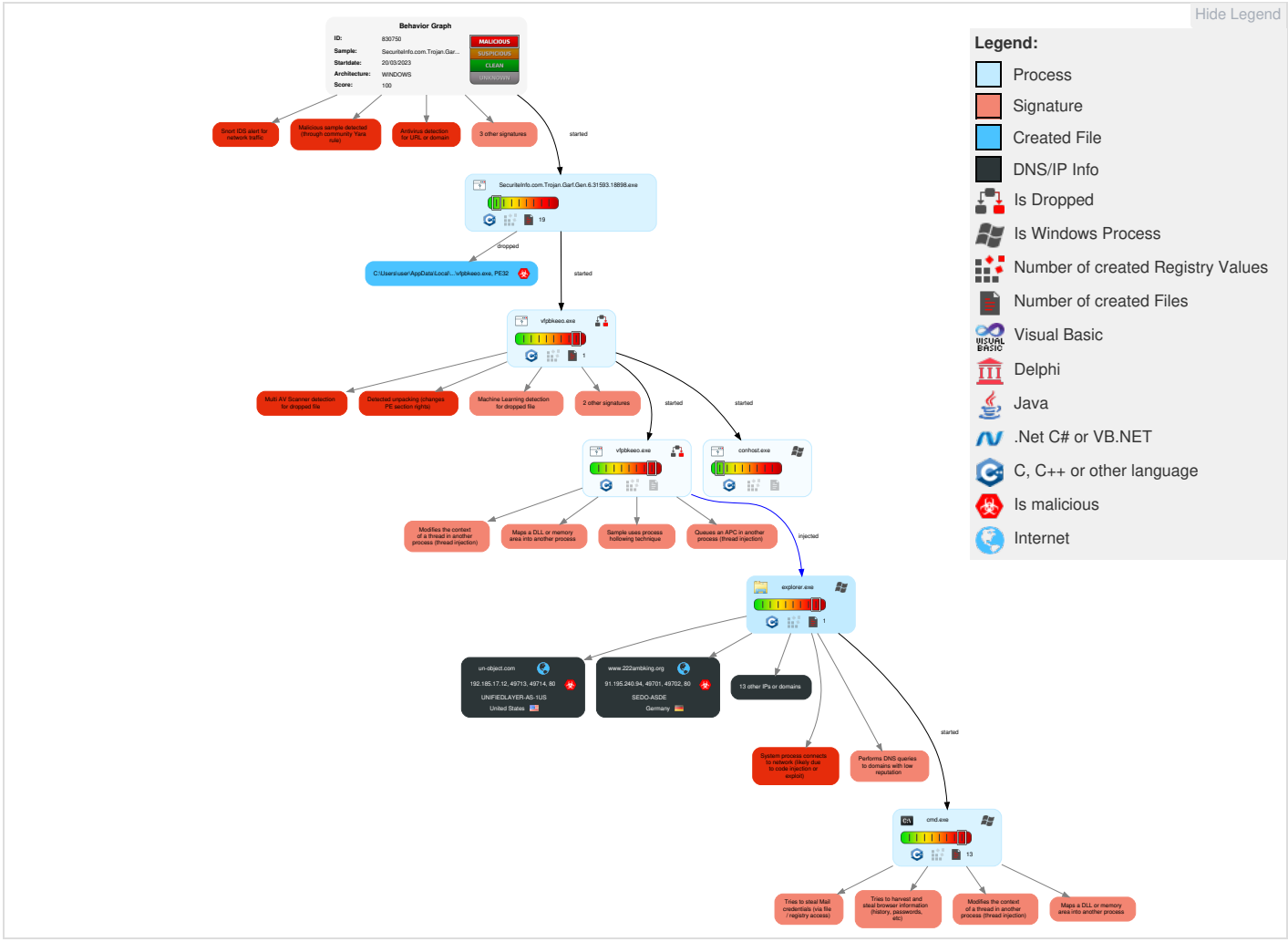
Remote Access Functionality

Yara detected FormBook

Mitre Att&ck Matrix

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

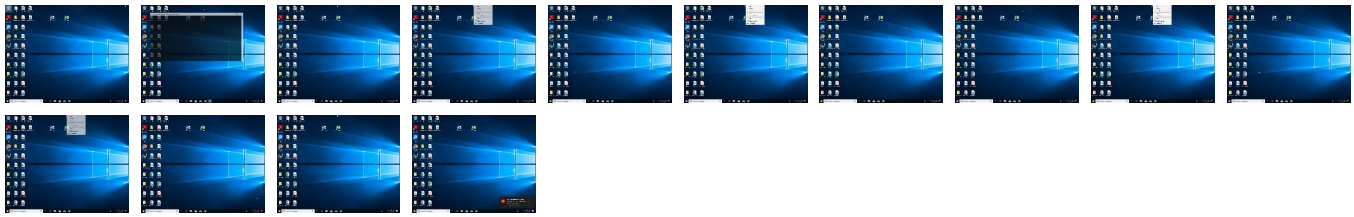
Behavior Graph



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
SecuriteInfo.com.Trojan.Garf.Gen.6.31593.18898.exe	42%	ReversingLabs	Win32.Trojan.FormBook	
SecuriteInfo.com.Trojan.Garf.Gen.6.31593.18898.exe	42%	Virustotal		Browse
SecuriteInfo.com.Trojan.Garf.Gen.6.31593.18898.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\vfpbkeeo.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\vfpbkeeo.exe	39%	ReversingLabs	Win32.Trojan.Lazy	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.vfpbkeeo.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.vfpbkeeo.exe.2080000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.bitservicesltd.com	2%	Virustotal		Browse
www.younrock.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.energyservicestation.com/u2kb/?pJ=y0bMVGhK3R&s7=IK59b/MdFRha+CUVMWpzDpHQ2riuD6F66TLC1fPPNwLnZq29gpb12AWvlZbo17UEh0sBgFvevrMQsuZfYKuNRicmmGgsJT37Uw==	100%	Avira URL Cloud	malware	
http://www.thedivinerudraksha.com/u2kb/	1%	Virustotal		Browse
http://www.avisrezervee.com/u2kb/www.avisrezervee.com	100%	Avira URL Cloud	malware	
http://www.mygloballojistik.online	0%	Avira URL Cloud	safe	
http://www.thedivinerudraksha.com/u2kb/	100%	Avira URL Cloud	malware	
http://www.gritslab.com/u2kb/www.gritslab.com	100%	Avira URL Cloud	malware	
http://www.thewildphotographer.co.uk/u2kb/www.thewildphotographer.co.uk	100%	Avira URL Cloud	malware	
http://www.germanreps.com	0%	Avira URL Cloud	safe	
http://www.shapshit.xyz	0%	Avira URL Cloud	safe	
http://www.ecomofietsen.com	0%	Avira URL Cloud	safe	
http://www.white-hat.uk/u2kb/www.white-hat.uk	100%	Avira URL Cloud	malware	
http://www.thedivinerudraksha.com	0%	Avira URL Cloud	safe	
http://thedivinerudraksha.com/u2kb/?pJ=y0bMVGhK3R&s7=im5SXjRwbJIZeY2yeMVWNNnKg99Etck2UhYi2fNZ2Kf/X7l	100%	Avira URL Cloud	malware	
http://www.bitservicesltd.com/u2kb/?pJ=y0bMVGhK3R&s7=rr+sOBvEXsBdGevUkZEAvniGWrNxzC1YNHmXivr92FQhRIIYsedRhL+YGaN2VCieGtjtLTUTzUqxDX3Wf7Wl2JIBHu0WW9vDmQ==	100%	Avira URL Cloud	malware	
http://www.thedivinerudraksha.com/u2kb/?pJ=y0bMVGhK3R&s7=im5SXjRwbJIZeY2yeMVWNNnKg99Etck2UhYi2fNZ2Kf/X7lq2SPR1Q6pROq8Gck3yLtOH/fXnE++yuD9U7pi0el0K5lBX7KNLg==	100%	Avira URL Cloud	malware	
http://www.energyservicestation.com/u2kb/www.energyservicestation.com	100%	Avira URL Cloud	malware	
http://www.un-object.com/u2kb/	100%	Avira URL Cloud	malware	
http://www.energyservicestation.com/u2kb/	100%	Avira URL Cloud	malware	
http://www.white-hat.uk	0%	Avira URL Cloud	safe	
http://www.dzyngiri.com	0%	Avira URL Cloud	safe	
http://www.employerseervices.com/u2kb/www.employerseervices.com	0%	Avira URL Cloud	safe	
http://www.younrock.com/u2kb/?s7=05tPwqSdqXO2xf32BHQi8E1nUfoFa2c80hhB3sQ3FFDNPs5AZDU6EjUymll22Wm6Scj5xbzg3GdXyuHgSKq8rTPQW1vWIa2Wug==&pJ=y0bMVGhK3R	100%	Avira URL Cloud	malware	
http://www.avisrezervee.com	0%	Avira URL Cloud	safe	
http://www.mygloballojistik.online/u2kb/	0%	Avira URL Cloud	safe	
http://www.bitservicesltd.com	0%	Avira URL Cloud	safe	
http://justinmezzell.com	0%	Avira URL Cloud	safe	
http://www.thewildphotographer.co.uk/u2kb/	100%	Avira URL Cloud	malware	
http://www.gritslab.com	0%	Avira URL Cloud	safe	
http://www.white-hat.uk/u2kb/	100%	Avira URL Cloud	malware	
http://https://alldomains.hosting/domain-registrieren.html	0%	Avira URL Cloud	safe	
http://www.bitservicesltd.com/u2kb/	100%	Avira URL Cloud	malware	
http://www.thewildphotographer.co.uk	0%	Avira URL Cloud	safe	
http://www.fclaimrewardccpointq.shop/u2kb/www.fclaimrewardccpointq.shop	100%	Avira URL Cloud	malware	
http://www.222ambking.org/u2kb/www.222ambking.org	100%	Avira URL Cloud	malware	
http://www.gritslab.com/u2kb/	100%	Avira URL Cloud	malware	
http://www.employerseervices.com/u2kb/	0%	Avira URL Cloud	safe	
http://www.fclaimrewardccpointq.shop/u2kb/	100%	Avira URL Cloud	malware	
http://www.energyservicestation.com	0%	Avira URL Cloud	safe	
http://www.gritslab.com/u2kb/?s7=ydCzFiH7iMWnz6xHMre3lWaEcfnK5+fYQUsmgPEoYCSsyD6HgT3yZXCBsea1O+OKnOGwPNRrrKn2ANadQmZjx8zjtO3/lmb0Gg==&pJ=y0bMVGhK3R	100%	Avira URL Cloud	malware	
http://www.younrock.com	0%	Avira URL Cloud	safe	
http://https://alldomains.hosting/e-mail-server.html	0%	Avira URL Cloud	safe	
http://www.younrock.com/u2kb/?ch=1&js=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhdWQiOiJKb2tlbiIsImV4c	100%	Avira URL Cloud	malware	
http://www.shapshit.xyz/u2kb/?s7=Yd5Rzn4EVOpL1Cl/e5Amzdaa+E7UlYBpl8BtE0ZhlgLGbR5cH1Fns9iDSFPM0EqDoX1il4mP+EMsdt2zebBtiTAOJDfFAse6Fg==&pJ=y0bMVGhK3R	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://www.un-object.com/u2kb/?pJ=y0bMVGhK3R&s7=pRDkJdNDOVoQCU+9NHQShuJ8RIIM2fjCZpxzdvjpnmqfDHzh6n+FGyromdVZx0/+Z3ctR0ZwX+ep4hJ0NBR+2QmcJmTx4hb/kQ==	100%	Avira URL Cloud	malware	
http://www.un-object.com/u2kb/www.un-object.com	100%	Avira URL Cloud	malware	
http://white-hat.uk/u2kb/?pJ=y0bMVGhK3R&s7=PXfMycAZpTAipct8YsIgv6PR3Y11yPgF2k7967nf/qU1A0mUqq9Jy2mfr	100%	Avira URL Cloud	malware	
