ID: 830301
Sample Name:
SC.028UCCP.exe
Cookbook: default.jbs
Time: 09:06:32
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

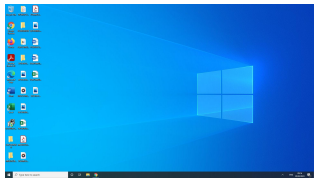
Windows Analysis Report

SC.028UCCP.exe

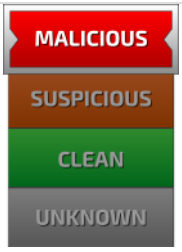
Overview

General Information

Sample Name:	SC.028UCCP.exe
Analysis ID:	830301
MD5:	3f8f4a7f43b562..
SHA1:	1c1931fe8db9b..
SHA256:	0ae741990942...
Infos:	



Detection



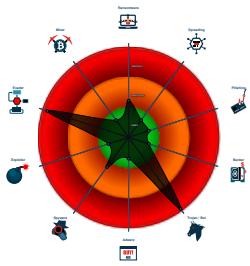
FormBook, GuLoader

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…
- Yara detected GuLoader
- Snort IDS alert for network traffic
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Tries to detect Any.run
- Modifies the prolog of user mode fun…
- Queues an APC in another process …
- Modifies the context of a thread in a…

Classification



Process Tree

- **System is w10x64native**
- SC.028UCCP.exe (PID: 6716 cmdline: C:\Users\user\Desktop\SC.028UCCP.exe MD5: 3F8F4A7F43B5627ED45128BB99F0B471)
  - SC.028UCCP.exe (PID: 2704 cmdline: C:\Users\user\Desktop\SC.028UCCP.exe MD5: 3F8F4A7F43B5627ED45128BB99F0B471)
    - explorer.exe (PID: 4768 cmdline: C:\Windows\Explorer.EXE MD5: 5EA66FF5AE5612F921BC9DA23BAC95F7)
      - mstsc.exe (PID: 1800 cmdline: C:\Windows\SysWOW64\mstsc.exe MD5: B038F39C887BE2A810E20B08613F3B84)
        - cmd.exe (PID: 2296 cmdline: /c del "C:\Users\user\Desktop\SC.028UCCP.exe" MD5: D0FCE3AFA6AA1D58CE9FA336CC2B675B)
          - conhost.exe (PID: 4136 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **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

Name	Description	Attribution	Blogpost URLs	Link

Name	Description	Attribution	Blogpost URLs	Link
CloudEyE, GuLoader	CloudEyE (initially named GuLoader) is a small VB5/6 downloader. It typically downloads RATs/Stealers, such as Agent Tesla, Arkei/Vidar, Formbook, Lokibot, Netwire and Remcos, often but not always from Google Drive. The downloaded payload is xored.	No Attribution	**http://** https://0x00sec.org/t/analyzing-modern-malware-techniques-part-3/18943https://blog.malwarebytes.com/scams/2020/08/sba-phishing-scams-from-malware-to-advanced-social-engineering/https://blog.morphisec.com/guloader-the-rat-downloaderhttps://blog.vincss.net/2020/05/re014-guloader-antivm-techniques.htmlhttps://cert-agid.gov.it/news/malware/tecniche-per-semplificare-lanalisi-del-malware-guloader/	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.cloudeye

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.eliteequinewellness.com/ms12/"
  ],
  "decoy": [
    "familywealthsociety.com",
    "hypnotherapywashington.com",
    "top-promotion.net",
    "tovber.xyz",
    "guiadestudio.com",
    "alibabas.international",
    "campsitecredits.com",
    "18370327105.com",
    "yvhome.net",
    "triknblog.net",
    "limpiezasturisticas.com",
    "khaivisuals.com",
    "amyjohnsonrealtor.com",
    "websponsorzone.net",
    "cobblestonemineralslp.com",
    "women-clothing-64680.com",
    "houtme.com",
    "404shadydale.com",
    "laposadaapts.com",
    "paparazirestaurant.co.uk",
    "helios.moe",
    "kx2662.com",
    "expatsturkiye.com",
    "levelhsealth.com",
    "eeccu.info",
    "princestrustawards.co.uk",
    "lingdangcj.com",
    "goverifyvin.com",
    "innovapay.africa",
    "dvxlbw.top",
    "g20.xn--fiq228c5hs",
    "fdbezd.top",
    "findcar.uk",
    "lordsbury.co.uk",
    "brainmovementinternational.com",
    "slysz.com",
