ID: 830804
Sample Name:
u8QPnVhq0N.exe
Cookbook: default.jbs
Time: 17:49:26
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

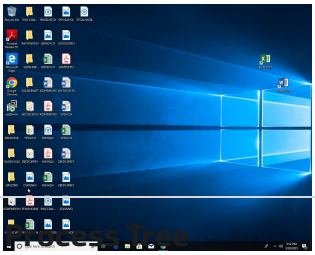
Windows Analysis Report

u8QPnVhq0N.exe

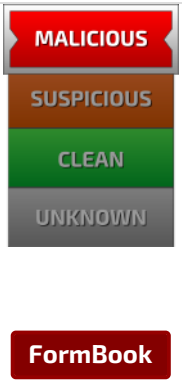
Overview

General Information

Sample Name:	u8QPnVhq0N.exe
Original Sample Name:	7de990046a20…
Analysis ID:	830804
MD5:	7de990046a20…
SHA1:	55ebccd35c23…
SHA256:	ebce15ad53b9…
Tags:	32 exe Formbook trojan
Infos:	



Detection

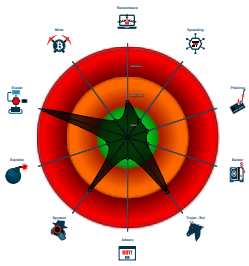


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- 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…
- Performs DNS queries to domains w…

Classification



- **System is w10x64**
- u8QPnVhq0N.exe (PID: 5836 cmdline: C:\Users\user\Desktop\u8QPnVhq0N.exe MD5: 7DE990046A20E6666627273589B014A5)
  - mcwfy.exe (PID: 5952 cmdline: "C:\Users\user\AppData\Local\Temp\mcwfy.exe" C:\Users\user\AppData\Local\Temp\ytljtt.f MD5: 6CB712E482D150A185F713D75314A75A)
    - conhost.exe (PID: 5936 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - mcwfy.exe (PID: 4964 cmdline: C:\Users\user\AppData\Local\Temp\mcwfy.exe MD5: 6CB712E482D150A185F713D75314A75A)
      - explorer.exe (PID: 3324 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - autoconv.exe (PID: 2832 cmdline: C:\Windows\SysWOW64\autoconv.exe MD5: 4506BE56787EDCD771A351C10B5AE3B7)
        - cmstp.exe (PID: 5232 cmdline: C:\Windows\SysWOW64\cmstp.exe MD5: 4833E65ED211C7F118D4A11E6FB58A09)
- **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
00000003.00000002.361208868.0000000000400000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000003.00000002.361208868.0000000000400000.00000040.80000000.00040000.00000000.sdmp	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:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000003.00000002.361208868.0000000000400000.00000040.80000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x19f18:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x199b4:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1a01a:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1a192:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xc83d:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x18bff:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1fcaa:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x20c5d:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000002.361529431.00000000009F0000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000003.00000002.361529431.00000000009F0000.00000040.10000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x1f0e0:$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.mcwfy.exe.400000.0.unpack	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
3.2.mcwfy.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:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
3.2.mcwfy.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x19118:$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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.mcwfy.exe.400000.0.raw.unpack	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
3.2.mcwfy.exe.400000.0.raw.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x20f03:$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

No Snort rule has matched

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)

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)

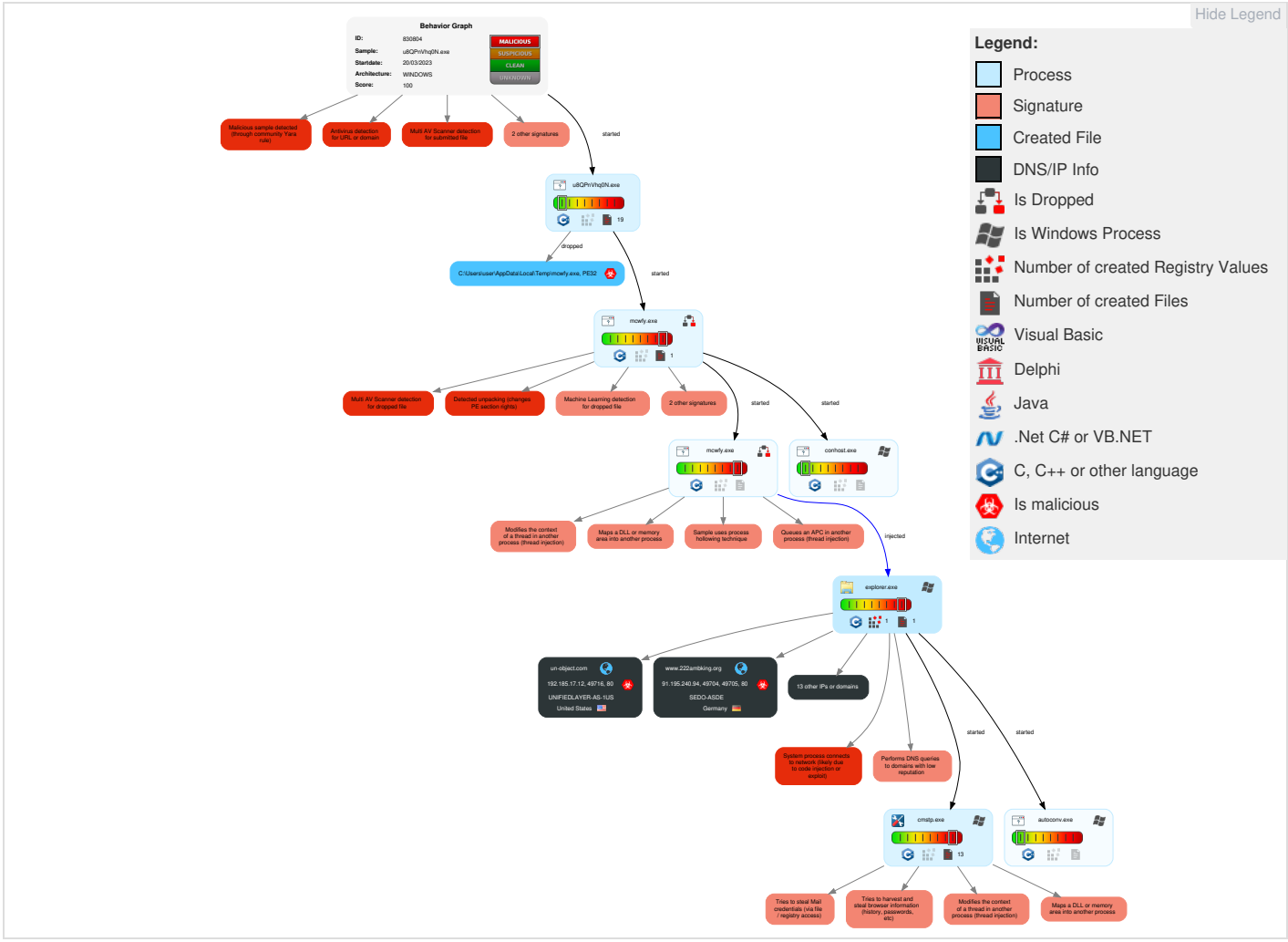
Remote Access Functionality

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	1 Input Capture	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 Input Capture	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	1 Clipboard Data	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