http://www.thedivinerudraksha.com/u2kb/www.thedivinerudraksha.com	100%	Avira URL Cloud	malware	
http://www.fclaimrewardccpointq.shop	100%	Avira URL Cloud	malware	
http://www.white-hat.uk/u2kb/?pJ=y0bMVGhK3R&s7=PXfMycAZpTAipct8YsIgv6PR3Y11yPgF2k7967nf/qU1A0mUqq9Jy2mfr4kURdfD0IyZUuXLnrTzZCke5/3tklxZoaLCmex8cw==	100%	Avira URL Cloud	malware	
http://www.shapshit.xyz/u2kb/	100%	Avira URL Cloud	malware	
http://www.mygloballojistik.online/u2kb/www.mygloballojistik.online	0%	Avira URL Cloud	safe	
http://https://alldomains.hosting/	0%	Avira URL Cloud	safe	
http://www.ecomofietsen.com/u2kb/	100%	Avira URL Cloud	malware	
http://www.avisrezervee.com/u2kb/	100%	Avira URL Cloud	malware	
http://https://alldomains.hosting/hosting-webhosting.html	0%	Avira URL Cloud	safe	
http://www.germanreps.com/u2kb/www.germanreps.com	100%	Avira URL Cloud	malware	
http://www.younrock.com/u2kb/www.younrock.com	100%	Avira URL Cloud	malware	
http://www.222ambking.org/u2kb/?s7=IEUpLmGg2fqLmrhwDd0CH8vm0i8ubOQDFcodV2ACJcW4bHSQscR3aN4MRDv2q1O0g2vnwuasF99orDvyVUesQZcBXW4MNplrrg==&pJ=y0bMVGhK3R	100%	Avira URL Cloud	malware	
http://www.222ambking.org	0%	Avira URL Cloud	safe	
http://www.germanreps.com/u2kb/	100%	Avira URL Cloud	malware	
http://www.222ambking.org/u2kb/	100%	Avira URL Cloud	malware	
http://www.employerseervices.com	0%	Avira URL Cloud	safe	
http://www.shapshit.xyz/u2kb/www.shapshit.xyz	100%	Avira URL Cloud	malware	
http://www.un-object.com	0%	Avira URL Cloud	safe	
http://www.younrock.com/u2kb/	100%	Avira URL Cloud	malware	
http://www.ecomofietsen.com/u2kb/www.ecomofietsen.com	100%	Avira URL Cloud	malware	
http://www.bitservicesltd.com/u2kb/www.bitservicesltd.com	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.bitservicesltd.com	161.97.163.8	true	true	• 2%, Virustotal, Browse	unknown
www.younrock.com	81.17.18.198	true	true	• 1%, Virustotal, Browse	unknown
www.energyservicestation.com	213.145.228.111	true	true		unknown
www.thewildphotographer.co.uk	45.33.30.197	true	true		unknown
www.shapshit.xyz	199.192.30.147	true	true		unknown
www.222ambking.org	91.195.240.94	true	true		unknown
thedivinerudraksha.com	85.187.128.34	true	true		unknown
un-object.com	192.185.17.12	true	true		unknown
white-hat.uk	94.176.104.86	true	true		unknown
gritslab.com	78.141.192.145	true	true		unknown
www.un-object.com	unknown	unknown	true		unknown
www.white-hat.uk	unknown	unknown	true		unknown
www.gritslab.com	unknown	unknown	true		unknown
www.thedivinerudraksha.com	unknown	unknown	true		unknown
www.fclaimrewardccpointq.shop	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.energyservicestation.com/u2kb/?pJ=y0bMVGhK3R&s7=IK59b/MdFRha+CUVMWpzDpHQ2riuD6F66TLC1fPPNwLnZq29gpb12AWvlZbo17UEh0sBgFvevrMQsuZfYKuNRicmmGgsJT37Uw==	true	• Avira URL Cloud: malware	unknown
http://www.thedivinerudraksha.com/u2kb/	true	• 1%, Virustotal, Browse • Avira URL Cloud: malware	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.bitservicesltd.com/u2kb/?pJ=y0bMVGhK3R&s7=rr+sOBvEXsBdGevUkZEAvniGWrNxzC1YNHmXivr92FQhRIIYsedRhL+YGaN2VCieGtjtLTUTzUqxDX3Wf7Wl2JIBHu0WW9vDmQ==	true	• Avira URL Cloud: malware	unknown
http://www.thedivinerudraksha.com/u2kb/?pJ=y0bMVGhK3R&s7=im5SXjRwbJIZeY2yeMVWNNnKg99Etck2UhYi2fNZ2Kf/X7lq2SPR1Q6pROq8Gck3yLtOH/fXnE++yuD9U7pi0eI0K5lBX7KNLg==	true	• Avira URL Cloud: malware	unknown
http://www.energyservicestation.com/u2kb/	true	• Avira URL Cloud: malware	unknown
http://www.un-object.com/u2kb/	true	• Avira URL Cloud: malware	unknown
http://www.younrock.com/u2kb/?s7=05tPwqSdqXO2xf32BHQi8E1nUfoFa2c80hhB3sQ3FFDNPs5AZDU6EjUymlI22Wm6Scj5xbzg3GdXyuHgSKq8rTPQW1vWIa2Wug==&pJ=y0bMVGhK3R	true	• Avira URL Cloud: malware	unknown
http://www.thewildphotographer.co.uk/u2kb/	true	• Avira URL Cloud: malware	unknown
http://www.bitservicesltd.com/u2kb/	true	• Avira URL Cloud: malware	unknown
http://www.gritslab.com/u2kb/	true	• Avira URL Cloud: malware	unknown
http://www.gritslab.com/u2kb/?s7=ydCzFiH7iMWnz6xHMre3IWaEcfnK5+fYQUsmgPEoYCSsyD6HgT3yZXCBsea1O+OKnOGwPNRrrKn2ANadQmZjx8zjtO3/lmb0Gg==&pJ=y0bMVGhK3R	true	• Avira URL Cloud: malware	unknown
http://www.un-object.com/u2kb/?pJ=y0bMVGhK3R&s7=pRDkJdNDOVoQCU+9NHQShuJ8RlIM2fjCZpxzdvjpnmqfDHzh6n+FGyromdVZx0/+Z3ctR0ZwX+ep4hJ0NBR+2QmcJmTx4hb/kQ==	true	• Avira URL Cloud: malware	unknown
http://www.shapshit.xyz/u2kb/?s7=Yd5Rzn4EVOpL1Cl/e5Amzdaa+E7UlYBpl8BtE0ZhlgLGbR5cH1Fns9iDSFPM0EqDoX1il4mP+EMsdt2zebBtiTAOJDfFAse6Fg==&pJ=y0bMVGhK3R	true	• Avira URL Cloud: malware	unknown
http://www.white-hat.uk/u2kb/?pJ=y0bMVGhK3R&s7=PXfMycAZpTAipct8Yslgv6PR3Y11yPgF2k7967nf/qU1A0mUqq9Jy2mfr4kURdfD0IyZUuXLnrTzZCke5/3tklxZoaLCmex8cw==	true	• Avira URL Cloud: malware	unknown
http://www.shapshit.xyz/u2kb/	true	• Avira URL Cloud: malware	unknown
http://www.222ambking.org/u2kb/?s7=IEUpLmGg2fqLmrhwDd0CH8vm0i8ubOQDFcodV2ACJcW4bHSQscR3aN4MRDv2q1O0g2vnwuasF99orDvyVUesQZcBXW4MNpIrrg==&pJ=y0bMVGhK3R	true	• Avira URL Cloud: malware	unknown
http://www.222ambking.org/u2kb/	true	• Avira URL Cloud: malware	unknown
http://www.younrock.com/u2kb/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