    "thinkdev.africa",
    "garageautosaintthomas.com",
    "bhspharmas.com",
    "likemommy.online",
    "hospitalityhsia.com",
    "friendsofquarepianos.co.uk",
    "chejukongjian.com",
    "drugtestingservices.co.uk",
    "abimpianti.ch",
    "lasvegasestimates.com",
    "expertprestartupbootcamp.co.uk",
    "centersuico.com",
    "consolewars.net",
    "cafemarita.site",
    "findyellowfreightjobs.com",
    "economjchq.space",
    "everwoodpreserving.net",
    "lists-cellphones.life",
    "buckleyassociates.co.uk",
    "littel-italy.com",
    "hangrytots.com",
    "ss777.net",
    "arborfinancialgroup.info",
    "hookspatqp.space",
    "finesttravels.africa",
    "fullhousemarketer.com",
    "conscienciaretroprogresiva.com",
    "arialttnr.com"
  ]
}
```


Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\Unepitomizeds\Indlaansrenter\Patter.Lam	JoeSecurity_GuLoader_5	Yara detected GuLoader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.2969977740.0000000001660000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_5	Yara detected GuLoader	Joe Security	
00000008.00000002.7446412536.0000000004940000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook_1	Yara detected FormBook	Joe Security	
00000008.00000002.7446412536.0000000004940000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000008.00000002.7446412536.0000000004940000.00000004.00000800.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
00000008.00000002.7446412536.0000000004940000.00000004.00000800.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 25 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 188.114.97.3

Timestamp:	192.168.11.20188.114.97.349822802031449 03/20/23-09:10:34.025355
SID:	2031449
Source Port:	49822
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 142.250.186.51

Timestamp:	192.168.11.20142.250.186.5149827802031412 03/20/23-09:11:35.414280
SID:	2031412
Source Port:	49827
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 104.21.39.114

Timestamp:	192.168.11.20104.21.39.11449842802031449 03/20/23-09:15:00.044344
SID:	2031449
Source Port:	49842
Destination Port:	80
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 198.185.159.144	
Timestamp:	192.168.11.20198.185.159.14449830802031412 03/20/23-09:12:15.932254
SID:	2031412
Source Port:	49830
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 13.248.157.32	
Timestamp:	192.168.11.2013.248.157.3249840802031449 03/20/23-09:14:39.545243
SID:	2031449
Source Port:	49840
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 165.160.15.20	
Timestamp:	192.168.11.20165.160.15.2049835802031449 03/20/23-09:13:17.988587
SID:	2031449
Source Port:	49835
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 198.185.159.144	
Timestamp:	192.168.11.20198.185.159.14449830802031453 03/20/23-09:12:15.932254
SID:	2031453
Source Port:	49830
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 81.17.29.147	
Timestamp:	192.168.11.2081.17.29.14749823802031412 03/20/23-09:10:54.265433
SID:	2031412
Source Port:	49823
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 198.185.159.144	
Timestamp:	192.168.11.20198.185.159.14449830802031449 03/20/23-09:12:15.932254
SID:	2031449
Source Port:	49830
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 169.60.232.139	
Timestamp:	192.168.11.20169.60.232.13949844802031449 03/20/23-09:15:33.016841
SID:	2031449
Source Port:	49844