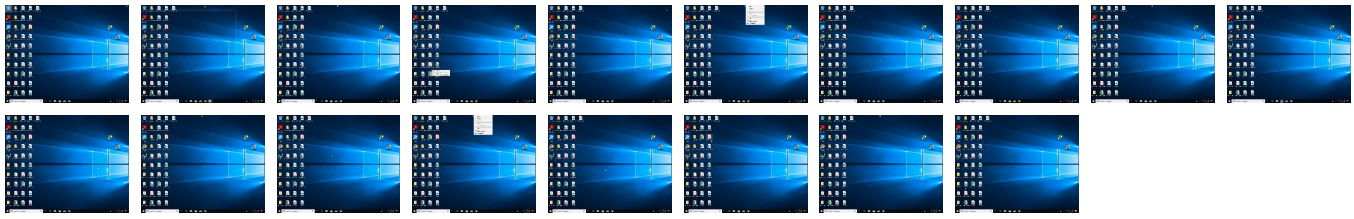
Behavior Graph



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
u8QPnVhq0N.exe	46%	ReversingLabs	Win32.Trojan.Nsisx	
u8QPnVhq0N.exe	49%	Virustotal		Browse
u8QPnVhq0N.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\mcwfy.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\mcwfy.exe	33%	ReversingLabs	Win32.Trojan.Lazy	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.cmstp.exe.12a0000.1.unpack	100%	Avira	HEUR/AGEN.1252160		Download File
3.2.mcwfy.exe.a30000.2.unpack	100%	Avira	HEUR/AGEN.1252160		Download File
3.2.mcwfy.exe.6d4700.1.unpack	100%	Avira	HEUR/AGEN.1252160		Download File
3.2.mcwfy.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
1.2.mcwfy.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
www.energyservicestation.com	0%	Virustotal		Browse
www.thewildphotographer.co.uk	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.ecomofietsen.com	0%	Avira URL Cloud	safe	
http://www.germanreps.com	0%	Avira URL Cloud	safe	
http://www.thedivinerudraksha.com	0%	Avira URL Cloud	safe	
http://www.shapshit.xyz	0%	Avira URL Cloud	safe	
http://www.younrock.com/u2kb/?X51Qjm=05tPwqSdqXO2xf32BHQi8E1nUfoFa2c80hhB3sQ3FFDNPs5AZDU6EjUymll22Wm	100%	Avira URL Cloud	malware	
http://www.white-hat.uk	0%	Avira URL Cloud	safe	
http://white-hat.uk/u2kb/?X51Qjm=PXfMycAZpTAipct8YsIgv6PR3Y11yPgF2k7967nf/qU1A0mUqq9Jy2mfr4kURdfD0Iy	100%	Avira URL Cloud	malware	
http://www.thewildphotographer.co.uk/u2kb/www.thewildphotographer.co.uk	100%	Avira URL Cloud	malware	
http://www.avisrezervee.com/u2kb/www.avisrezervee.com	100%	Avira URL Cloud	malware	
http://www.thedivinerudraksha.com/u2kb/	100%	Avira URL Cloud	malware	
http://www.mygloballojistik.online	0%	Avira URL Cloud	safe	
http://www.employerseervices.com/u2kb/www.employerseervices.com	0%	Avira URL Cloud	safe	
http://www.gritslab.com/u2kb/www.gritslab.com	100%	Avira URL Cloud	malware	
http://www.energyservicestation.com/u2kb/	100%	Avira URL Cloud	malware	
http://www.gritslab.com/u2kb/?X51Qjm=ydCzFiH7iMWnz6xHMre3IWaEcfnK5+fYQUsmgPEoYCSsyD6HgT3yZXCBsea1O+OKnOGwPNRrrKn2ANadQmZuoq3zmdf3x1nRXg==&w6DN_=E0EQSM0RCb349p	100%	Avira URL Cloud	malware	
http://www.white-hat.uk/u2kb/www.white-hat.uk	100%	Avira URL Cloud	malware	
http://www.energyservicestation.com/u2kb/www.energyservicestation.com	100%	Avira URL Cloud	malware	
http://www.avisrezervee.com	0%	Avira URL Cloud	safe	
http://www.un-object.com/u2kb/	100%	Avira URL Cloud	malware	
http://www.bitservicesltd.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.mygloballojistik.online/u2kb/	0%	Avira URL Cloud	safe	
http://www.shapshit.xyz/u2kb/?X51Qjm=Yd5Rzn4EVOpL1Cl/e5Amzdaa+E7UlYBpl8BtE0ZhlgLGbR5cH1Fns9iDSFPM0EqDoX1il4mP+EMsdt2zebBg7FEeCQ3NU/ifUg==&w6DN_=E0EQSM0RCb349p	100%	Avira URL Cloud	malware	
http://justinmezzell.com	0%	Avira URL Cloud	safe	
http://www.dzyngiri.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.bitservicesltd.com/u2kb/	100%	Avira URL Cloud	malware	
http://www.thewildphotographer.co.uk	0%	Avira URL Cloud	safe	
http://www.gritslab.com/u2kb/	100%	Avira URL Cloud	malware	
http://www.222ambking.org/u2kb/www.222ambking.org	100%	Avira URL Cloud	malware	
http://www.fclaimrewardccpointq.shop/u2kb/	100%	Avira URL Cloud	malware	
http://www.energyservicestation.com/u2kb/?X51Qjm=IK59b/MdFRha+CUVMWpzDpHQ2riuD6F66TLC1fPPNwLnZq29gpb12AWvlZbo17UEh0sBgFvevrMQsuZfYKuAI0Y2tVIkdALeFw==&w6DN_=E0EQSM0RCb349p	100%	Avira URL Cloud	malware	
http://www.employerseervices.com/u2kb/	0%	Avira URL Cloud	safe	
http://www.fclaimrewardccpointq.shop/u2kb/www.fclaimrewardccpointq.shop	100%	Avira URL Cloud	malware	
http://www.younrock.com	0%	Avira URL Cloud	safe	
http://www.energyservicestation.com	0%	Avira URL Cloud	safe	
http://www.avisrezervee.com/u2kb/	100%	Avira URL Cloud	malware	
http://www.un-object.com/u2kb/www.un-object.com	100%	Avira URL Cloud	malware	
http://www.shapshit.xyz/u2kb/	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://www.bitservicesltd.com/u2kb/?X51Qjm=rr+sOBvEXsBdGevUkZEAvniGWrNxzC1YNHmXivr92FQhRIIYsedRhL+YGaN2VCieGtjtLTUTzUqxDX3Wf7WovfMRM9ceCuTm3Q==&w6DN_=E0EQSM0RCb349p	100%	Avira URL Cloud	malware	
http://www.mygloballojistik.online/u2kb/www.mygloballojistik.online	0%	Avira URL Cloud	safe	
http://www.thedivinerudraksha.com/u2kb/www.thedivinerudraksha.com	100%	Avira URL Cloud	malware	
http://https://alldomains.hosting/	0%	Avira URL Cloud	safe	
http://www.fclaimrewardccpointq.shop	100%	Avira URL Cloud	malware	
http://www.ecomofietsen.com/u2kb/	100%	Avira URL Cloud	malware	
http://https://alldomains.hosting/hosting-webhosting.html	0%	Avira URL Cloud	safe	
http://www.222ambking.org/u2kb/?X51Qjm=IEUpLmGg2fqLmrhwDd0CH8vm0i8ubOQDFcodV2ACJcW4bHSQscR3aN4MRDv2q1O0g2vnwuasF99orDvyVUehJPYRcFQEZ60O6g==&w6DN_=E0EQSM0RCb349p	100%	Avira URL Cloud	malware	
http://www.white-hat.uk/u2kb/?X51Qjm=PXfMycAZpTAipct8Yslgv6PR3Y11yPgF2k7967nf/qU1A0mUqq9Jy2mfr4kURdfD0lyZUuXLnrTzZCke5/3g9z1JjJjKyNNZNw==&w6DN_=E0EQSM0RCb349p	100%	Avira URL Cloud	malware	
http://www.employerseervices.com	0%	Avira URL Cloud	safe	
http://www.222ambking.org/u2kb/	100%	Avira URL Cloud	malware	
http://www.germanreps.com/u2kb/	100%	Avira URL Cloud	malware	
http://www.germanreps.com/u2kb/www.germanreps.com	100%	Avira URL Cloud	malware	
http://www.younrock.com/u2kb/?X51Qjm=05tPwqSdqXO2xf32BHQi8E1nUfoFa2c80hhB3sQ3FFDNPs5AZDU6EjUymll22Wm6Scj5xbzg3GdXyuHgSKqxyFLAdmHecJKz/g==&w6DN_=E0EQSM0RCb349p	100%	Avira URL Cloud	malware	
http://www.younrock.com/u2kb/www.younrock.com	100%	Avira URL Cloud	malware	
http://www.222ambking.org	0%	Avira URL Cloud	safe	
http://thedivinerudraksha.com/u2kb/?X51Qjm=im5SXjRwbJIZeY2yeMVWNNnKg99Etck2UhYi2fNZ2Kf/X7lq2SPR1Q6pR	100%	Avira URL Cloud	malware	
http://www.younrock.com/u2kb/	100%	Avira URL Cloud	malware	
http://www.shapshit.xyz/u2kb/www.shapshit.xyz	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	
http://www.un-object.com	0%	Avira URL Cloud	safe	
http://www.thedivinerudraksha.com/u2kb/?X51Qjm=im5SXjRwbJIZeY2yeMVWNNnKg99Etck2UhYi2fNZ2Kf/X7lq2SPR1Q6pROq8Gck3yLtOH/fXnE++yuD9U7pvtIMkBqNJDo2oag==&w6DN_=E0EQSM0RCb349p	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	81.17.29.149	true	true	• 1%, Virustotal, Browse	unknown
www.energyservicestation.com	213.145.228.111	true	true	• 0%, Virustotal, Browse	unknown
www.thewildphotographer.co.uk	72.14.185.43	true	true	• 0%, Virustotal, Browse	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.thedivinerudraksha.com/u2kb/	true	• Avira URL Cloud: malware	unknown
http://www.energyservicestation.com/u2kb/	true	• Avira URL Cloud: malware	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.gritslab.com/u2kb/?X51Qjm=ydCzFiH7iMWnz6xHMre3IWaEcfnK5+fYQUsmgPEoYCSsyD6HgT3yZXCBsea1O+OKnOGwPNRrrKn2ANadQmZuoq3zmdf3x1nRXg==&w6DN_=E0EQSM0RCb349p	true	• Avira URL Cloud: malware	unknown