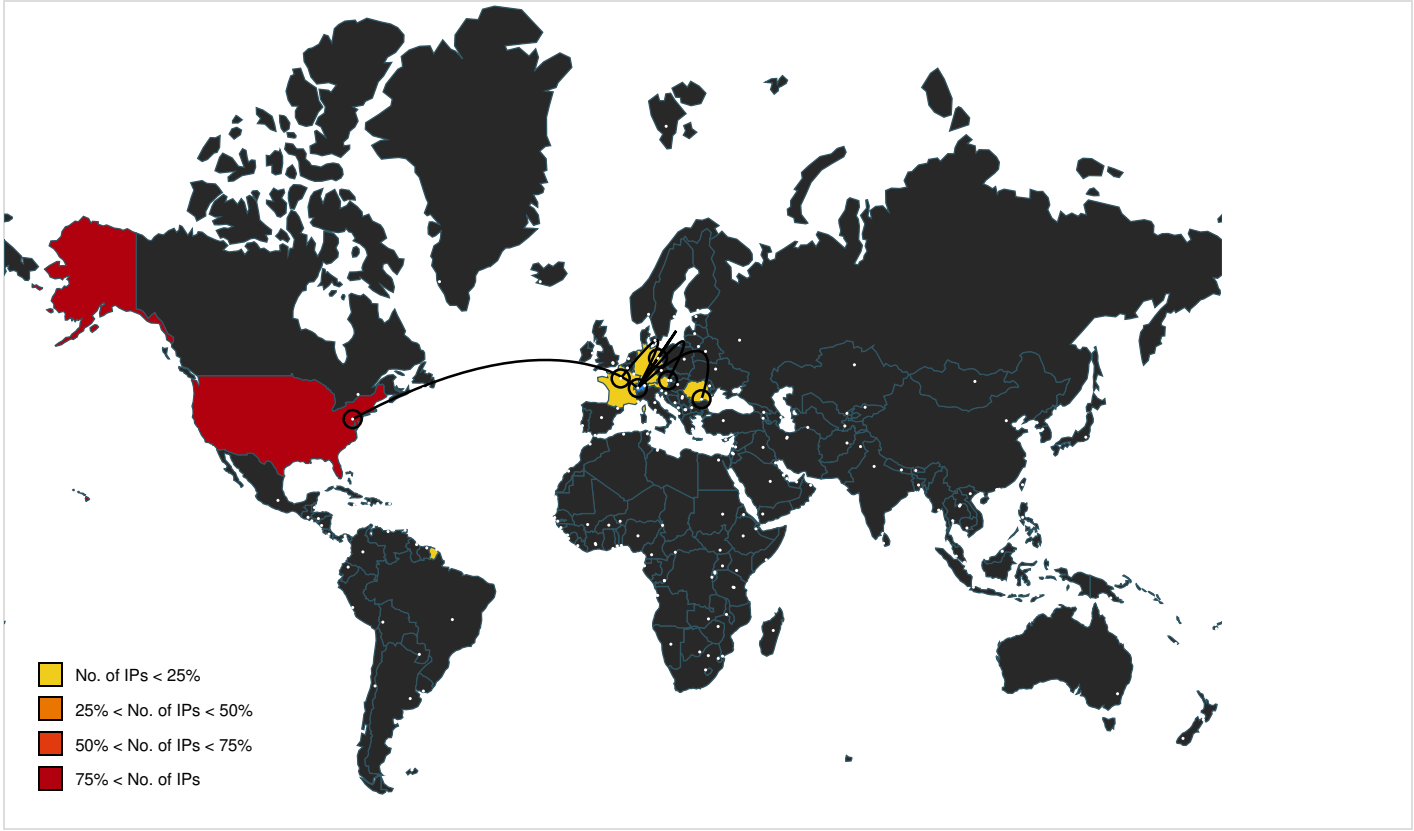
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	cmd.exe, 00000005.00000003.393433818.000000000320B000.00000004.00000020.00020000.00000000.sdmp, HI4NJ046K.5.dr	false		high
http://www.avisrezervee.com/u2kb/www.avisrezervee.com	explorer.exe, 00000004.00000002.571954158.0000000005AC6000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.450261230.0000000005AC3000.00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://duckduckgo.com/ac/?q=	HI4NJ046K.5.dr	false		high
http://www.gritslab.com/u2kb/www.gritslab.com	explorer.exe, 00000004.00000002.571954158.0000000005AC6000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.450261230.0000000005AC3000.00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://www.name.com/domain/renew/222ambking.org?utm_source=Sedo_parked_page&utm_medium=button&utm_c	cmd.exe, 00000005.00000002.569647158.0000000005FE0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://img.sedoparking.com	explorer.exe, 00000004.00000002.580448726.00000000150CC000.00000004.80000000.00040000.00000000.sdmp, cmd.exe, 00000005.00000002.569051526.00000000042BC000.00000004.10000000.00040000.00000000.sdmp, cmd.exe, 00000005.00000002.569647158.0000000005FE0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	cmd.exe, 00000005.00000003.393433818.000000000320B000.00000004.00000020.00020000.00000000.sdmp, HI4NJ046K.5.dr	false		high
http://www.thewildphotographer.co.uk/u2kb/www.thewildphotographer.co.uk	explorer.exe, 00000004.00000002.571954158.0000000005AC6000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.450261230.0000000005AC3000.00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.myglobalIojistik.online	explorer.exe, 00000004.00000003.450261230.0000000005AC3000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.shapshit.xyz	explorer.exe, 00000004.00000003.45026123 0.0000000005AC3000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.germanreps.com	explorer.exe, 00000004.00000003.45026123 0.0000000005AC3000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://thedivinerudraksha.com/u2kb/?pJ=y0bMVGhK3R&s7=im5SXjRwbJIZeY2yeMVWNNnKg99Etck2UhYi2fNZ2Kf/X7l	explorer.exe, 00000004.00000002.58044872 6.00000000158A6000.00000004.80000000.000 40000.00000000.sdmp, cmd.exe, 00000005.0 0000002.569051526.0000000004A96000.00000 004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.ecomofietsen.com	explorer.exe, 00000004.00000003.45026123 0.0000000005AC3000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.thedivinerudraksha.com	explorer.exe, 00000004.00000003.45026123 0.0000000005AC3000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.white-hat.uk/u2kb/www.white-hat.uk	explorer.exe, 00000004.00000002.57195415 8.0000000005AC6000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.450261230.0000000005AC3000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.energyservicestation.com/u2kb/www.energyservicestation.com	explorer.exe, 00000004.00000002.57195415 8.0000000005AC6000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.450261230.0000000005AC3000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.white-hat.uk	explorer.exe, 00000004.00000003.45026123 0.0000000005AC3000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.employerseervices.com/u2kb/www.employerseervices.com	explorer.exe, 00000004.00000002.57195415 8.0000000005AC6000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.450261230.0000000005AC3000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.dzyngiri.com	explorer.exe, 00000004.00000002.58044872 6.0000000015714000.00000004.80000000.000 40000.00000000.sdmp, cmd.exe, 00000005.0 0000002.569051526.0000000004904000.00000 004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.myglobalojistik.online/u2kb/	explorer.exe, 00000004.00000002.57195415 8.0000000005AC6000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.450261230.0000000005AC3000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.avisrezervee.com	explorer.exe, 00000004.00000003.45026123 0.0000000005AC3000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bitservicesltd.com	explorer.exe, 00000004.00000003.45026123 0.0000000005AC3000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://justinmezzell.com	explorer.exe, 00000004.00000002.58044872 6.0000000015714000.00000004.80000000.000 40000.00000000.sdmp, cmd.exe, 00000005.0 0000002.569051526.0000000004904000.00000 004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.white-hat.uk/u2kb/	explorer.exe, 00000004.00000002.57195415 8.0000000005AC6000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.450261230.0000000005AC3000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://alldomains.hosting/domain-registrieren.html	explorer.exe, 00000004.00000002.58044872 6.000000001525E000.00000004.80000000.000 40000.00000000.sdmp, cmd.exe, 00000005.0 0000002.569051526.000000000444E000.00000 004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.gritslab.com	explorer.exe, 00000004.00000003.45026123 0.0000000005AC3000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.thewildphotographer.co.uk	explorer.exe, 00000004.00000003.45026123 0.0000000005AC3000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fclaimrewardccpointq.shop/u2kb/www.fclaimrewardccpointq.shop	explorer.exe, 00000004.00000002.57195415 8.0000000005AC6000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.450261230.0000000005AC3000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.222ambking.org/u2kb/www.222ambking.org	explorer.exe, 00000004.00000002.57195415 8.0000000005AC6000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.450261230.0000000005AC3000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.fclaimrewardccpointq.shop/u2kb/	explorer.exe, 00000004.00000002.57195415 8.0000000005AC6000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.450261230.0000000005AC3000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000004.00000000.32726350 4.0000000008260000.00000004.00000001.000 20000.00000000.sdmp	false		high
http://https://www.name.com/domain/rene	explorer.exe, 00000004.00000002.58044872 6.00000000150CC000.00000004.80000000.000 40000.00000000.sdmp, cmd.exe, 00000005.0 0000002.569051526.00000000042BC000.00000 004.10000000.00040000.00000000.sdmp	false		high
http://www.energyservicestation.com	explorer.exe, 00000004.00000003.45026123 0.0000000005AC3000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	cmd.exe, 00000005.00000003.393433818.000 000000320B000.00000004.00000020.00020000 .00000000.sdmp, HI4NJ046K.5.dr	false		high