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 142.250.186.51	
Timestamp:	192.168.11.20142.250.186.5149827802031453 03/20/23-09:11:35.414280

SID:	2031453
Source Port:	49827
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 81.17.29.147

Timestamp:	192.168.11.2081.17.29.14749823802031453 03/20/23-09:10:54.265433
SID:	2031453
Source Port:	49823
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 165.160.15.20

Timestamp:	192.168.11.20165.160.15.2049835802031412 03/20/23-09:13:17.988587
SID:	2031412
Source Port:	49835
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 104.21.39.114

Timestamp:	192.168.11.20104.21.39.11449842802031453 03/20/23-09:15:00.044344
SID:	2031453
Source Port:	49842
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 142.250.186.51

Timestamp:	192.168.11.20142.250.186.5149827802031449 03/20/23-09:11:35.414280
SID:	2031449
Source Port:	49827
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 104.21.39.114

Timestamp:	192.168.11.20104.21.39.11449842802031412 03/20/23-09:15:00.044344
SID:	2031412
Source Port:	49842
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 165.160.15.20

Timestamp:	192.168.11.20165.160.15.2049835802031453 03/20/23-09:13:17.988587
SID:	2031453
Source Port:	49835
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Generic .bin download from Dotted Quad - Source IP: 192.168.11.20 - Destination IP: 195.133.40.46

Timestamp:	192.168.11.20195.133.40.4649810802018752 03/20/23-09:09:13.434535
SID:	2018752
Source Port:	49810
Destination Port:	80
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 188.114.97.3	
Timestamp:	192.168.11.20188.114.97.349822802031412 03/20/23-09:10:34.025355
SID:	2031412
Source Port:	49822
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 13.248.157.32	
Timestamp:	192.168.11.2013.248.157.3249840802031453 03/20/23-09:14:39.545243
SID:	2031453
Source Port:	49840
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 188.114.97.3	
Timestamp:	192.168.11.20188.114.97.349822802031453 03/20/23-09:10:34.025355
SID:	2031453
Source Port:	49822
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 13.248.157.32	
Timestamp:	192.168.11.2013.248.157.3249840802031412 03/20/23-09:14:39.545243
SID:	2031412
Source Port:	49840
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 169.60.232.139	
Timestamp:	192.168.11.20169.60.232.13949844802031453 03/20/23-09:15:33.016841
SID:	2031453
Source Port:	49844
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 169.60.232.139	
Timestamp:	192.168.11.20169.60.232.13949844802031412 03/20/23-09:15:33.016841
SID:	2031412
Source Port:	49844
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.11.20 - Destination IP: 81.17.29.147	
Timestamp:	192.168.11.2081.17.29.14749823802031449 03/20/23-09:10:54.265433
SID:	2031449
Source Port:	49823
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

Networking

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

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Yara detected GuLoader

Hooking and other Techniques for Hiding and Protection

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion

Tries to detect Any.run

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

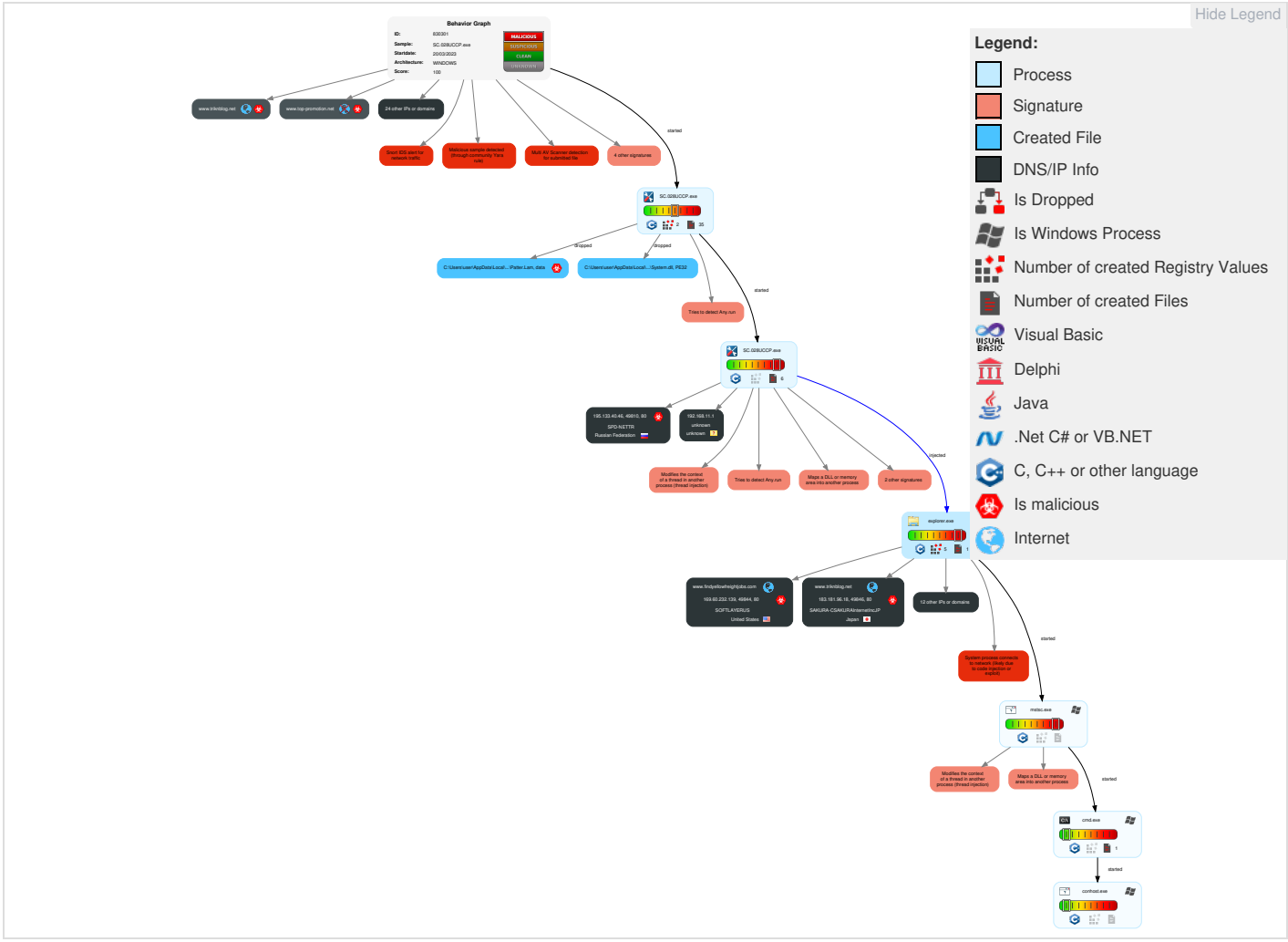
Remote Access Functionality