http://www.un-object.com/u2kb/	true	• Avira URL Cloud: malware	unknown
http://www.shapshit.xyz/u2kb/?X51Qjm=Yd5Rzn4EVOpL1Cl/e5Amzdaa+E7UlYBpl8BtE0ZhlgLGbR5cH1Fns9iDSFPM0EqDoX1il4mP+EMsdt2zebBg7FEeCQ3NU/ifUg==&w6DN_=E0EQSM0RCb349p	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.energyservicestation.com/u2kb/?X51Qjm=IK59b/MdFRha+CUVMWpzDpHQ2riuD6F66TLC1fPPNwLnZq29gpb12AWvlZbo17UEh0sBgFvevrMQsuZfYKuAI0Y2tVIkdALeFw==&w6DN_=E0EQSM0RCb349p	true	• Avira URL Cloud: malware	unknown
http://www.gritslab.com/u2kb/	true	• Avira URL Cloud: malware	unknown
http://www.bitservicesltd.com/u2kb/?X51Qjm=rr+sOBvEXsBdGevUkZEAvniGWrNxzC1YNHmXivr92FQhRIIYsedRhL+YGaN2VCieGtjtLTUTzUqxDX3Wf7WovfMRM9ceCuTm3Q==&w6DN_=E0EQSM0RCb349p	true	• Avira URL Cloud: malware	unknown
http://www.shapshit.xyz/u2kb/	true	• Avira URL Cloud: malware	unknown
http://www.white-hat.uk/u2kb/?X51Qjm=PXfMycAZpTAipct8Yslgv6PR3Y11yPgF2k7967nf/qU1A0mUqq9Jy2mfr4kURdfD0lyZUuXLnrTzZCke5/3g9z1JjJjKyNNZNw==&w6DN_=E0EQSM0RCb349p	true	• Avira URL Cloud: malware	unknown
http://www.222ambking.org/u2kb/?X51Qjm=IEUpLmGg2fqLmrhwDd0CH8vm0i8ubOQDFcodV2ACJcW4bHSQscR3aN4MRDv2q1O0g2vnwuasF99orDvyVUehJPYRcFQEZ60O6g==&w6DN_=E0EQSM0RCb349p	true	• Avira URL Cloud: malware	unknown
http://www.222ambking.org/u2kb/	true	• Avira URL Cloud: malware	unknown
http://www.younrock.com/u2kb/?X51Qjm=05tPwqSdqXO2xf32BHQi8E1nUfoFa2c80hhB3sQ3FFDNPs5AZDU6EjUymll22Wm6Scj5xbzg3GdXyuHgSKqxyFLAdmHecJKz/g==&w6DN_=E0EQSM0RCb349p	true	• Avira URL Cloud: malware	unknown
http://www.younrock.com/u2kb/	true	• Avira URL Cloud: malware	unknown
http://www.thedivinerudraksha.com/u2kb/?X51Qjm=im5SXjRwbJIZeY2yeMVWNNnKg99Etck2UhYi2fNZ2Kf/X7lq2SPR1Q6pROq8Gck3yLtOH/fXnE++yuD9U7pvtIMkBqNJDo2oag==&w6DN_=E0EQSM0RCb349p	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://duckduckgo.com/chrome_newtab	cmstp.exe, 00000006.00000003.402261377.000000000B1C000.00000004.00000020.00020000.00000000.sdmp, HI4NJ046K.6.dr	false		high
http://www.avisrezervee.com/u2kb/www.avisrezervee.com	explorer.exe, 00000004.00000003.559686788.000000000F0AA000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000002.581679941.000000000F0AE000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.555754627.000000000F0AA000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.533458319.000000000F0AC000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.562408741.000000000F0AC000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://duckduckgo.com/ac/?q=	HI4NJ046K.6.dr	false		high
http://www.gritslab.com/u2kb/www.gritslab.com	explorer.exe, 00000004.00000003.559686788.000000000F0AA000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000002.581679941.000000000F0AE000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.555754627.000000000F0AA000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.533458319.000000000F0AC000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.562408741.000000000F0AC000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://www.name.com/domain/renew/222ambking.org?utm_source=Sedo_parked_page&utm_medium=button&utm_c	explorer.exe, 00000004.00000002.583702124.00000000159DC000.00000004.80000000.00040000.00000000.sdmp, cmstp.exe, 00000006.00000002.569660808.000000000542C000.00000004.10000000.00040000.00000000.sdmp, cmstp.exe, 00000006.00000002.570208700.000000007150000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://img.sedoparking.com	explorer.exe, 00000004.00000002.58370212 4.00000000159DC000.00000004.80000000.000 40000.00000000.sdmp, cmstp.exe, 00000006 .00000002.569660808.000000000542C000.000 00004.10000000.00040000.00000000.sdmp, c mstp.exe, 00000006.00000002.570208700.00 00000007150000.00000004.00000800.0002000 0.00000000.sdmp	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	cmstp.exe, 00000006.00000003.402261377.0 000000000B1C000.00000004.00000020.000200 00.00000000.sdmp, HI4NJ046K.6.dr	false		high
http://www.thewildphotographer.co.uk/u2kb/www.thewildphotographer.co.uk	explorer.exe, 00000004.00000003.55968678 8.000000000F0AA000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.581679941.000000000F0AE000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.555754627.000000 000F0AA000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000004.0000 0003.533458319.000000000F0AC000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.562408741.000000000F0AC0 00.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.younrock.com/u2kb/?X51Qjm=05tPwqSdqXO2xf32BHQi8E1nUfoFa2c80hhB3sQ3FFDNPs5AZDU6EjUymll22Wm	cmstp.exe, 00000006.00000002.570208700.0 000000007150000.00000004.00000800.000200 00.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.myglobalLojistik.online	explorer.exe, 00000004.00000003.56240874 1.000000000F0AC000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.shapshit.xyz	explorer.exe, 00000004.00000003.56240874 1.000000000F0AC000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.germanreps.com	explorer.exe, 00000004.00000003.56240874 1.000000000F0AC000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ecomofietsen.com	explorer.exe, 00000004.00000003.56240874 1.000000000F0AC000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.thedivinerudraksha.com	explorer.exe, 00000004.00000003.56240874 1.000000000F0AC000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.white-hat.uk/u2kb/www.white-hat.uk	explorer.exe, 00000004.00000003.55968678 8.000000000F0AA000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.581679941.000000000F0AE000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.555754627.000000 000F0AA000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000004.0000 0003.533458319.000000000F0AC000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.562408741.000000000F0AC0 00.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.energyservicestation.com/u2kb/www.energyservicestation.com	explorer.exe, 00000004.00000003.55968678 8.000000000F0AA000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.581679941.000000000F0AE000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.555754627.000000 000F0AA000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000004.0000 0003.533458319.000000000F0AC000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.562408741.000000000F0AC0 00.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://white-hat.uk/u2kb/?X51Qjm=PXfMycAZpTAipct8YsIgv6PR3Y11yPgF2k7967nf/qU1A0mUqq9Jy2mfr4kURdfD0Iy	explorer.exe, 00000004.00000002.58370212 4.0000000015526000.00000004.80000000.000 40000.00000000.sdmp, cmstp.exe, 00000006 .00000002.569660808.0000000004F76000.000 00004.10000000.00040000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://www.white-hat.uk	explorer.exe, 00000004.00000003.56240874 1.000000000F0AC000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