http://www.employerseervices.com/u2kb/	explorer.exe, 00000004.00000002.57195415 8.0000000005AC6000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.450261230.0000000005AC3000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://alldomains.hosting/e-mail-server.html	explorer.exe, 00000004.00000002.58044872 6.000000001525E000.00000004.80000000.000 40000.00000000.sdmp, cmd.exe, 00000005.0 0000002.569051526.000000000444E000.00000 004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.younrock.com/u2kb/?ch=1&js=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJhdWQiOiJKb2tlbiIsImV4c	cmd.exe, 00000005.00000002.569647158.000 0000005FE0000.00000004.00000800.00020000 .00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.younrock.com	explorer.exe, 00000004.00000003.45026123 0.0000000005AC3000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	HI4NJ046K.5.dr	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	cmd.exe, 00000005.00000003.393433818.000 000000320B000.00000004.00000020.00020000 .00000000.sdmp, HI4NJ046K.5.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	SecuriteInfo.com.Trojan.Garf.Gen.6.31593.18898.exe	false		high
http://www.un-object.com/u2kb/www.un-object.com	explorer.exe, 00000004.00000002.57195415 8.0000000005AC6000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.450261230.0000000005AC3000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://white-hat.uk/u2kb/?pJ=y0bMVGhK3R&s7=PXfMycAZpTAipct8YsIgv6PR3Y11yPgF2k7967nf/qU1A0mUqq9Jy2mfr	explorer.exe, 00000004.00000002.58044872 6.0000000014C16000.00000004.80000000.000 40000.00000000.sdmp, cmd.exe, 00000005.0 0000002.569051526.0000000003E06000.00000 004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.avisrezervee.com/u2kb/	explorer.exe, 00000004.00000002.57195415 8.0000000005AC6000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.450261230.0000000005AC3000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.myglobalojistik.online/u2kb/www.myglobalojistik.online	explorer.exe, 00000004.00000002.57195415 8.0000000005AC6000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.450261230.0000000005AC3000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	cmd.exe, 00000005.00000003.393433818.000 000000320B000.00000004.00000020.00020000 .00000000.sdmp, HI4NJ046K.5.dr	false		high
http://www.thedivinerudraksha.com/u2kb/www.thedivinerudraksha.com	explorer.exe, 00000004.00000002.57195415 8.0000000005AC6000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.450261230.0000000005AC3000. 00000004.00000001.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://alldomains.hosting/	explorer.exe, 00000004.00000002.58044872 6.000000001525E000.00000004.80000000.000 40000.00000000.sdmp, cmd.exe, 00000005.0 0000002.569051526.000000000444E000.00000 004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fclaimrewardccpointq.shop	explorer.exe, 00000004.00000003.45026123 0.0000000005AC3000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://www.sedo.com/services/parking.php3	cmd.exe, 00000005.00000002.569647158.000 0000005FE0000.00000004.00000800.00020000 .00000000.sdmp	false		high
http://https://ac.ecosia.org/autocomplete?q=	HI4NJ046K.5.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfp	cmd.exe, 00000005.00000003.393433818.000 000000320B000.00000004.00000020.00020000 .00000000.sdmp, HI4NJ046K.5.dr	false		high
http://www.ecomofietsen.com/u2kb/	explorer.exe, 00000004.00000002.57195415 8.0000000005AC6000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.450261230.0000000005AC3000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://alldomains.hosting/hosting-webhosting.html	cmd.exe, 00000005.00000002.569051526.000 000000444E000.00000004.10000000.00040000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.germanreps.com/u2kb/www.germanreps.com	explorer.exe, 00000004.00000002.57195415 8.0000000005AC6000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.450261230.0000000005AC3000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.germanreps.com/u2kb/	explorer.exe, 00000004.00000002.57195415 8.0000000005AC6000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.450261230.0000000005AC3000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.employerseervices.com	explorer.exe, 00000004.00000003.45026123 0.0000000005AC3000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.younrock.com/u2kb/www.younrock.com	explorer.exe, 00000004.00000002.57195415 8.0000000005AC6000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.450261230.0000000005AC3000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.222ambking.org	explorer.exe, 00000004.00000003.45026123 0.0000000005AC3000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.shapshit.xyz/u2kb/www.shapshit.xyz	explorer.exe, 00000004.00000002.57195415 8.0000000005AC6000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.450261230.0000000005AC3000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.ecomofietsen.com/u2kb/www.ecomofietsen.com	explorer.exe, 00000004.00000002.57195415 8.0000000005AC6000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.450261230.0000000005AC3000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.un-object.com	explorer.exe, 00000004.00000003.45026123 0.0000000005AC3000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	HI4NJ046K.5.dr	false		high
http://www.bitservicesltd.com/u2kb/www.bitservicesltd.com	explorer.exe, 00000004.00000002.57195415 8.0000000005AC6000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000003.450261230.0000000005AC3000. 00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
85.187.128.34	thedivinerudraksha.com	United States		55293	A2HOSTINGUS	true
91.195.240.94	www.222ambking.org	Germany		47846	SEDO-ASDE	true
45.33.30.197	www.thewildphotographer.co.uk	United States		63949	LINODE-APLinodeLLCUS	true
78.141.192.145	gritslab.com	France		20473	AS-CHOOPAUS	true
161.97.163.8	www.bitservicesltd.com	United States		51167	CONTABODE	true
81.17.18.198	www.younrock.com	Switzerland		51852	PLI-ASCH	true
192.185.17.12	un-object.com	United States		46606	UNIFIEDLAYER-AS-1US	true
94.176.104.86	white-hat.uk	Romania		5588	GTSCEGTSCentralEurope AntelGermanyCZ	true
213.145.228.111	www.energyservicestation.com	Austria		25575	DOMAINTECHNIKAT	true
199.192.30.147	www.shapshit.xyz	United States		22612	NAMECHEAP-NETUS	true