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	1 DLL Side-Loading	5 1 2 Process Injection	1 Rootkit	1 Credential API Hooking	1 2 1 Security Software Discovery	Remote Services	1 Credential API Hooking	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Shared Modules	Boot or Logon Initialization Scripts	1 DLL Side-Loading	1 Masquerading	LSASS Memory	1 2 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	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 2 Virtualization/Sandbox Evasion	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	1 Clipboard Data	Automated Exfiltration	3 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)	5 1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	2 File and Directory Discovery	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	2 Obfuscated Files or Information	Cached Domain Credentials	4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Software Packing	DCSync	Network Sniffing	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	1 DLL Side-Loading	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

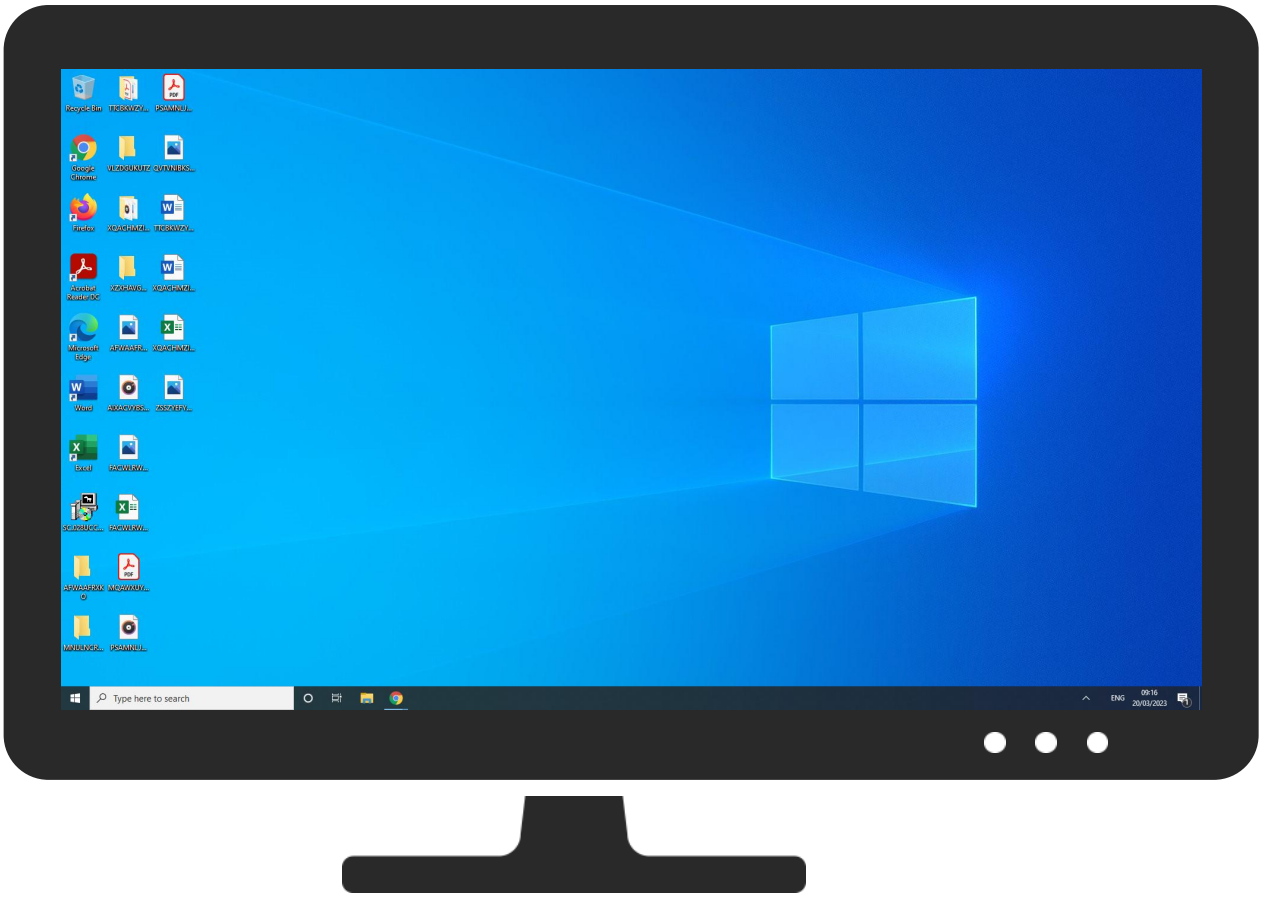
Behavior Graph



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
SC.028UCCP.exe	51%	Virustotal		Browse
SC.028UCCP.exe	33%	ReversingLabs	Win32.Trojan.Generic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsc7F31.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.mstsc.exe.50cf840.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.2.mstsc.exe.2f43518.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.2.explorer.exe.13c7f840.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
amyjohnsonrealtor.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://195.133.40.46/CsPlxqjFa224.bin0	0%	Avira URL Cloud	safe	
http://inference.location.live.com11111111-1111-1111-1111-111111111111https://partnernext-inference.	0%	Avira URL Cloud	safe	
http://195.133.40.46/CsPlxqjFa224.bin3	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.economjchq.space/ms12/?a6A8=p0GhgVm0MHDdp8m&hT=GEgy5f1eXaBWyRpWMBxBbWcEY1MHcvciQ8raEzEPejcDf7w8zE5rQdkYfLeQVLgbPBXb	0%	Avira URL Cloud	safe	
http://www.findyellowfreightjobs.com/ms12/?hT=G6LlIRn2UhCgoj9/NoDttLpXGK4pGwfwFGBz2EgLi6yWMZIZhDysno0vSCCcnKmdw4QQ&UlWl0=MBZlMJlh34CHQ	0%	Avira URL Cloud	safe	
http://www.amyjohnsonrealtor.com/ms12/?a6A8=p0GhgVm0MHDdp8m&hT=KsItnxjux7GTZO7TUTKtm8QLzBBO9NcCFMwewp8NtohxkT6a6dLohlItrjGlglAawoap	0%	Avira URL Cloud	safe	
http://www.hospitalityhsia.com/ms12/?a6A8=p0GhgVm0MHDdp8m&hT=i6mctz/lYNz9iKxESYWey4cK6TMKWjJsbrWHZTfqTQLBeE+tWIBGneMXWwL4vjyr8Zpy	0%	Avira URL Cloud	safe	
http://www.triknblog.net/ms12/?hT=lfzlfRYQFuadehd27GXthwlbqohm3e93HBX/EbDE1KV1AljB6VPD+GnlvvGiXqJ/lo6n&UlWl0=MBZlMJlh34CHQ	0%	Avira URL Cloud	safe	
http://https://www.laposadaapts.com/ms12/?hT=vo99NxIlv9atltQAf5	0%	Avira URL Cloud	safe	
http://www.friendsofquarepianos.co.uk/ms12/?hT=rKVQxN6JSordSXvKLLfEBVUre63ztGesQlGfCtix5zz1Yo/EERiTRw3ZQxg6mz/OTP1R&a6A8=p0GhgVm0MHDdp8m	0%	Avira URL Cloud	safe	
http://195.133.40.46/CsPlxqjFa224.bin	0%	Avira URL Cloud	safe	
http://www.drugtestingservices.co.uk/ms12/?a6A8=p0GhgVm0MHDdp8m&hT=dB2SKHnvFm/evHV5UtSyv0UoYXCrydohCzjDkTmDf/VJc0uDcAnYtxnT/Jo2TNbLuMGT	0%	Avira URL Cloud	safe	
http://www.gopher.ftp://ftp.	0%	Avira URL Cloud	safe	
http://https://excel.office.coma	0%	Avira URL Cloud	safe	
http://www.conscienciaretroprogresiva.com/ms12/?hT=YOOWDLIFFjmzpH1SAG7YZM+LVKYOCEYmA0eV1woM6pvlajKzKUVwFam52RyaFl1jbOMY&UlWl0=MBZlMJlh34CHQ	0%	Avira URL Cloud	safe	
http://schemas.micro	0%	Avira URL Cloud	safe	