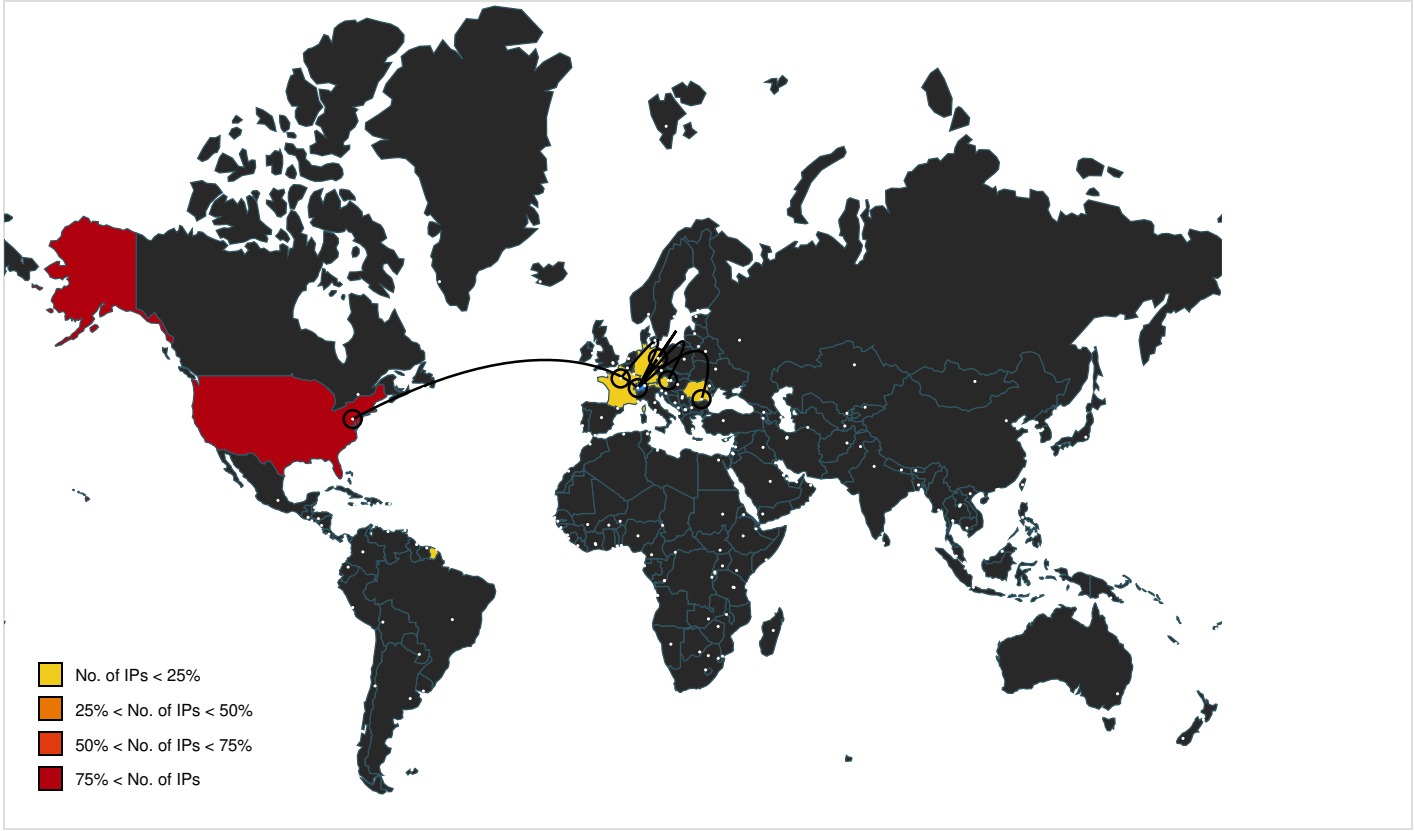
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.employerseervices.com/u2kb/www.employerseervices.com	explorer.exe, 00000004.00000003.55968678 8.000000000F0AA000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.581679941.000000000F0AE000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.555754627.000000 000F0AA000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000004.0000 0003.533458319.000000000F0AC000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.562408741.000000000F0AC0 00.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.dzyngiri.com	explorer.exe, 00000004.00000002.58370212 4.0000000016024000.00000004.80000000.000 40000.00000000.sdmp, cmstp.exe, 00000006 .00000002.569660808.0000000005A74000.000 00004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.myglobalIojistik.online/u2kb/	explorer.exe, 00000004.00000003.55968678 8.000000000F0AA000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.581679941.000000000F0AE000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.555754627.000000 000F0AA000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000004.0000 0003.533458319.000000000F0AC000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.562408741.000000000F0AC0 00.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.avisrezervee.com	explorer.exe, 00000004.00000003.56240874 1.000000000F0AC000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bitservicesltd.com	explorer.exe, 00000004.00000003.56240874 1.000000000F0AC000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://justinmezzell.com	explorer.exe, 00000004.00000002.58370212 4.0000000016024000.00000004.80000000.000 40000.00000000.sdmp, cmstp.exe, 00000006 .00000002.569660808.0000000005A74000.000 00004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.white-hat.uk/u2kb/	explorer.exe, 00000004.00000003.55968678 8.000000000F0AA000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.581679941.000000000F0AE000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.555754627.000000 000F0AA000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000004.0000 0003.533458319.000000000F0AC000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.562408741.000000000F0AC0 00.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://alldomains.hosting/domain-registrieren.html	explorer.exe, 00000004.00000002.58370212 4.0000000015B6E000.00000004.80000000.000 40000.00000000.sdmp, cmstp.exe, 00000006 .00000002.569660808.00000000055BE000.000 00004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.gritslab.com	explorer.exe, 00000004.00000003.56240874 1.000000000F0AC000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.thewildphotographer.co.uk	explorer.exe, 00000004.00000003.56240874 1.000000000F0AC000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fclaimrewardccpointq.shop/u2kb/www.fclaimrewardccpointq.shop	explorer.exe, 00000004.00000003.55968678 8.000000000F0AA000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.581679941.000000000F0AE000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.555754627.000000 000F0AA000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000004.0000 0003.533458319.000000000F0AC000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.562408741.000000000F0AC0 00.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.222ambking.org/u2kb/www.222ambking.org	explorer.exe, 00000004.00000003.55968678 8.000000000F0AA000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.581679941.000000000F0AE000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.555754627.000000 000F0AA000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000004.0000 0003.533458319.000000000F0AC000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.562408741.000000000F0AC0 00.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.fclaimrewardccpointq.shop/u2kb/	explorer.exe, 00000004.00000003.55968678 8.000000000F0AA000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.581679941.000000000F0AE000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.555754627.000000 000F0AA000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000004.0000 0003.533458319.000000000F0AC000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.562408741.000000000F0AC0 00.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000004.00000003.56196897 1.000000000ED28000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.566841892.0000000000921000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.344218674.000000 000ED28000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000004.0000 0002.580393358.000000000ED28000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.320444720.000000000091F0 00.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.energyservicestation.com	explorer.exe, 00000004.00000003.56240874 1.000000000F0AC000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	cmstp.exe, 00000006.00000003.402261377.0 000000000B1C000.00000004.00000020.000200 00.00000000.sdmp, HI4NJ046K.6.dr	false		high
http://www.employerseervices.com/u2kb/	explorer.exe, 00000004.00000003.55968678 8.000000000F0AA000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.581679941.000000000F0AE000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.555754627.000000 000F0AA000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000004.0000 0003.533458319.000000000F0AC000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.562408741.000000000F0AC0 00.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.younrock.com	explorer.exe, 00000004.00000003.56240874 1.000000000F0AC000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	HI4NJ046K.6.dr	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	cmstp.exe, 00000006.00000003.402261377.0 000000000B1C000.00000004.00000020.000200 00.00000000.sdmp, HI4NJ046K.6.dr	false		high
http://nsis.sf.net/NSIS_ErrorError	u8QPnVhq0N.exe	false		high
http://www.un-object.com/u2kb/www.un-object.com	explorer.exe, 00000004.00000003.55968678 8.000000000F0AA000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.581679941.000000000F0AE000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.555754627.000000 000F0AA000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000004.0000 0003.533458319.000000000F0AC000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.562408741.000000000F0AC0 00.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.avisrezervee.com/u2kb/	explorer.exe, 00000004.00000003.55968678 8.000000000F0AA000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.581679941.000000000F0AE000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.555754627.000000 000F0AA000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000004.0000 0003.533458319.000000000F0AC000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.562408741.000000000F0AC0 00.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.mygloballojistik.online/u2kb/www.mygloballojistik.online	explorer.exe, 00000004.00000003.55968678 8.000000000F0AA000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.581679941.000000000F0AE000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.555754627.000000 000F0AA000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000004.0000 0003.533458319.000000000F0AC000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.562408741.000000000F0AC0 00.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	cmstp.exe, 00000006.00000003.402261377.0 000000000B1C000.00000004.00000020.000200 00.00000000.sdmp, HI4NJ046K.6.dr	false		high
http://www.thedivinerudraksha.com/u2kb/www.thedivinerudraksha.com	explorer.exe, 00000004.00000003.55968678 8.000000000F0AA000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.581679941.000000000F0AE000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.555754627.000000 000F0AA000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000004.0000 0003.533458319.000000000F0AC000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.562408741.000000000F0AC0 00.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://alldomains.hosting/	explorer.exe, 00000004.00000002.58370212 4.0000000015B6E000.00000004.80000000.000 40000.00000000.sdmp, cmstp.exe, 00000006 .00000002.569660808.00000000055BE000.000 00004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fclaimrewardccpointq.shop	explorer.exe, 00000004.00000003.56240874 1.000000000F0AC000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://www.sedo.com/services/parking.php3	cmstp.exe, 00000006.00000002.570208700.0 000000007150000.00000004.00000800.000200 00.00000000.sdmp	false		high
http://https://ac.ecosia.org/autocomplete?q=	HI4NJ046K.6.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfp	cmstp.exe, 00000006.00000003.402261377.0 000000000B1C000.00000004.00000020.000200 00.00000000.sdmp, HI4NJ046K.6.dr	false		high
http://www.ecomofietsen.com/u2kb/	explorer.exe, 00000004.00000003.55968678 8.000000000F0AA000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.581679941.000000000F0AE000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.555754627.000000 000F0AA000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000004.0000 0003.533458319.000000000F0AC000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.562408741.000000000F0AC0 00.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://alldomains.hosting/hosting-webhosting.html	explorer.exe, 00000004.00000002.58370212 4.0000000015B6E000.00000004.80000000.000 40000.00000000.sdmp, cmstp.exe, 00000006 .00000002.569660808.00000000055BE000.000 00004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.germanreps.com/u2kb/www.germanreps.com	explorer.exe, 00000004.00000003.55968678 8.000000000F0AA000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.581679941.000000000F0AE000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.555754627.000000 000F0AA000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000004.0000 0003.533458319.000000000F0AC000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.562408741.000000000F0AC0 00.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.germanreps.com/u2kb/	explorer.exe, 00000004.00000003.55968678 8.000000000F0AA000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.581679941.000000000F0AE000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.555754627.000000 000F0AA000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000004.0000 0003.533458319.000000000F0AC000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.562408741.000000000F0AC0 00.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.employerseervices.com	explorer.exe, 00000004.00000003.56240874 1.000000000F0AC000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.younrock.com/u2kb/www.younrock.com	explorer.exe, 00000004.00000003.55968678 8.000000000F0AA000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.581679941.000000000F0AE000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.555754627.000000 000F0AA000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000004.0000 0003.533458319.000000000F0AC000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.562408741.000000000F0AC0 00.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.222ambking.org	explorer.exe, 00000004.00000003.56240874 1.000000000F0AC000.00000004.00000001.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.shapshit.xyz/u2kb/www.shapshit.xyz	explorer.exe, 00000004.00000003.55968678 8.000000000F0AA000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.581679941.000000000F0AE000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.555754627.000000 000F0AA000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000004.0000 0003.533458319.000000000F0AC000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.562408741.000000000F0AC0 00.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://thedivinerudraksha.com/u2kb/?X51Qjm=im5SXjRwbJIZeY2yeMVWNNnKg99Etck2UhYi2fNZ2Kf/X7lq2SPR1Q6pR	explorer.exe, 00000004.00000002.58370212 4.00000000161B6000.00000004.80000000.000 40000.00000000.sdmp, cmstp.exe, 00000006 .00000002.569660808.0000000005C06000.000 00004.10000000.00040000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.ecomofietsen.com/u2kb/www.ecomofietsen.com	explorer.exe, 00000004.00000003.55968678 8.000000000F0AA000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.581679941.000000000F0AE000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.555754627.000000 000F0AA000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000004.0000 0003.533458319.000000000F0AC000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.562408741.000000000F0AC0 00.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://www.un-object.com	explorer.exe, 00000004.00000003.56240874 1.000000000F0AC000.00000004.00000001.000 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.6.dr	false		high
http://www.bitservicesltd.com/u2kb/www.bitservicesltd.com	explorer.exe, 00000004.00000003.55968678 8.000000000F0AA000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000002.581679941.000000000F0AE000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.555754627.000000 000F0AA000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000004.0000 0003.533458319.000000000F0AC000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000003.562408741.000000000F0AC0 00.00000004.00000001.00020000.00000000.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
78.141.192.145	gritslab.com	France		20473	AS-CHOOPAUS	true
161.97.163.8	www.bitservicesltd.com	United States		51167	CONTABODE	true
81.17.29.149	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
72.14.185.43	www.thewildphotographer.co.uk	United States		63949	LINODE-APLinodeLLCUS	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:	830804
Start date and time:	2023-03-20 17:49:26 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 12s
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:	9
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:	u8QPnVhq0N.exe
Original Sample Name:	7de990046a20e6666627273589b014a5.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@10/5@12/10
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 75.9% (good quality ratio 69.9%) • Quality average: 76% • Quality standard deviation: 30.2%
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, WMIADAP.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size 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
17:51:00	API Interceptor	659x 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\cmstp.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):	1.287139506398081
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPF6n/YVuzdqfEwn7PrH944:QS/indc/YVuzdqfEwn7b944
MD5:	292F98D765C8712910776C89ADDE2311
SHA1:	E9F4CCB4577B3E6857C6116C9CBA0F3EC63878C5
SHA-256:	9C63F8321526F04D4CD0CFE11EA32576D1502272FE8333536B9DEE2C3B49825E
SHA-512:	205764B34543D8B53118B3AEA88C550B2273E6EBC880AAD5A106F8DB11D520EB8FD6EFD3DB3B87A4500D287187832FCF18F60556072DD7F5CC947BB7A4E3C3 1
Malicious:	false
Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