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830750
Start date and time:	2023-03-20 16:58:12 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	10
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	SecuriteInfo.com.Trojan.Garf.Gen.6.31593.18898.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@8/5@12/10
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 80.6% (good quality ratio 73.9%) • Quality average: 74.7% • Quality standard deviation: 31.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe
- TCP Packets have been reduced to 100
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:00:00	API Interceptor	498x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\HI4NJ046K

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2880737026424216
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPQ6YVucbj8Ewn7PrH944:QS/inojVucbj8Ewn7b944
MD5:	5F02C426BCF0D3E3DC81F002F9125663
SHA1:	EA50920666E30250E4BE05194FA7B3F44967BE94
SHA-256:	DF93CD763CFEC79473D0DCF58C77D45C99D246CE347652BF215A97D8D1267EFA
SHA-512:	53EFE8F752484B48C39E1ABFBA05840FF2B968DE2BCAE16287877F69BABE8C54617E76C6953A22789043E27C9CCA9DB4FED5D2C2A512CBDDB5015F4CAB57C198
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

C:\Users\user\AppData\Local\Temp\bzuxwizqdxf.m

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Garf.Gen.6.31593.18898.exe
File Type:	data
Category:	dropped
Size (bytes):	5738
Entropy (8bit):	7.164987839661835
Encrypted:	false
SSDEEP:	96:Farc6oY7g/DrYu+k2XO5oSwYiAVW9aRDGDprAhThqwDQgNDQXzL2gf:FarcRfWhX1S9H9tGlg9h3hgf
MD5:	EE48E241B19CF476BAB747E7BFFBE1E6
SHA1:	ECD535B070BAC75909809590AE8CEE602A65F8FF
SHA-256:	2F25ECE58FD26C56F04DCDCDA1273E75D2101A78FD0717605F0148ADEA9E83EA
SHA-512:	2ED2C6059DD18824BE7B217023A78B4FDCE37424D1C1949E896B4C311C16F084B86DC7178C06174A5ECC5988653AC97CB9B67307A6B766166BABC063B942AD57
Malicious:	false
Preview:	.005m..f.F<...05o.:.....?v>.3.3.<.....M.knl.02a..c.E<...42c. .....4.D63.6.3.?.....E.gni.53P..805.p8.q?.2.8.u .a..beabo.H0..v..v.@3.`..i/7.p.6.t(2..g.}.u<..G-.0.3.h.f....w8L$.m.r .D;F...okc..m.;4.q.?.<@.4.0...m..u<f...@%.`4..D'd.O$..A5..=..<r..4M.knl.82a..Q..401ec.t4.M4...D;.D..d580..E9....E....3.u.mje.18e..`W..480.x<.p=.4.4.p-P..6.c.!....D%.|.eX. ....+..t..0....e.a..`beP..580.p=.t>.8.5.p,XE..Md.....M9..e...@4.....F1..u.|c.....Lq.}<...v<+480.}<;.&<.>..r.^.q8F0....q.^.q8F0...^..M...3uc.....}<F...kloe.=8e...548.r...t..w.(058. q..v..l.0A..q..34.q.p.}..u.{.w....}.p013.....u.L.4F".u..04.t.t.q..p.x.u....q.8580..Y...}..E.4D'.q..80.}.t.t..w.p.p...X+AK..M.....v.ZXK.J.E.....}.]..O.F.....u.X_.M.M.....H...X...K.D.....}. \&....A..B....G...P5..O.E..P....\...Y...K.E..a....B...].4.T.4.q0.p..q..~<1|..x.q.>.t&.u.|1,.t..w.pe..\...w.p..u.T.4.Q.0.}.;.q%..5M%.}.;.qm..tL9.}.5013.6.].5.u...K...P3480..u...dR0. m...D4...B358.q.0342.}.e.....dX4R0]<048[3^2^8Z5..p...d.a..

C:\Users\user\AppData\Local\Temp\nsjF9DC.tmp

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Garf.Gen.6.31593.18898.exe
File Type:	data
Category:	dropped
Size (bytes):	326683
Entropy (8bit):	7.56585074937259
Encrypted:	false
SSDEEP:	6144:llDH7L09bR9XjKk1c85uxmCum7ZjmOLPzCu/GZVZxML7L26P:llnL0w0cxxmidCODzCu/QZOL2
MD5:	DB1F24D7DE5473B1FEB30958D5620614
SHA1:	956E2FCB636FBA3FEFC9EBFCA96CCEC7605B252B
SHA-256:	A635BBBC73BA851204F9242C529EF59C9C1A133D1A98D8BCBFE1B0161216400B
SHA-512:	35D949222412B4CA343454A4CE247067C3A74B5CB4CCA3FFEAA0C0F7AE5734C82D6E552FB1EBB984A4953EA760F24BBF5C249B83FE3C85959AB78E6625F0B642
Malicious:	false
Preview:	.7.....,.....(.....6.....p7.....$..... .....G.....j.....=..... ....

C:\Users\user\AppData\Local\Temp\rdypmbfg.qv

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Garf.Gen.6.31593.18898.exe

File Type:	data
Category:	dropped
Size (bytes):	211481
Entropy (8bit):	**7.998948076055924**
Encrypted:	**true**
SSDEEP:	3072:mKd38ED05C8QZ/bLX8NWvByZA6XRxnIGb/D/Kk7iVSc8k1wPuxD6QH+0gZm7IKjS:hlDH7L09bR9XjKk1c85uxmCum7ZjmOLy
MD5:	4C2A176B3C04DB72501ED445A646E276
SHA1:	26C8DCB493EB56374B0A96D5453BB535F7A515CC
SHA-256:	F9713AB900F44015FD669DF94861D50D98281D447964913B0132E1CAC002351B
SHA-512:	B0673860453637C95F09AE4766DBB10B5DFA0282D48B0B351EE8231C304C08EEADC721E8A64C941462E93C175431CECBE5F9530C2A5FDF937ADE42FCE3FA0ED5
Malicious:	false
Preview:	...R..#D6....N>.R.*.}jW.;Q.w;.E..|.r....b..eA..<..}U....^...t..qmu.....Ry..H.[...xe.(*....x.c3.<.P...;.\U..q^.P..Bl..a.i.v.5#.q..c.kj...EX.1..Y..5.eG..N=.u.@./.....V..V$6#.X...-.W(.'.....fh&.U....P#M.R.>..Ec..z4R.....*s..J.yEQ@..&.G..ntP.....#..x...&..~...{.....\p7..E..\|Br....b.1eA..<k.}U....^..)..X..n.%/....Y.k.J.....\Q.8.....t..#. *.\....n.'..n..]..Bl...."c?/~...E$o._..U.....F...).F.....^.6g..I..5..V..V$6#.{.LW-.WM4-.....A.4UN...P#M.R.AR..cO...4R.....*S`.J..EQ@tz.&.....tP.D..)....#D..x...&.....{.....pw;.E..\|.r....b..eA..<..}U....^..)..X..n.%/....Y.k.J.....\Q.8....t..#. *.\....n.'..n..]..Bl...."c?/~...E$o._..U.....F...).F.....^.6g..I..5..V..V$6#.X...-.WYh'....[.4U....P#M.R.AR..c..z4R.....*S`.J..EQ@tz.&.....tP.D..)....#D..x...&.....{.....pw;.E..\|.r....b..eA..<..}U....^..)..X..n.%/....Y.k.J.....\Q.8.....t..#. *.\....n.'..n..]..Bl...."c?/~...E$o._..U.....F...).F.....^.6g..I..5..V..V$6#.X...-.WYh'....[.4U....P#M.R.AR..c..z4R.....*

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

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Garf.Gen.6.31593.18898.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	95232
Entropy (8bit):	6.23150349499231
Encrypted:	false
SSDEEP:	1536:opZrDPCXLdr7zQN/GZGLaYeZjtBaKaedCRVLR8dpxekydJrD9iiU71aC4sWBlVmI:oHTCB7Y/GZGPeZxaGCRVLR9kydI7sCUJ
MD5:	6D30D26416D626447BA4298A59111F6D
SHA1:	C7F0941793929D391369F59FD92FFD4B2DC5C598
SHA-256:	C53E0E6337805EC801493437F7811672A1B3C187611799116D5490AB2E63B1EC
SHA-512:	79946C7F1D3F1F9A56ED7A3F6BCA739F73801B6BCEFB6CC41945BE28A4542A1FD511D52269A61DB887CD2DF42D8B87D7E497295FDBC9E226B25FDB745DF7940F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 39%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....{.8-?.V~?.V~?.V~t.U.5.V~t.S...V~t.R.+.V~..S...V~..R...V~..U.,.V~t.W.(.V~?.W~@.V~..^.>.V~..T.>.V~Rich?.V~.....PE..L...gX.d.....!.....z.....@.....<k.....^.....]..@.....text..... ..`.rdata...e.....f.....@..@.data...l.....j.....@.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.926529383010501
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:	SecuriteInfo.com.Trojan.Garf.Gen.6.31593.18898.exe
File size:	299717
MD5:	c7714b273571ba64c0b77afca236ac6d
SHA1:	c24d9460bee8a724abe8b0dcf3d74851dd5737ed
SHA256:	e62c1e809c48e66104c34ae3e977b82fbea2e984dee708bda431b608c2774c28
SHA512:	e70d15e6d9e318e509013088a42f02c2298af5f85ca91c8463f1fb7fc3d5216ec7ef6e9a8c343f95f5a0b457260014d8c15c5e0b7e8d1a050c3963618adb159e
SSDEEP:	6144:vYa69KnJK2Vi0/1olkMjLow/9AO3xVFLFlXT+rcYGRleg3Cdl2xHW7:vYnKndVJAnow/6O3xV5TD+rcYCKyy
TLSH:	435412A63178C03BF5A141306F7512AA9EFDDA1278F90A0B4B901B6D7F7AB14650F393
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....h...*.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x403640
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x614F9B1F [Sat Sep 25 21:56:47 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	61259b55b8912888e90f516ca08dc514