http://195.133.40.46/G	0%	Avira URL Cloud	safe	
http://195.133.40.46/	0%	Avira URL Cloud	safe	
www.eliteequinewellness.com/ms12/	0%	Avira URL Cloud	safe	
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	0%	Avira URL Cloud	safe	
http://195.133.40.46/CsPlxqjFa224.binU	0%	Avira URL Cloud	safe	
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	0%	Avira URL Cloud	safe	
http://www.arialttnr.com/ms12/?hT=aVqkBEdIHBWaW/lsOPNfNUdw5ZC180ox2ANf6BVSo52uRq15en0/dTfjz5sq7L16GRwO&a6A8=p0GhgVm0MHDdp8m	0%	Avira URL Cloud	safe	
http://195.133.40.46/CsPlxqjFa224.bin~	0%	Avira URL Cloud	safe	
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	0%	Avira URL Cloud	safe	
http://www.paparazirestaurant.co.uk/ms12/?a6A8=p0GhgVm0MHDdp8m&hT=qQKx9PCKTcR0X3fJLav3D/FI6bogqcX+QhlqDFXKzmg3lH7RMn/qXLrYouNPLK8mW2//	0%	Avira URL Cloud	safe	
http://www.eliteequinewellness.com/ms12/?hT=3vbl2R1UVlik5qBB6wrenITxXeLVrWa6N7N62KRalH+vVSA16yD/agKPQdEyB3rsS7Yj&a6A8=p0GhgVm0MHDdp8m	0%	Avira URL Cloud	safe	
http://www.lists-cellphones.life/ms12/?hT=XQDAKTxCfPAtZ1kZf5EiiDFWaFS1BQmSMuwLBzPPFACL8OgktJOl440l6bHrpdhUiEnu&a6A8=p0GhgVm0MHDdp8m	0%	Avira URL Cloud	safe	
http://www.garageautosaintthomas.com/ms12/?hT=rnwHnBjC2B91WSvUx5IF3sWIhMPrpsyX3rQSnskEXaZlLwDtCWtuXGHAHocTRNCypERK&a6A8=p0GhgVm0MHDdp8m	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.lists-cellphones.life	104.21.39.114	true	true		unknown
www.friendsofquarepianos.co.uk	81.17.29.147	true	true		unknown
www.economjchq.space	188.114.97.3	true	true		unknown
amyjohnsonrealtor.com	13.248.157.32	true	true	• 0%, Virustotal, Browse	unknown
www.hospitalityhsia.com	206.233.207.174	true	true		unknown
conscienciaretroprogresiva.com	34.102.136.180	true	false		unknown
www.triknblog.net	183.181.96.18	true	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.paparazirestaurant.co.uk	192.187.111.221	true	true		unknown
www.findyellowfreightjobs.com	169.60.232.139	true	true		unknown
www.drugtestingservices.co.uk	165.160.15.20	true	true		unknown
www.abimpianti.ch	217.26.48.101	true	true		unknown
ext-sq.squarespace.com	198.185.159.144	true	false		high
ghs.googlehosted.com	142.250.185.211	true	false		unknown
www.goverifyvin.com	unknown	unknown	true		unknown
97.97.242.52.in-addr.arpa	unknown	unknown	true		unknown
www.top-promotion.net	unknown	unknown	true		unknown
www.amyjohnsonrealtor.com	unknown	unknown	true		unknown
www.conscienciaretroprogresiva.com	unknown	unknown	true		unknown
www.eliteequinewellness.com	unknown	unknown	true		unknown
www.arialttnr.com	unknown	unknown	true		unknown
www.garageautosaintthomas.com	unknown	unknown	true		unknown
www.laposadaapts.com	unknown	unknown	true		unknown
www.eeccu.info	unknown	unknown	true		unknown
www.thinkdev.africa	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.friendsofquarepianos.co.uk/ms12/?hT=rKVQxN6JSordSXvKLLfEBVUre63ztGesQlGfCtix5zz1Yo/EERiTRw3ZQxg6mz/OTP1R&a6A8=p0GhgVm0MHDdp8m	true	• Avira URL Cloud: safe	unknown
http://www.hospitalityhsia.com/ms12/?a6A8=p0GhgVm0MHDdp8m&hT=i6mctz/lYNz9iKxESYWey4cK6TMKWjJsbrWHZTfqTQLBeE+tWIBGneMXWwL4vjyr8Zpy	true	• Avira URL Cloud: safe	unknown
http://www.findyellowfreightjobs.com/ms12/?hT=G6LlIRn2UhCgoj9/NoDttLpXGK4pGwfwFGBz2EgLi6yWMZlZhDysno0vSCCcnKmdw4QQ&UlWl0=MBZlMJlh34CHQ	true	• Avira URL Cloud: safe	unknown
http://www.economjchq.space/ms12/?a6A8=p0GhgVm0MHDdp8m&hT=GEgy5f1eXaBWyRpWMBxBbWcEY1MHcvciQ8raEzEPejcDf7w8zE5rQdkYfLeQVLgbPBXb	true	• Avira URL Cloud: safe	unknown