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

Process:	C:\Users\user\Desktop\u8QPnVhq0N.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	95232
Entropy (8bit):	6.231519588351459
Encrypted:	false
SSDEEP:	1536:opZrDPCXLdr7zQN/GZGLaYeZjtBaKaedCRVLR8dpxekydJrD9iiU71aC4sWBlVmc:oHTCB7Y/GZGPeZxaGCRVLR9kydI7sCU5
MD5:	6CB712E482D150A185F713D75314A75A
SHA1:	0EE7D4AB0D46C6A668AA500470AAFB632F1ACD99
SHA-256:	C5E0F86A68DCBD03B9A506768F86C385C360D3CF67B9CC0B5760F7B3F1D91F48
SHA-512:	042C3B3A24C35686FA11FBF052A8F278C12535B5F90ECDE5319AA86B8F3616A9A00FBE5E86BD644E2101201B994648BCE2B1F6D6E1F4EDA6C8140F93421CD6E 1
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 33%
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...2'.d.....!.....z.....@.....<k..... .....^.....]..@.....text..... ..`.rdata...e.....f.....@..@.data...l.....j.....@..... ....

C:\Users\user\AppData\Local\Temp\nsl6A3E.tmp

Process:	C:\Users\user\Desktop\u8QPnVhq0N.exe
File Type:	data
Category:	dropped
Size (bytes):	329165
Entropy (8bit):	7.541945169368556
Encrypted:	false
SSDEEP:	6144:WVez7cuIYLUvLfkWAdTEkQUOM1sXFQveBUQZKQldIDMzCu/GZVZxML7L2+P:WKcsCftAdTEarq3BUQZKQfuMzCu/QZOS
MD5:	4ED3CB08EC2E744A786A87B5FEA1AA59
SHA1:	76A5A491D05D504A367C19F0E9669BAA474A8D12
SHA-256:	A3710AFDDF05886219EB7EBA3A85F0AD33EAC1BA6C4BB67F7B389C6CDA15875D
SHA-512:	EEA49222FD83CA261685EB282985906AF43B0020960961CA8141446E432D594BEC294EC2A76747D6B9F834ABCD3218CA5A014A769DBB7F3B8959360E8FD5ECD C
Malicious:	false
Preview:	.A.....-.....@.....A.....H..... .....G.....j.....I.....I..... ....

C:\Users\user\AppData\Local\Temp\ortnkgsjk.g	
Process:	C:\Users\user\Desktop\u8QPnVhq0N.exe
File Type:	data
Category:	dropped
Size (bytes):	211209
Entropy (8bit):	**7.998782052319318**
Encrypted:	**true**
SSDEEP:	6144:7Vez7cuIYLUvLfkWAdTEkQUOM1sXFQveBUQZKQlu:7KcsCftAdTEarq3BUQZKQI
MD5:	0A629526F8AEC96658786151E6C3EA06
SHA1:	80B71B17469506F4023F5E3C35715A6A130AC4C5
SHA-256:	D61BEA82FCBA68CFBC5E6BBE882D5E373EAA26C0DD4AD9C5626EE13A780AB546
SHA-512:	848E3A46F2EAEF9656ADF2DAFE618C20BDDB19D98836F43065F219A58D14BEBB554A63B7844560CCF0EF2124F6D51AD2A6D71DA8AA0408EF639D6BB4FFF0A2F4
Malicious:	false
Preview:	...^.1s..E...g..0#YI.!.Dg.,$.K.....#>.....i..^...&..X..\|..,...\1....e.o.5.T`....;...>.Y..m.c.. ..X.}..mV_.6B]D...UQ.H.C.....x..?y..`...`...*.8.....K.z.x.o.;.}Z~]v.TO.....V.{...->i]..4-e.....[m^Bx.N..T!.[.E..yVD.q....."$m..0g.y.^\.B-.U.`.1s...QH.....4.Y....;...-.....@.#>....u.i..^.z.&..X.5|.....\.,.,Mrc?4....w+..'~&lO..5C.Y.*...I...'.5.}a..8/~.UQ.H.C...U<..*m$.xT..eQ...H...^.....j.w[m.H7..B..V.m.....qW.:..{.8....(.}v.....[.^~..,^..u.0.E..yVD....."....0....^\.B-.U.`.1s..QH.....MY....;.....K.....#>.....i..^...&..X.5\|.....\.,.,Mrc?4....w+..'~&lO..5C.Y.*...I..'.5.}a..8/~.UQ.H.C...U<..*m$.xT..eQ...H...^.....j.w[m.H7..B..V.m.....V.{.d.-..(.}{6.....[.^~..,^.Tu.[.E..yVD....."....0....^\.B-.U.`.1s..QH.....MY....;.....K.....#>.....i..^...&..X.5|.....\.,.,Mrc?4....w+..'~&lO..5C.Y.*...I..'.5.}a..8/~.UQ.H.C...U<..*m$.xT..eQ...H...^.....j.w[m.H7..B..V.m.....V.{.d.-..(.}{6.....[.^~..,^.Tu.[.E..yVD.