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A230h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080C8h]
mov esi, dword ptr [004080CCh]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007F57DC75144Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h

Instruction
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F57DC75141Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A318h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3b000	0xcd8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6676	0x6800	False	0.6568134014423077	data	6.4174599871908855	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.4498046875	data	5.141066817170598	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20378	0x600	False	0.509765625	data	4.110582127654237	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2b000	0x10000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x3b000	0xcd8	0xe00	False	0.4224330357142857	data	4.230532221238809	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3b1d8	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 640	English	United States
RT_DIALOG	0x3b4c0	0x100	data	English	United States
RT_DIALOG	0x3b5c0	0x11c	data	English	United States
RT_DIALOG	0x3b6e0	0x60	data	English	United States
RT_GROUP_ICON	0x3b740	0x14	data	English	United States
RT_VERSION	0x3b758	0x240	data	English	United States
RT_MANIFEST	0x3b998	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, CreateFileW, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.491.195.240.94 49702802031449 03/20/23-17:00:09.343542	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49702	80	192.168.2.4	91.195.240.94

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.481.17.18.1984 9706802031412 03/20/23- 17:00:25.955923	TCP	203141 2	ET TROJAN FormBook CnC Checkin (GET)	49706	80	192.168.2.4	81.17.18.198
192.168.2.481.17.18.1984 9706802031453 03/20/23- 17:00:25.955923	TCP	203145 3	ET TROJAN FormBook CnC Checkin (GET)	49706	80	192.168.2.4	81.17.18.198
192.168.2.494.176.104.86 49696802031453 03/20/23- 16:59:46.201874	TCP	203145 3	ET TROJAN FormBook CnC Checkin (GET)	49696	80	192.168.2.4	94.176.104.8 6
192.168.2.491.195.240.94 49702802031453 03/20/23- 17:00:09.343542	TCP	203145 3	ET TROJAN FormBook CnC Checkin (GET)	49702	80	192.168.2.4	91.195.240.9 4
192.168.2.494.176.104.86 49696802031412 03/20/23- 16:59:46.201874	TCP	203141 2	ET TROJAN FormBook CnC Checkin (GET)	49696	80	192.168.2.4	94.176.104.8 6
192.168.2.491.195.240.94 49702802031412 03/20/23- 17:00:09.343542	TCP	203141 2	ET TROJAN FormBook CnC Checkin (GET)	49702	80	192.168.2.4	91.195.240.9 4
192.168.2.494.176.104.86 49696802031449 03/20/23- 16:59:46.201874	TCP	203144 9	ET TROJAN FormBook CnC Checkin (GET)	49696	80	192.168.2.4	94.176.104.8 6
192.168.2.481.17.18.1984 9706802031449 03/20/23- 17:00:25.955923	TCP	203144 9	ET TROJAN FormBook CnC Checkin (GET)	49706	80	192.168.2.4	81.17.18.198

Network Port Distribution

Total Packets: 49

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 16:59:46.164385080 CET	49696	80	192.168.2.4	94.176.104.86
Mar 20, 2023 16:59:46.201606989 CET	80	49696	94.176.104.86	192.168.2.4
Mar 20, 2023 16:59:46.201721907 CET	49696	80	192.168.2.4	94.176.104.86
Mar 20, 2023 16:59:46.201874018 CET	49696	80	192.168.2.4	94.176.104.86
Mar 20, 2023 16:59:46.239142895 CET	80	49696	94.176.104.86	192.168.2.4
Mar 20, 2023 16:59:46.439270973 CET	80	49696	94.176.104.86	192.168.2.4
Mar 20, 2023 16:59:46.439304113 CET	80	49696	94.176.104.86	192.168.2.4
Mar 20, 2023 16:59:46.439450979 CET	49696	80	192.168.2.4	94.176.104.86
Mar 20, 2023 16:59:46.439614058 CET	49696	80	192.168.2.4	94.176.104.86
Mar 20, 2023 16:59:46.476691008 CET	80	49696	94.176.104.86	192.168.2.4
Mar 20, 2023 16:59:51.479353905 CET	49697	80	192.168.2.4	78.141.192.145
Mar 20, 2023 16:59:51.508332968 CET	80	49697	78.141.192.145	192.168.2.4
Mar 20, 2023 16:59:51.510864019 CET	49697	80	192.168.2.4	78.141.192.145

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 16:59:51.510987997 CET	49697	80	192.168.2.4	78.141.192.145
Mar 20, 2023 16:59:51.538568974 CET	80	49697	78.141.192.145	192.168.2.4
Mar 20, 2023 16:59:51.538933992 CET	80	49697	78.141.192.145	192.168.2.4
Mar 20, 2023 16:59:51.539037943 CET	80	49697	78.141.192.145	192.168.2.4
Mar 20, 2023 16:59:51.539123058 CET	49697	80	192.168.2.4	78.141.192.145
Mar 20, 2023 16:59:53.025367975 CET	49697	80	192.168.2.4	78.141.192.145
Mar 20, 2023 16:59:54.043806076 CET	49698	80	192.168.2.4	78.141.192.145
Mar 20, 2023 16:59:54.071490049 CET	80	49698	78.141.192.145	192.168.2.4
Mar 20, 2023 16:59:54.071722031 CET	49698	80	192.168.2.4	78.141.192.145
Mar 20, 2023 16:59:54.072148085 CET	49698	80	192.168.2.4	78.141.192.145
Mar 20, 2023 16:59:54.099571943 CET	80	49698	78.141.192.145	192.168.2.4
Mar 20, 2023 16:59:54.099611998 CET	80	49698	78.141.192.145	192.168.2.4
Mar 20, 2023 16:59:54.099633932 CET	80	49698	78.141.192.145	192.168.2.4
Mar 20, 2023 16:59:54.099822998 CET	49698	80	192.168.2.4	78.141.192.145
Mar 20, 2023 16:59:54.100164890 CET	49698	80	192.168.2.4	78.141.192.145
Mar 20, 2023 16:59:54.127706051 CET	80	49698	78.141.192.145	192.168.2.4
Mar 20, 2023 16:59:59.126749039 CET	49699	80	192.168.2.4	161.97.163.8
Mar 20, 2023 16:59:59.153734922 CET	80	49699	161.97.163.8	192.168.2.4
Mar 20, 2023 16:59:59.153947115 CET	49699	80	192.168.2.4	161.97.163.8
Mar 20, 2023 16:59:59.154143095 CET	49699	80	192.168.2.4	161.97.163.8
Mar 20, 2023 16:59:59.181529999 CET	80	49699	161.97.163.8	192.168.2.4
Mar 20, 2023 16:59:59.182496071 CET	80	49699	161.97.163.8	192.168.2.4
Mar 20, 2023 16:59:59.182528019 CET	80	49699	161.97.163.8	192.168.2.4
Mar 20, 2023 16:59:59.182634115 CET	49699	80	192.168.2.4	161.97.163.8
Mar 20, 2023 17:00:00.666766882 CET	49699	80	192.168.2.4	161.97.163.8
Mar 20, 2023 17:00:01.683223009 CET	49700	80	192.168.2.4	161.97.163.8
Mar 20, 2023 17:00:01.707376957 CET	80	49700	161.97.163.8	192.168.2.4
Mar 20, 2023 17:00:01.707633018 CET	49700	80	192.168.2.4	161.97.163.8
Mar 20, 2023 17:00:01.707849026 CET	49700	80	192.168.2.4	161.97.163.8
Mar 20, 2023 17:00:01.731712103 CET	80	49700	161.97.163.8	192.168.2.4
Mar 20, 2023 17:00:01.732481956 CET	80	49700	161.97.163.8	192.168.2.4
Mar 20, 2023 17:00:01.732547998 CET	80	49700	161.97.163.8	192.168.2.4
Mar 20, 2023 17:00:01.732713938 CET	49700	80	192.168.2.4	161.97.163.8
Mar 20, 2023 17:00:01.732954979 CET	49700	80	192.168.2.4	161.97.163.8
Mar 20, 2023 17:00:01.756808043 CET	80	49700	161.97.163.8	192.168.2.4
Mar 20, 2023 17:00:06.786604881 CET	49701	80	192.168.2.4	91.195.240.94
Mar 20, 2023 17:00:06.806010008 CET	80	49701	91.195.240.94	192.168.2.4
Mar 20, 2023 17:00:06.807351112 CET	49701	80	192.168.2.4	91.195.240.94
Mar 20, 2023 17:00:06.807351112 CET	49701	80	192.168.2.4	91.195.240.94
Mar 20, 2023 17:00:06.827474117 CET	80	49701	91.195.240.94	192.168.2.4
Mar 20, 2023 17:00:06.827512026 CET	80	49701	91.195.240.94	192.168.2.4
Mar 20, 2023 17:00:06.832981110 CET	49701	80	192.168.2.4	91.195.240.94
Mar 20, 2023 17:00:08.308280945 CET	49701	80	192.168.2.4	91.195.240.94
Mar 20, 2023 17:00:09.324009895 CET	49702	80	192.168.2.4	91.195.240.94
Mar 20, 2023 17:00:09.343242884 CET	80	49702	91.195.240.94	192.168.2.4
Mar 20, 2023 17:00:09.343389988 CET	49702	80	192.168.2.4	91.195.240.94
Mar 20, 2023 17:00:09.343542099 CET	49702	80	192.168.2.4	91.195.240.94
Mar 20, 2023 17:00:09.394530058 CET	80	49702	91.195.240.94	192.168.2.4
Mar 20, 2023 17:00:09.394562960 CET	80	49702	91.195.240.94	192.168.2.4
Mar 20, 2023 17:00:09.394582987 CET	80	49702	91.195.240.94	192.168.2.4
Mar 20, 2023 17:00:09.394602060 CET	80	49702	91.195.240.94	192.168.2.4
Mar 20, 2023 17:00:09.394620895 CET	80	49702	91.195.240.94	192.168.2.4
Mar 20, 2023 17:00:09.394639969 CET	80	49702	91.195.240.94	192.168.2.4
Mar 20, 2023 17:00:09.394659042 CET	80	49702	91.195.240.94	192.168.2.4
Mar 20, 2023 17:00:09.394673109 CET	80	49702	91.195.240.94	192.168.2.4
Mar 20, 2023 17:00:09.394748926 CET	80	49702	91.195.240.94	192.168.2.4
Mar 20, 2023 17:00:09.394779921 CET	49702	80	192.168.2.4	91.195.240.94
Mar 20, 2023 17:00:09.394840002 CET	80	49702	91.195.240.94	192.168.2.4
Mar 20, 2023 17:00:09.394848108 CET	49702	80	192.168.2.4	91.195.240.94