http://www.amyjohnsonrealtor.com/ms12/?a6A8=p0GhgVm0MHDdp8m&hT=KsItnxjux7GTZO7TUTKtm8QLzBBO9NcCFMwewp8NtohxkT6a6dLohIItrjGlglAawoap	true	• Avira URL Cloud: safe	unknown
http://www.triknblog.net/ms12/?hT=lfzlfRYQFuadehd27GXthwlbqohm3e93HBX/EbDE1KV1AljB6VPD+GnlvvGiXqJ/lo6n&UlWl0=MBZlMJlh34CHQ	true	• Avira URL Cloud: safe	unknown
http://195.133.40.46/CsPlxqjFa224.bin	true	• Avira URL Cloud: safe	unknown
http://www.drugtestingservices.co.uk/ms12/?a6A8=p0GhgVm0MHDdp8m&hT=dB2SKHnvFm/evHV5UtSyv0UoYXCrydohCzjDkTmDf/VJc0uDcAnYtxnT/Jo2TNbLuMGT	true	• Avira URL Cloud: safe	unknown
http://www.conscienciaretroprogresiva.com/ms12/?hT=YOOWDLIFFjmzpH1SAG7YZM+LVKYOCEYmA0eV1woM6pvlajKzKUVwFam52RyaFl1jbOMY&UlWl0=MBZlMJlh34CHQ	false	• Avira URL Cloud: safe	unknown
www.eliteequinewellness.com/ms12/	true	• Avira URL Cloud: safe	low
http://www.arialttnr.com/ms12/?hT=aVqkBEdIHBWaW/lsOPNfNUdw5ZC180ox2ANf6BVSo52uRq15en0/dTfjz5sq7L16GRwO&a6A8=p0GhgVm0MHDdp8m	false	• Avira URL Cloud: safe	unknown
http://www.eliteequinewellness.com/ms12/?hT=3vbl2R1UVlik5qBB6wrenITxXeLVrWa6N7N62KRalH+vVSA16yD/agKPQdEyB3rsS7Yj&a6A8=p0GhgVm0MHDdp8m	false	• Avira URL Cloud: safe	unknown
http://www.paparazirestaurant.co.uk/ms12/?a6A8=p0GhgVm0MHDdp8m&hT=qQKx9PCKTcR0X3fJLav3D/FI6bogqcX+QhlqDFXKzmg3lH7RMn/qXLrYouNPLK8mW2//	true	• Avira URL Cloud: safe	unknown
http://www.lists-cellphones.life/ms12/?hT=XQDAKTxCfPAtZ1kZf5EiiDFWaFS1BQmSMuwLBzPPFACL8OgktJOl440l6bHrpdhUiEnu&a6A8=p0GhgVm0MHDdp8m	true	• Avira URL Cloud: safe	unknown
http://www.garageautosaintthomas.com/ms12/?hT=rnwHnBjC2B91WSvUx5IF3sWIhMPrpsyX3rQSnskEXaZlLwDtCWtuXGHAHocTRNCypERK&a6A8=p0GhgVm0MHDdp8m	true	• Avira URL Cloud: safe	unknown

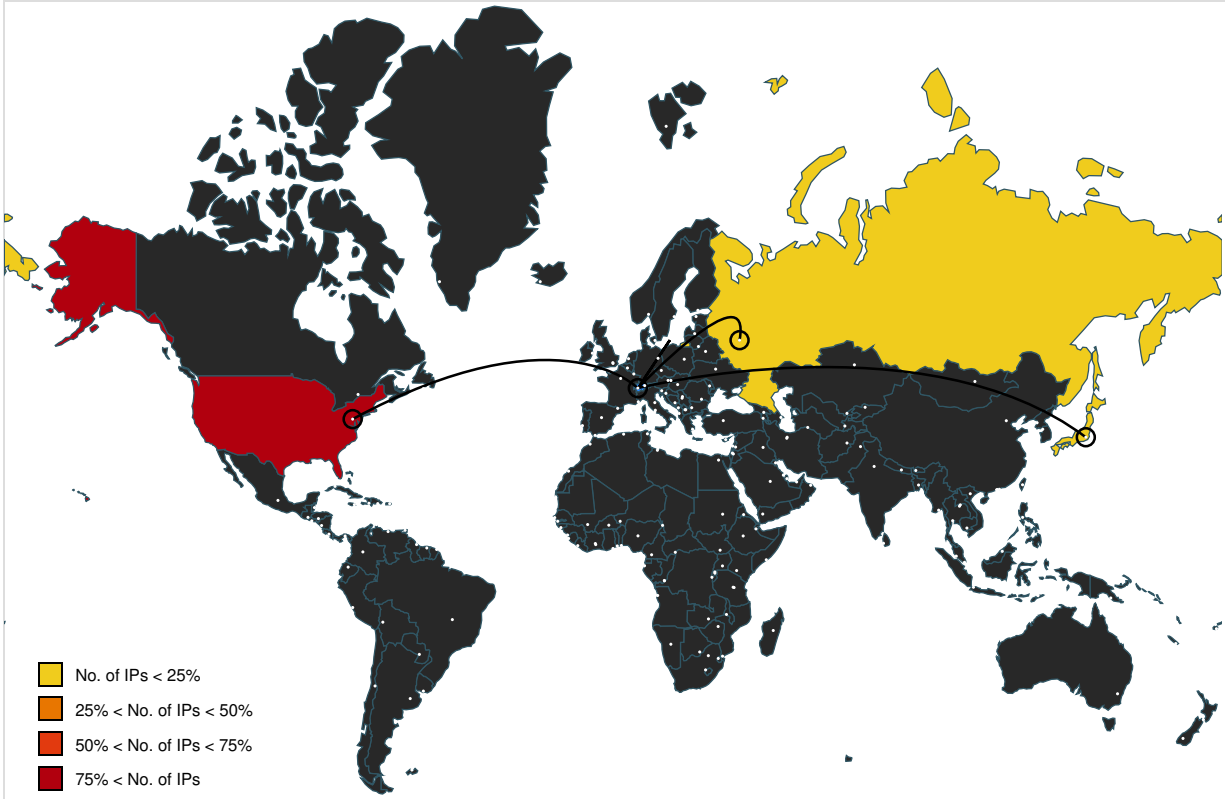
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.msn.com/v1/news/Feed/Windows?	explorer.exe, 00000007.00000000.28980336 99.000000000996D000.00000004.00000001.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://195.133.40.46/CsPlxqjFa224.bin3	SC.028UCCP.exe, 00000006.00000002.3034808343.0000000004C83000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://195.133.40.46/CsPlxqjFa224.bin0	SC.028UCCP.exe, 00000006.00000002.3034808343.0000000004C18000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://inference.location.live.com11111111-1111-1111-1111-111111111111https://partnernext-inference.	SC.028UCCP.exe, 00000006.00000001.27478744116.0000000000649000.00000020.00000001.01000000.00000007.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.laposadaapts.com/ms12/?hT=vo99NxIlv9atltQAf5	explorer.exe, 00000007.00000002.74852271 28.000000001416F000.00000004.80000000.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	SC.028UCCP.exe, 00000000.00000000.2396678614.0000000000409000.00000008.00000001.01000000.00000003.sdmp, SC.028UCCP.exe, 00000000.00000002.2934571208.0000000000409000.00000004.00000001.01000000.00000003.sdmp, SC.028UCCP.exe, 00000006.00000000.2747209758.0000000000409000.00000008.00000001.01000000.00000003.sdmp	false		high
http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd-//W3O//DTD	SC.028UCCP.exe, 00000006.00000001.27478744116.0000000000626000.00000020.00000001.01000000.00000007.sdmp	false		high