C:\Users\user\AppData\Local\Temp\ytljtt.f	
Process:	C:\Users\user\Desktop\u8QPnVhq0N.exe
File Type:	data
Category:	dropped
Size (bytes):	5854
Entropy (8bit):	7.162377453768944
Encrypted:	false
SSDEEP:	96:Farc6oY3g/DrYujk2XO5oSwYgCP7Yc3NdN6d35O4pTU15Fn9O2PGiMCmbvrfjXC:FarcRXrhX1S9PPN6d3ZpTU15EJLrLXC
MD5:	452A3EE71E9BA72BB78302A46C6D5B12
SHA1:	F86411F3F43C4351EF651B38A1402C63B90DB7AC
SHA-256:	521E94034E7166D401C6831BFEE91A92848BF821EAE75ADBD857F503C3D42BC2
SHA-512:	0BB5A96F91E37AB5B89A02C2B25D449C27D1A1E25EB42D461D4B52AE2FB067FDF288EF7F7A4C43955BD7A3A1B32CC514F1C4DD27DBFBB6FE6C7916763056DFD3
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..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.926593256630463
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:	u8QPnVhq0N.exe
File size:	299979
MD5:	7de990046a20e6666627273589b014a5
SHA1:	55ebccd35c2329c5816cd0240b0919651ac58321
SHA256:	ebce15ad53b98d7aba7f7544ee947e88f58d696e22ca4bc5d15b2ded37b577ac
SHA512:	850914621b366494bba2a64aef1b3df7c619c7e6bb321a67bc1a1a97bd0182118a1e5648ee48d24449e6341ab7f7989369797114fa521db8c26ccd5eb3386a42
SSDEEP:	6144:PYa6J+5gUNIG+sCfq3V++iY3aub8kFiLGG9qFP2ipkHj3DR7gy7y:PYDghNESPX3ZZq9q1b6DRc
TLSH:	B2542255E6DDC947D8624E306C7FCA25ABE6F9112D740A1B2320AF45B973240E90F3AF
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 00007F07D0BACB2Ah
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

Instruction
add ecx, FFFFFFD0h
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 00007F07D0BACAFAh
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	0xce8	.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	0xce8	0xe00	False	0.4229910714285714 5	data	4.232621117991543	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	0x250	data	English	United States
RT_MANIFEST	0x3b9a8	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

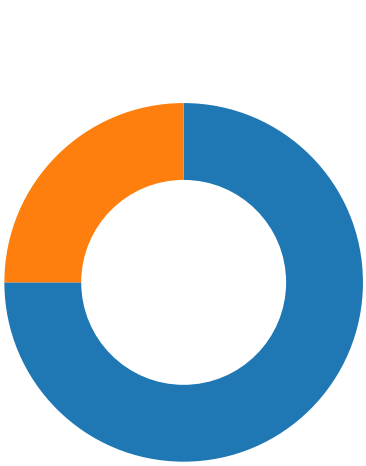
DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, 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

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 17:51:05.667118073 CET	49698	80	192.168.2.5	94.176.104.86
Mar 20, 2023 17:51:05.704344034 CET	80	49698	94.176.104.86	192.168.2.5
Mar 20, 2023 17:51:05.704581022 CET	49698	80	192.168.2.5	94.176.104.86
Mar 20, 2023 17:51:05.712644100 CET	49698	80	192.168.2.5	94.176.104.86
Mar 20, 2023 17:51:05.752857924 CET	80	49698	94.176.104.86	192.168.2.5
Mar 20, 2023 17:51:05.980328083 CET	80	49698	94.176.104.86	192.168.2.5
Mar 20, 2023 17:51:05.980354071 CET	80	49698	94.176.104.86	192.168.2.5
Mar 20, 2023 17:51:05.980566025 CET	49698	80	192.168.2.5	94.176.104.86
Mar 20, 2023 17:51:05.980846882 CET	49698	80	192.168.2.5	94.176.104.86
Mar 20, 2023 17:51:06.017899036 CET	80	49698	94.176.104.86	192.168.2.5
Mar 20, 2023 17:51:11.020831108 CET	49699	80	192.168.2.5	78.141.192.145
Mar 20, 2023 17:51:11.048405886 CET	80	49699	78.141.192.145	192.168.2.5
Mar 20, 2023 17:51:11.048645020 CET	49699	80	192.168.2.5	78.141.192.145
Mar 20, 2023 17:51:11.048825026 CET	49699	80	192.168.2.5	78.141.192.145
Mar 20, 2023 17:51:11.076636076 CET	80	49699	78.141.192.145	192.168.2.5
Mar 20, 2023 17:51:11.076663017 CET	80	49699	78.141.192.145	192.168.2.5
Mar 20, 2023 17:51:11.076689005 CET	80	49699	78.141.192.145	192.168.2.5
Mar 20, 2023 17:51:11.076894999 CET	49699	80	192.168.2.5	78.141.192.145
Mar 20, 2023 17:51:12.550728083 CET	49699	80	192.168.2.5	78.141.192.145
Mar 20, 2023 17:51:13.566399097 CET	49700	80	192.168.2.5	78.141.192.145
Mar 20, 2023 17:51:13.594280005 CET	80	49700	78.141.192.145	192.168.2.5
Mar 20, 2023 17:51:13.594413996 CET	49700	80	192.168.2.5	78.141.192.145
Mar 20, 2023 17:51:13.594569921 CET	49700	80	192.168.2.5	78.141.192.145
Mar 20, 2023 17:51:13.621995926 CET	80	49700	78.141.192.145	192.168.2.5
Mar 20, 2023 17:51:13.622102022 CET	80	49700	78.141.192.145	192.168.2.5
Mar 20, 2023 17:51:13.622251987 CET	80	49700	78.141.192.145	192.168.2.5
Mar 20, 2023 17:51:13.622320890 CET	49700	80	192.168.2.5	78.141.192.145
Mar 20, 2023 17:51:13.628089905 CET	49700	80	192.168.2.5	78.141.192.145
Mar 20, 2023 17:51:13.657012939 CET	80	49700	78.141.192.145	192.168.2.5
Mar 20, 2023 17:51:18.720860004 CET	49702	80	192.168.2.5	161.97.163.8
Mar 20, 2023 17:51:18.747663975 CET	80	49702	161.97.163.8	192.168.2.5
Mar 20, 2023 17:51:18.747811079 CET	49702	80	192.168.2.5	161.97.163.8
Mar 20, 2023 17:51:18.747998953 CET	49702	80	192.168.2.5	161.97.163.8
Mar 20, 2023 17:51:18.774467945 CET	80	49702	161.97.163.8	192.168.2.5
Mar 20, 2023 17:51:18.775655985 CET	80	49702	161.97.163.8	192.168.2.5
Mar 20, 2023 17:51:18.775684118 CET	80	49702	161.97.163.8	192.168.2.5
Mar 20, 2023 17:51:18.775814056 CET	49702	80	192.168.2.5	161.97.163.8
Mar 20, 2023 17:51:20.257500887 CET	49702	80	192.168.2.5	161.97.163.8
Mar 20, 2023 17:51:21.286931038 CET	49703	80	192.168.2.5	161.97.163.8
Mar 20, 2023 17:51:21.314835072 CET	80	49703	161.97.163.8	192.168.2.5
Mar 20, 2023 17:51:21.315018892 CET	49703	80	192.168.2.5	161.97.163.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 17:51:21.315146923 CET	49703	80	192.168.2.5	161.97.163.8
Mar 20, 2023 17:51:21.342814922 CET	80	49703	161.97.163.8	192.168.2.5
Mar 20, 2023 17:51:21.343677998 CET	80	49703	161.97.163.8	192.168.2.5
Mar 20, 2023 17:51:21.343713999 CET	80	49703	161.97.163.8	192.168.2.5
Mar 20, 2023 17:51:21.343878984 CET	49703	80	192.168.2.5	161.97.163.8
Mar 20, 2023 17:51:21.344151020 CET	49703	80	192.168.2.5	161.97.163.8
Mar 20, 2023 17:51:21.370907068 CET	80	49703	161.97.163.8	192.168.2.5
Mar 20, 2023 17:51:26.427524090 CET	49704	80	192.168.2.5	91.195.240.94
Mar 20, 2023 17:51:26.446513891 CET	80	49704	91.195.240.94	192.168.2.5
Mar 20, 2023 17:51:26.448134899 CET	49704	80	192.168.2.5	91.195.240.94
Mar 20, 2023 17:51:26.448251963 CET	49704	80	192.168.2.5	91.195.240.94
Mar 20, 2023 17:51:26.468321085 CET	80	49704	91.195.240.94	192.168.2.5
Mar 20, 2023 17:51:26.468364954 CET	80	49704	91.195.240.94	192.168.2.5
Mar 20, 2023 17:51:26.468543053 CET	49704	80	192.168.2.5	91.195.240.94
Mar 20, 2023 17:51:27.964165926 CET	49704	80	192.168.2.5	91.195.240.94
Mar 20, 2023 17:51:28.974808931 CET	49705	80	192.168.2.5	91.195.240.94
Mar 20, 2023 17:51:28.994070053 CET	80	49705	91.195.240.94	192.168.2.5
Mar 20, 2023 17:51:28.994333029 CET	49705	80	192.168.2.5	91.195.240.94
Mar 20, 2023 17:51:28.994477987 CET	49705	80	192.168.2.5	91.195.240.94
Mar 20, 2023 17:51:29.054166079 CET	80	49705	91.195.240.94	192.168.2.5
Mar 20, 2023 17:51:29.079484940 CET	80	49705	91.195.240.94	192.168.2.5
Mar 20, 2023 17:51:29.079541922 CET	80	49705	91.195.240.94	192.168.2.5
Mar 20, 2023 17:51:29.079590082 CET	80	49705	91.195.240.94	192.168.2.5
Mar 20, 2023 17:51:29.079637051 CET	80	49705	91.195.240.94	192.168.2.5
Mar 20, 2023 17:51:29.079684973 CET	80	49705	91.195.240.94	192.168.2.5
Mar 20, 2023 17:51:29.079731941 CET	80	49705	91.195.240.94	192.168.2.5
Mar 20, 2023 17:51:29.079747915 CET	49705	80	192.168.2.5	91.195.240.94
Mar 20, 2023 17:51:29.079782963 CET	80	49705	91.195.240.94	192.168.2.5
Mar 20, 2023 17:51:29.079797983 CET	49705	80	192.168.2.5	91.195.240.94
Mar 20, 2023 17:51:29.079828978 CET	80	49705	91.195.240.94	192.168.2.5
Mar 20, 2023 17:51:29.079874992 CET	80	49705	91.195.240.94	192.168.2.5
Mar 20, 2023 17:51:29.079876900 CET	49705	80	192.168.2.5	91.195.240.94
Mar 20, 2023 17:51:29.079921007 CET	80	49705	91.195.240.94	192.168.2.5
Mar 20, 2023 17:51:29.079973936 CET	49705	80	192.168.2.5	91.195.240.94
Mar 20, 2023 17:51:29.099098921 CET	80	49705	91.195.240.94	192.168.2.5
Mar 20, 2023 17:51:29.099133015 CET	80	49705	91.195.240.94	192.168.2.5
Mar 20, 2023 17:51:29.099155903 CET	80	49705	91.195.240.94	192.168.2.5
Mar 20, 2023 17:51:29.099188089 CET	80	49705	91.195.240.94	192.168.2.5
Mar 20, 2023 17:51:29.099210978 CET	80	49705	91.195.240.94	192.168.2.5
Mar 20, 2023 17:51:29.099232912 CET	80	49705	91.195.240.94	192.168.2.5
Mar 20, 2023 17:51:29.099253893 CET	80	49705	91.195.240.94	192.168.2.5
Mar 20, 2023 17:51:29.099299908 CET	49705	80	192.168.2.5	91.195.240.94
Mar 20, 2023 17:51:29.099364996 CET	49705	80	192.168.2.5	91.195.240.94
Mar 20, 2023 17:51:29.100024939 CET	80	49705	91.195.240.94	192.168.2.5
Mar 20, 2023 17:51:29.102252007 CET	49705	80	192.168.2.5	91.195.240.94
Mar 20, 2023 17:51:29.102482080 CET	49705	80	192.168.2.5	91.195.240.94
Mar 20, 2023 17:51:29.121347904 CET	80	49705	91.195.240.94	192.168.2.5
Mar 20, 2023 17:51:34.198955059 CET	49706	80	192.168.2.5	213.145.228.111
Mar 20, 2023 17:51:34.220103979 CET	80	49706	213.145.228.111	192.168.2.5
Mar 20, 2023 17:51:34.220273018 CET	49706	80	192.168.2.5	213.145.228.111
Mar 20, 2023 17:51:34.220527887 CET	49706	80	192.168.2.5	213.145.228.111
Mar 20, 2023 17:51:34.241683006 CET	80	49706	213.145.228.111	192.168.2.5
Mar 20, 2023 17:51:34.411031961 CET	80	49706	213.145.228.111	192.168.2.5
Mar 20, 2023 17:51:34.411067963 CET	80	49706	213.145.228.111	192.168.2.5
Mar 20, 2023 17:51:34.411088943 CET	80	49706	213.145.228.111	192.168.2.5
Mar 20, 2023 17:51:34.411154032 CET	49706	80	192.168.2.5	213.145.228.111
Mar 20, 2023 17:51:34.418124914 CET	80	49706	213.145.228.111	192.168.2.5
Mar 20, 2023 17:51:34.418153048 CET	80	49706	213.145.228.111	192.168.2.5
Mar 20, 2023 17:51:34.418204069 CET	49706	80	192.168.2.5	213.145.228.111