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 17:00:09.394885063 CET	49702	80	192.168.2.4	91.195.240.94
Mar 20, 2023 17:00:09.413861036 CET	80	49702	91.195.240.94	192.168.2.4
Mar 20, 2023 17:00:09.413888931 CET	80	49702	91.195.240.94	192.168.2.4
Mar 20, 2023 17:00:09.413908958 CET	80	49702	91.195.240.94	192.168.2.4
Mar 20, 2023 17:00:09.413927078 CET	80	49702	91.195.240.94	192.168.2.4
Mar 20, 2023 17:00:09.413945913 CET	80	49702	91.195.240.94	192.168.2.4
Mar 20, 2023 17:00:09.413964033 CET	80	49702	91.195.240.94	192.168.2.4
Mar 20, 2023 17:00:09.413973093 CET	49702	80	192.168.2.4	91.195.240.94
Mar 20, 2023 17:00:09.413983107 CET	80	49702	91.195.240.94	192.168.2.4
Mar 20, 2023 17:00:09.414005041 CET	80	49702	91.195.240.94	192.168.2.4
Mar 20, 2023 17:00:09.414017916 CET	49702	80	192.168.2.4	91.195.240.94
Mar 20, 2023 17:00:09.414125919 CET	49702	80	192.168.2.4	91.195.240.94
Mar 20, 2023 17:00:09.414351940 CET	49702	80	192.168.2.4	91.195.240.94
Mar 20, 2023 17:00:09.433420897 CET	80	49702	91.195.240.94	192.168.2.4
Mar 20, 2023 17:00:15.521128893 CET	49703	80	192.168.2.4	213.145.228.111
Mar 20, 2023 17:00:15.542534113 CET	80	49703	213.145.228.111	192.168.2.4
Mar 20, 2023 17:00:15.542710066 CET	49703	80	192.168.2.4	213.145.228.111
Mar 20, 2023 17:00:15.542984962 CET	49703	80	192.168.2.4	213.145.228.111
Mar 20, 2023 17:00:15.564192057 CET	80	49703	213.145.228.111	192.168.2.4
Mar 20, 2023 17:00:15.750376940 CET	80	49703	213.145.228.111	192.168.2.4
Mar 20, 2023 17:00:15.750427961 CET	80	49703	213.145.228.111	192.168.2.4
Mar 20, 2023 17:00:15.750452995 CET	80	49703	213.145.228.111	192.168.2.4
Mar 20, 2023 17:00:15.750571012 CET	49703	80	192.168.2.4	213.145.228.111
Mar 20, 2023 17:00:15.758713961 CET	80	49703	213.145.228.111	192.168.2.4
Mar 20, 2023 17:00:15.758759975 CET	80	49703	213.145.228.111	192.168.2.4
Mar 20, 2023 17:00:15.758881092 CET	49703	80	192.168.2.4	213.145.228.111
Mar 20, 2023 17:00:17.061141014 CET	49703	80	192.168.2.4	213.145.228.111
Mar 20, 2023 17:00:18.075567007 CET	49704	80	192.168.2.4	213.145.228.111

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 16:59:46.136440992 CET	56572	53	192.168.2.4	8.8.8.8
Mar 20, 2023 16:59:46.156369925 CET	53	56572	8.8.8.8	192.168.2.4
Mar 20, 2023 16:59:51.451244116 CET	50911	53	192.168.2.4	8.8.8.8
Mar 20, 2023 16:59:51.474733114 CET	53	50911	8.8.8.8	192.168.2.4
Mar 20, 2023 16:59:59.107836008 CET	59683	53	192.168.2.4	8.8.8.8
Mar 20, 2023 16:59:59.125689983 CET	53	59683	8.8.8.8	192.168.2.4
Mar 20, 2023 17:00:06.763504028 CET	64167	53	192.168.2.4	8.8.8.8
Mar 20, 2023 17:00:06.785231113 CET	53	64167	8.8.8.8	192.168.2.4
Mar 20, 2023 17:00:15.491092920 CET	58565	53	192.168.2.4	8.8.8.8
Mar 20, 2023 17:00:15.519546032 CET	53	58565	8.8.8.8	192.168.2.4
Mar 20, 2023 17:00:23.355577946 CET	52239	53	192.168.2.4	8.8.8.8
Mar 20, 2023 17:00:23.388257980 CET	53	52239	8.8.8.8	192.168.2.4
Mar 20, 2023 17:00:31.040029049 CET	56807	53	192.168.2.4	8.8.8.8
Mar 20, 2023 17:00:31.183070898 CET	53	56807	8.8.8.8	192.168.2.4
Mar 20, 2023 17:00:39.271570921 CET	61007	53	192.168.2.4	8.8.8.8
Mar 20, 2023 17:00:39.320899963 CET	53	61007	8.8.8.8	192.168.2.4
Mar 20, 2023 17:00:47.549798012 CET	60686	53	192.168.2.4	8.8.8.8
Mar 20, 2023 17:00:47.680247068 CET	53	60686	8.8.8.8	192.168.2.4
Mar 20, 2023 17:00:56.317701101 CET	61124	53	192.168.2.4	8.8.8.8
Mar 20, 2023 17:00:56.368645906 CET	53	61124	8.8.8.8	192.168.2.4
Mar 20, 2023 17:00:57.380626917 CET	59444	53	192.168.2.4	8.8.8.8
Mar 20, 2023 17:00:57.408945084 CET	53	59444	8.8.8.8	192.168.2.4
Mar 20, 2023 17:01:02.477611065 CET	55570	53	192.168.2.4	8.8.8.8
Mar 20, 2023 17:01:02.627077103 CET	53	55570	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 16:59:46.136440992 CET	192.168.2.4	8.8.8.8	0x7d04	Standard query (0)	www.white-hat.uk	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:59:51.451244116 CET	192.168.2.4	8.8.8.8	0xcb57	Standard query (0)	www.gritslab.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:59:59.107836008 CET	192.168.2.4	8.8.8.8	0x9da5	Standard query (0)	www.bitservicesltd.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:00:06.763504028 CET	192.168.2.4	8.8.8.8	0xf43c	Standard query (0)	www.222ambking.org	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:00:15.491092920 CET	192.168.2.4	8.8.8.8	0x4b72	Standard query (0)	www.energyservicestation.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:00:23.355577946 CET	192.168.2.4	8.8.8.8	0xe0bc	Standard query (0)	www.younrock.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:00:31.040029049 CET	192.168.2.4	8.8.8.8	0x5edb	Standard query (0)	www.thewildphotographer.co.uk	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:00:39.271570921 CET	192.168.2.4	8.8.8.8	0x317e	Standard query (0)	www.shapshit.xyz	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:00:47.549798012 CET	192.168.2.4	8.8.8.8	0x692b	Standard query (0)	www.thedivinerudraksha.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:00:56.317701101 CET	192.168.2.4	8.8.8.8	0x95e7	Standard query (0)	www.fclaimrewardccpointq.shop	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:00:57.380626917 CET	192.168.2.4	8.8.8.8	0x29b0	Standard query (0)	www.fclaimrewardccpointq.shop	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:01:02.477611065 CET	192.168.2.4	8.8.8.8	0xbf61	Standard query (0)	www.un-object.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 16:59:46.156369925 CET	8.8.8.8	192.168.2.4	0x7d04	No error (0)	www.white-hat.uk	white-hat.uk		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 16:59:46.156369925 CET	8.8.8.8	192.168.2.4	0x7d04	No error (0)	white-hat.uk		94.176.104.86	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:59:51.474733114 CET	8.8.8.8	192.168.2.4	0xcb57	No error (0)	www.gritslab.com	gritslab.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 16:59:51.474733114 CET	8.8.8.8	192.168.2.4	0xcb57	No error (0)	gritslab.com		78.141.192.145	A (IP address)	IN (0x0001)	false
Mar 20, 2023 16:59:59.125689983 CET	8.8.8.8	192.168.2.4	0x9da5	No error (0)	www.bitservicesltd.com		161.97.163.8	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:00:06.785231113 CET	8.8.8.8	192.168.2.4	0xf43c	No error (0)	www.222ambking.org		91.195.240.94	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:00:15.519546032 CET	8.8.8.8	192.168.2.4	0x4b72	No error (0)	www.energyservicestation.com		213.145.228.111	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:00:23.388257980 CET	8.8.8.8	192.168.2.4	0xe0bc	No error (0)	www.younrock.com		81.17.18.198	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:00:31.183070898 CET	8.8.8.8	192.168.2.4	0x5edb	No error (0)	www.thewildphotographer.co.uk		45.33.30.197	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:00:31.183070898 CET	8.8.8.8	192.168.2.4	0x5edb	No error (0)	www.thewildphotographer.co.uk		45.79.19.196	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:00:31.183070898 CET	8.8.8.8	192.168.2.4	0x5edb	No error (0)	www.thewildphotographer.co.uk		45.56.79.23	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:00:31.183070898 CET	8.8.8.8	192.168.2.4	0x5edb	No error (0)	www.thewildphotographer.co.uk		45.33.20.235	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:00:31.183070898 CET	8.8.8.8	192.168.2.4	0x5edb	No error (0)	www.thewildphotographer.co.uk		72.14.178.174	A (IP address)	IN (0x0001)	false