http://schemas.micro	explorer.exe, 00000007.00000002.74459592 37.0000000002C70000.00000002.00000001.00040000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.gopher.ftp://ftp.	SC.028UCCP.exe, 00000006.00000001.27478744116.0000000000649000.00000020.00000001.01000000.00000007.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://outlook.com	explorer.exe, 00000007.00000000.29069712 22.000000000D89D000.00000004.00000001.00020000.00000000.sdmp	false		high
http://https://excel.office.coma	explorer.exe, 00000007.00000000.29069712 22.000000000D89D000.00000004.00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://195.133.40.46/G	SC.028UCCP.exe, 00000006.00000002.3034808343.0000000004C7E000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.w3c.org/TR/1999/REC-html401-19991224/frameset.dtd	SC.028UCCP.exe, 00000006.00000001.27478744116.00000000005F2000.00000020.00000001.01000000.00000007.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.msn.com/j	explorer.exe, 00000007.00000003.31159282 29.000000000D7B8000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000007.00000003.4196973708.000000000D7B8000.00000004.00000001.00020000.00000000.sdmp	false		high
http://nsis.sf.net/NSIS_Error	SC.028UCCP.exe, SC.028UCCP.exe, 00000000.00000000.2396678614.0000000000409000.00000008.00000001.01000000.00000003.sdmp, SC.028UCCP.exe, 00000000.00000002.2934571208.0000000000409000.00000004.00000001.01000000.00000003.sdmp, SC.028UCCP.exe, 00000006.00000000.2747209758.0000000000409000.00000008.00000001.01000000.00000003.sdmp	false		high
http://195.133.40.46/	SC.028UCCP.exe, 00000006.00000002.3034808343.0000000004C7B000.00000004.00000020.00020000.00000000.sdmp, SC.028UCCP.exe, 00000006.00000002.3034808343.0000000004C5B000.00000004.00000020.00020000.00000000.sdmp, SC.028UCCP.exe, 00000006.00000002.3034808343.0000000004C7E000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://195.133.40.46/CsPlxqjFa224.binU	SC.028UCCP.exe, 00000006.00000002.3034808343.0000000004C18000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://inference.location.live.net/inferenceservice/v21/Pox/GetLocationUsingFingerprinte1e71f6b-214	SC.028UCCP.exe, 00000006.00000001.27478744116.0000000000649000.00000020.00000001.01000000.00000007.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.w3c.org/TR/1999/REC-html401-19991224/loose.dtd	SC.028UCCP.exe, 00000006.00000001.27478744116.00000000005F2000.00000020.00000001.01000000.00000007.sdmp	false	• Avira URL Cloud: safe	unknown
http://195.133.40.46/CsPlxqjFa224.bin~	SC.028UCCP.exe, 00000006.00000002.3034808343.0000000004C83000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.msn.com/	explorer.exe, 00000007.00000003.31159282 29.000000000D7B8000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 0007.00000003.4196973708.000000000D7B800 0.00000004.00000001.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
165.160.15.20	www.drugtestingservices.co.uk	United States		19574	CSCUS	true
195.133.40.46	unknown	Russian Federation		57844	SPD-NETTR	true
206.233.207.174	www.hospitalityhsia.com	United States		174	COGENT-174US	true
142.250.185.211	ghs.googlehosted.com	United States		15169	GOOGLEUS	false
183.181.96.18	www.triknblog.net	Japan		9371	SAKURA-CSAKURAInternetIncJP	true
192.187.111.221	www.paparazirestaurant.co.uk	United States		33387	NOCIXUS	true
13.248.157.32	amyjohnsonrealtor.com	United States		16509	AMAZON-02US	true
198.185.159.144	ext-sq.squarespace.com	United States		53831	SQUARESPACEUS	false
217.26.48.101	www.abimpianti.ch	Switzerland		29097	HOSTPOINT-ASCH	true
188.114.97.3	www.economjchq.space	European Union		13335	CLOUDFLARENETUS	true