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 17:51:05.616214037 CET	50295	53	192.168.2.5	8.8.8.8
Mar 20, 2023 17:51:05.659106016 CET	53	50295	8.8.8.8	192.168.2.5
Mar 20, 2023 17:51:10.996087074 CET	60841	53	192.168.2.5	8.8.8.8
Mar 20, 2023 17:51:11.019247055 CET	53	60841	8.8.8.8	192.168.2.5
Mar 20, 2023 17:51:18.648199081 CET	60649	53	192.168.2.5	8.8.8.8
Mar 20, 2023 17:51:18.673597097 CET	53	60649	8.8.8.8	192.168.2.5
Mar 20, 2023 17:51:26.386713982 CET	51441	53	192.168.2.5	8.8.8.8
Mar 20, 2023 17:51:26.421905994 CET	53	51441	8.8.8.8	192.168.2.5
Mar 20, 2023 17:51:34.164959908 CET	49177	53	192.168.2.5	8.8.8.8
Mar 20, 2023 17:51:34.197314024 CET	53	49177	8.8.8.8	192.168.2.5
Mar 20, 2023 17:51:42.216943026 CET	49724	53	192.168.2.5	8.8.8.8
Mar 20, 2023 17:51:42.247035027 CET	53	49724	8.8.8.8	192.168.2.5
Mar 20, 2023 17:51:49.884217978 CET	61452	53	192.168.2.5	8.8.8.8
Mar 20, 2023 17:51:50.032006979 CET	53	61452	8.8.8.8	192.168.2.5
Mar 20, 2023 17:51:58.059444904 CET	65323	53	192.168.2.5	8.8.8.8
Mar 20, 2023 17:51:58.112246037 CET	53	65323	8.8.8.8	192.168.2.5
Mar 20, 2023 17:52:06.919426918 CET	51484	53	192.168.2.5	8.8.8.8
Mar 20, 2023 17:52:07.043114901 CET	53	51484	8.8.8.8	192.168.2.5
Mar 20, 2023 17:52:16.333122969 CET	63446	53	192.168.2.5	8.8.8.8
Mar 20, 2023 17:52:16.358932018 CET	53	63446	8.8.8.8	192.168.2.5
Mar 20, 2023 17:52:17.446403027 CET	56751	53	192.168.2.5	8.8.8.8
Mar 20, 2023 17:52:17.492475033 CET	53	56751	8.8.8.8	192.168.2.5
Mar 20, 2023 17:52:25.764822006 CET	55039	53	192.168.2.5	8.8.8.8
Mar 20, 2023 17:52:25.884392023 CET	53	55039	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 17:51:05.616214037 CET	192.168.2.5	8.8.8.8	0x82a4	Standard query (0)	www.white-hat.uk	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:51:10.996087074 CET	192.168.2.5	8.8.8.8	0x2eff	Standard query (0)	www.gritslab.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:51:18.648199081 CET	192.168.2.5	8.8.8.8	0xa7e2	Standard query (0)	www.bitservicesltd.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:51:26.386713982 CET	192.168.2.5	8.8.8.8	0x32b8	Standard query (0)	www.222ambking.org	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:51:34.164959908 CET	192.168.2.5	8.8.8.8	0x9d86	Standard query (0)	www.energyservicestation.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:51:42.216943026 CET	192.168.2.5	8.8.8.8	0x9c78	Standard query (0)	www.younrock.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:51:49.884217978 CET	192.168.2.5	8.8.8.8	0xcc3a	Standard query (0)	www.thewildphotographer.co.uk	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:51:58.059444904 CET	192.168.2.5	8.8.8.8	0xaf85	Standard query (0)	www.shapshit.xyz	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:52:06.919426918 CET	192.168.2.5	8.8.8.8	0xbcdf	Standard query (0)	www.thedivinerudraksha.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:52:16.333122969 CET	192.168.2.5	8.8.8.8	0x4dc3	Standard query (0)	www.fclaimrewardccpointq.shop	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:52:17.446403027 CET	192.168.2.5	8.8.8.8	0xca52	Standard query (0)	www.fclaimrewardccpointq.shop	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:52:25.764822006 CET	192.168.2.5	8.8.8.8	0xb97b	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 17:51:05.659106016 CET	8.8.8.8	192.168.2.5	0x82a4	No error (0)	www.white-hat.uk	white-hat.uk		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 17:51:05.659106016 CET	8.8.8.8	192.168.2.5	0x82a4	No error (0)	white-hat.uk		94.176.104.86	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:51:11.019247055 CET	8.8.8.8	192.168.2.5	0x2eff	No error (0)	www.gritslab.com	gritslab.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 17:51:11.019247055 CET	8.8.8.8	192.168.2.5	0x2eff	No error (0)	gritslab.com		78.141.192.145	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:51:18.673597097 CET	8.8.8.8	192.168.2.5	0xa7e2	No error (0)	www.bitservicesltd.com		161.97.163.8	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:51:26.421905994 CET	8.8.8.8	192.168.2.5	0x32b8	No error (0)	www.222ambking.org		91.195.240.94	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:51:34.197314024 CET	8.8.8.8	192.168.2.5	0x9d86	No error (0)	www.energyservicestation.com		213.145.228.111	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:51:42.247035027 CET	8.8.8.8	192.168.2.5	0x9c78	No error (0)	www.younrock.com		81.17.29.149	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:51:50.032006979 CET	8.8.8.8	192.168.2.5	0xcc3a	No error (0)	www.thewildphotographer.co.uk		72.14.185.43	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:51:50.032006979 CET	8.8.8.8	192.168.2.5	0xcc3a	No error (0)	www.thewildphotographer.co.uk		72.14.178.174	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:51:50.032006979 CET	8.8.8.8	192.168.2.5	0xcc3a	No error (0)	www.thewildphotographer.co.uk		45.79.19.196	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:51:50.032006979 CET	8.8.8.8	192.168.2.5	0xcc3a	No error (0)	www.thewildphotographer.co.uk		45.56.79.23	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:51:50.032006979 CET	8.8.8.8	192.168.2.5	0xcc3a	No error (0)	www.thewildphotographer.co.uk		45.33.23.183	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:51:50.032006979 CET	8.8.8.8	192.168.2.5	0xcc3a	No error (0)	www.thewildphotographer.co.uk		45.33.2.79	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:51:50.032006979 CET	8.8.8.8	192.168.2.5	0xcc3a	No error (0)	www.thewildphotographer.co.uk		96.126.123.244	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:51:50.032006979 CET	8.8.8.8	192.168.2.5	0xcc3a	No error (0)	www.thewildphotographer.co.uk		173.255.194.134	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:51:50.032006979 CET	8.8.8.8	192.168.2.5	0xcc3a	No error (0)	www.thewildphotographer.co.uk		45.33.30.197	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:51:50.032006979 CET	8.8.8.8	192.168.2.5	0xcc3a	No error (0)	www.thewildphotographer.co.uk		45.33.20.235	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:51:50.032006979 CET	8.8.8.8	192.168.2.5	0xcc3a	No error (0)	www.thewildphotographer.co.uk		45.33.18.44	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:51:50.032006979 CET	8.8.8.8	192.168.2.5	0xcc3a	No error (0)	www.thewildphotographer.co.uk		198.58.118.167	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:51:58.112246037 CET	8.8.8.8	192.168.2.5	0xaf85	No error (0)	www.shapshit.xyz		199.192.30.147	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:52:07.043114901 CET	8.8.8.8	192.168.2.5	0xbcdf	No error (0)	www.thedivinerudraksha.com	thedivinerudraksha.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 17:52:07.043114901 CET	8.8.8.8	192.168.2.5	0xbcdf	No error (0)	thedivinerudraksha.com		85.187.128.34	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:52:16.358932018 CET	8.8.8.8	192.168.2.5	0x4dc3	Name error (3)	www.fclaimrewardccpointq.shop	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 17:52:17.492475033 CET	8.8.8.8	192.168.2.5	0xca52	Name error (3)	www.fclaimrewardccpointq.shop	none	none	A (IP address)	IN (0x0001)	false