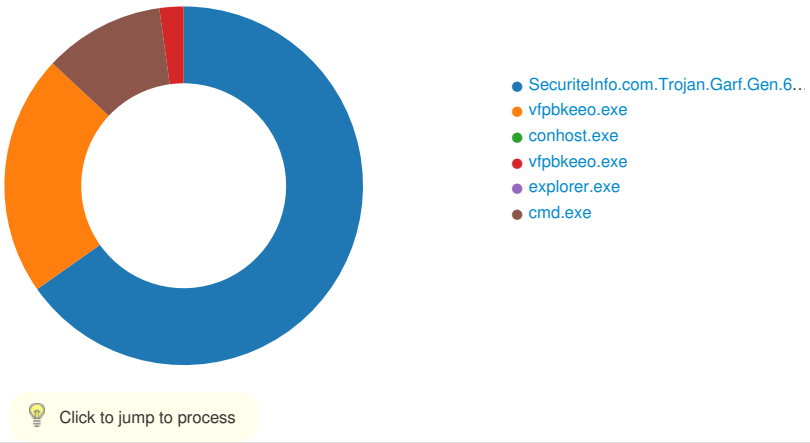
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 17:00:31.183070898 CET	8.8.8.8	192.168.2.4	0x5edb	No error (0)	www.thewildphotographer.co.uk		198.58.118.167	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:00:31.183070898 CET	8.8.8.8	192.168.2.4	0x5edb	No error (0)	www.thewildphotographer.co.uk		96.126.123.244	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:00:31.183070898 CET	8.8.8.8	192.168.2.4	0x5edb	No error (0)	www.thewildphotographer.co.uk		72.14.185.43	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:00:31.183070898 CET	8.8.8.8	192.168.2.4	0x5edb	No error (0)	www.thewildphotographer.co.uk		45.33.2.79	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:00:31.183070898 CET	8.8.8.8	192.168.2.4	0x5edb	No error (0)	www.thewildphotographer.co.uk		173.255.194.134	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:00:31.183070898 CET	8.8.8.8	192.168.2.4	0x5edb	No error (0)	www.thewildphotographer.co.uk		45.33.18.44	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:00:31.183070898 CET	8.8.8.8	192.168.2.4	0x5edb	No error (0)	www.thewildphotographer.co.uk		45.33.23.183	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:00:39.320899963 CET	8.8.8.8	192.168.2.4	0x317e	No error (0)	www.shapshit.xyz		199.192.30.147	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:00:47.680247068 CET	8.8.8.8	192.168.2.4	0x692b	No error (0)	www.thedivinerudraksha.com	thedivinerudraksha.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 17:00:47.680247068 CET	8.8.8.8	192.168.2.4	0x692b	No error (0)	thedivinerudraksha.com		85.187.128.34	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:00:56.368645906 CET	8.8.8.8	192.168.2.4	0x95e7	Name error (3)	www.fclaimrewardccpointq.shop	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:00:57.408945084 CET	8.8.8.8	192.168.2.4	0x29b0	Name error (3)	www.fclaimrewardccpointq.shop	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:01:02.627077103 CET	8.8.8.8	192.168.2.4	0xbf61	No error (0)	www.un-object.com	un-object.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 17:01:02.627077103 CET	8.8.8.8	192.168.2.4	0xbf61	No error (0)	un-object.com		192.185.17.12	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.white-hat.uk
- www.gritslab.com
- www.bitservicesltd.com
- www.222ambking.org
- www.energyservicestation.com
- www.younrock.com
- www.thewildphotographer.co.uk
- www.shapshit.xyz
- www.thedivinerudraksha.com
- www.un-object.com

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.Trojan.Garf.Gen.6.31593.18898.exe PID: **5020**, Parent PID: **3528**

General

Target ID:	0
Start time:	16:59:05
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Garf.Gen.6.31593.18898.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.Garf.Gen.6.31593.18898.exe
Imagebase:	0x400000
File size:	299717 bytes
MD5 hash:	C7714B273571BA64C0B77AFCA236AC6D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: vfpbkeeo.exe PID: **1316**, Parent PID: **5020**

General

Target ID:	1
Start time:	16:59:05
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Local\Temp\vfpbkeeo.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\vfpbkeeo.exe" C:\Users\user\AppData\Local\Temp\bzuxwizqdxf.m
Imagebase:	0x400000
File size:	95232 bytes
MD5 hash:	6D30D26416D626447BA4298A59111F6D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 39%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\bzuxwizqdxf.m	unknown	4096	success or wait	1	4077E4	ReadFile
C:\Users\user\AppData\Local\Temp\bzuxwizqdxf.m	unknown	4096	success or wait	1	4077E4	ReadFile
C:\Users\user\AppData\Local\Temp\rdypmbfg.qv	unknown	190464	success or wait	1	A40A2C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	A40E8B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	A40E8B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	A40E8B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	A40E8B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	A40E8B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	A40E8B	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	A40E8B	ReadFile

Analysis Process: conhost.exe PID: **1240**, Parent PID: **1316**

General

Target ID:	2
Start time:	16:59:05
Start date:	20/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: vfpbkeeo.exe PID: **1948**, Parent PID: **1316**

General

Target ID:	3
Start time:	16:59:06
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Local\Temp\vfpbkeeo.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\vfpbkeeo.exe
Imagebase:	0x400000
File size:	95232 bytes
MD5 hash:	6D30D26416D626447BA4298A59111F6D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000003.00000002.352371790.00000000008C0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.352371790.00000000008C0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.352371790.00000000008C0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000003.00000002.352064891.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.352064891.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.352064891.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000003.00000002.352209935.0000000000430000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.352209935.0000000000430000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.352209935.0000000000430000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41E74A	NtReadFile

Analysis Process: explorer.exe PID: **3528**, Parent PID: **1948**

General

Target ID:	4
Start time:	16:59:12
Start date:	20/03/2023
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff618f60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

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

Analysis Process: cmd.exe PID: **916**, Parent PID: **3528**

General

Target ID:	5
Start time:	16:59:25

Start date:	20/03/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmd.exe
Imagebase:	0xd90000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000005.00000002.567150912.0000000000D10000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000002.567150912.0000000000D10000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.567150912.0000000000D10000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000005.00000002.567279277.0000000000D50000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000002.567279277.0000000000D50000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.567279277.0000000000D50000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000005.00000002.567056934.0000000000C20000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000005.00000002.567056934.0000000000C20000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.567056934.0000000000C20000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vfpbkeeo.exe	success or wait	1	C3C957	NtDeleteFile
C:\Users\user\AppData\Local\Temp\HI4NJ046K	object name not found	1	C3C957	NtDeleteFile
C:\Users\user\AppData\Local\Temp\HI4NJ046K	sharing violation	1	C3C957	NtDeleteFile
C:\Users\user\AppData\Local\Temp\HI4NJ046K	sharing violation	1	C3C957	NtDeleteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	C3C927	NtReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Disassembly

No disassembly