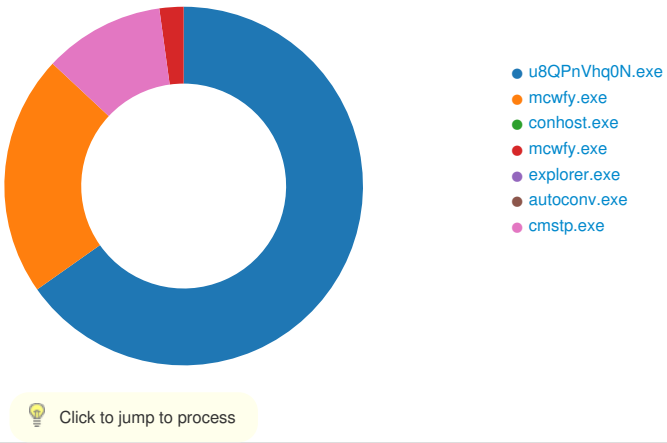
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 17:52:25.884392023 CET	8.8.8.8	192.168.2.5	0xb97b	No error (0)	www.un-object.com	un-object.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 17:52:25.884392023 CET	8.8.8.8	192.168.2.5	0xb97b	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



System Behavior

Analysis Process: u8QPnVhq0N.exe PID: **5836**, Parent PID: **3324**

General

Target ID:	0
Start time:	17:50:22
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\u8QPnVhq0N.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\u8QPnVhq0N.exe
Imagebase:	0x400000
File size:	299979 bytes
MD5 hash:	7DE990046A20E6666627273589B014A5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: mcwfy.exe PID: **5952**, Parent PID: **5836**

General

Target ID:	1
Start time:	17:50:22
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Local\Temp\mcwfy.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\mcwfy.exe" C:\Users\user\AppData\Local\Temp\ytljtt.f
Imagebase:	0x400000
File size:	95232 bytes
MD5 hash:	6CB712E482D150A185F713D75314A75A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 33%, 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\ytljtt.f	unknown	4096	success or wait	1	4077E4	ReadFile
C:\Users\user\AppData\Local\Temp\ytljtt.f	unknown	4096	success or wait	1	4077E4	ReadFile
C:\Users\user\AppData\Local\Temp\ortnkgsjk.g	unknown	190464	success or wait	1	2060A2C	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2060EFF	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2060EFF	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2060EFF	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2060EFF	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2060EFF	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2060EFF	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2060EFF	ReadFile

Analysis Process: conhost.exe PID: **5936**, Parent PID: **5952**

General

Target ID:	2
Start time:	17:50:22

Start date:	20/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7fcd70000
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: mcwfy.exe PID: **4964**, Parent PID: **5952**

General

Target ID:	3
Start time:	17:50:23
Start date:	20/03/2023
Path:	C:\Users\user\AppData\Local\Temp\mcwfy.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\mcwfy.exe
Imagebase:	0x400000
File size:	95232 bytes
MD5 hash:	6CB712E482D150A185F713D75314A75A
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: 00000003.00000002.361208868.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.361208868.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.361208868.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000003.00000002.361529431.00000000009F0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.361529431.00000000009F0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.361529431.00000000009F0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000003.00000002.361277802.0000000000540000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.361277802.0000000000540000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.361277802.0000000000540000.00000040.10000000.00040000.00000000.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: **3324**, Parent PID: **4964**

General

Target ID:	4
Start time:	17:50:31
Start date:	20/03/2023
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff69bc80000
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	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: autoconv.exe PID: **2832**, Parent PID: **3324**

General

Target ID:	5
Start time:	17:50:47
Start date:	20/03/2023
Path:	C:\Windows\SysWOW64\autoconv.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autoconv.exe
Imagebase:	0x13c0000
File size:	851968 bytes
MD5 hash:	4506BE56787EDCD771A351C10B5AE3B7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cmstp.exe PID: **5232**, Parent PID: **3324**

General

Target ID:	6
Start time:	17:50:47
Start date:	20/03/2023
Path:	C:\Windows\SysWOW64\cmstp.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmstp.exe
Imagebase:	0x12a0000
File size:	82944 bytes
MD5 hash:	4833E65ED211C7F118D4A11E6FB58A09
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: 00000006.00000002.566668495.0000000000550000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000006.00000002.566668495.0000000000550000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.566668495.0000000000550000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000006.00000002.567494212.0000000000B40000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000006.00000002.567494212.0000000000B40000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.567494212.0000000000B40000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000006.00000002.567601687.0000000000B70000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000006.00000002.567601687.0000000000B70000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.567601687.0000000000B70000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com

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\mcwfy.exe	cannot delete	1	56C957	NtDeleteFile
C:\Users\user\AppData\Local\Temp\HI4NJ046K	object name not found	1	56C957	NtDeleteFile
C:\Users\user\AppData\Local\Temp\HI4NJ046K	sharing violation	1	56C957	NtDeleteFile
C:\Users\user\AppData\Local\Temp\HI4NJ046K	sharing violation	1	56C957	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	56C927	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