81.17.29.147	www.friendsofquarepianos.co.uk	Switzerland		51852	PLI-ASCH	true
34.102.136.180	conscienciaretroprogresiva.com	United States		15169	GOOGLEUS	false
142.250.186.51	unknown	United States		15169	GOOGLEUS	false
169.60.232.139	www.findyellowfreightjobs.com	United States		36351	SOFTLAYERUS	true
104.21.39.114	www.lists-cellphones.life	United States		13335	CLOUDFLARENETUS	true

Private

IP
192.168.11.1

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830301
Start date and time:	2023-03-20 09:06:32 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Number of analysed new started processes analysed:	17
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:	SC.028UCCP.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@8/4@24/16
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 16% (good quality ratio 15.4%) • Quality average: 80.5% • Quality standard deviation: 25.7%
HCA Information:	• Successful, ratio: 87% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, audiodg.exe, UserOOBEBroker.exe, RuntimeBroker.exe, ShellExperienceHost.exe, WMIADAP.exe, backgroundTaskHost.exe, MoUsoCoreWorker.exe, svchost.exe, UsoClient.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 51.105.236.244, 104.17.167.40, 104.17.168.40, 104.17.169.40, 104.17.170.40, 104.17.171.40
- Excluded domains from analysis (whitelisted): www.rentcafecloudflarecn.com.cdn.cloudflare.net, client.wns.windows.com, wdcpalt.microsoft.com, slscr.update.microsoft.com, wd-prod-cp-eu-west-1-fe.westeurope.cloudapp.azure.com, ctldl.windowsupdate.com, wd-prod-cp.trafficmanager.net, fe3cr.delivery.mp.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtEnumerateKey calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

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\Unepitomizeds\Indlaansrenter\Patter.Lam

Process:	C:\Users\user\Desktop\SC.028UCCP.exe
File Type:	data
Category:	dropped
Size (bytes):	268768
Entropy (8bit):	7.143396451103385
Encrypted:	false
SSDEEP:	6144:qJAA/mPgVn081S1KOqplrh02aq18CUcmQd:TA/moVw1HP02J8CUcVd
MD5:	C6AF2E59D4C09946D5F809241D770F50
SHA1:	266B1073C52D94E9451AA08B2605F2237E5F8A0C
SHA-256:	89E42F99BB457998B2FA3A4D0973ABFE9A39163227F56C8D000CCE44F1EF0070
SHA-512:	B005D4324152790A8BDAAAEE6272A899639FF8D5E1E1FFE1E1219C569F9D271C4A21440F709CA3693A5F80A664501D3AB79EBA81B5B9D07C8870FE5AC15D5124
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_GuLoader_5, Description: Yara detected GuLoader, Source: C:\Users\user\AppData\Local\Temp\Unepitomizeds\Indlaansrenter\Patter.Lam, Author: Joe Security
Preview:	....

C:\Users\user\AppData\Local\Temp\Unepitomizeds\Indlaansrenter\cavil\Ablativers91\ArtDeco_green_7.bmp

Process:	C:\Users\user\Desktop\SC.028UCCP.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 100x100, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=3], baseline, precision 8, 110x110, components 3
Category:	dropped
Size (bytes):	5717
Entropy (8bit):	7.862470085974542
Encrypted:	false
SSDEEP:	96:BSTzREom7JPxQ7OTst5UcVq9JD6EgZEoW249KONYq9iwry9t1Bs6UQJaE424CZ:oXRgtPEOa6+q65Zr87YXwry9tzuCZ
MD5:	B182207A878FA708746DA5A94F08A581
SHA1:	4EF329C2643A9B5E19F491D644A96EF3E7388BE6
SHA-256:	40125E69AA66C655FA44F83BBDEB7E9F24FE81D69CC717651A42C908483FF687
SHA-512:	2368E6533A4D660C08C6F196F38CE2F706C8486AA9E5B1C2413988251184D6A928A348E74DDF0FB098F928D7FCFA4DD71829766E1964E3E5085D642497D034B4
Malicious:	false
Preview:	......JFIF.....d.d.....:Exif..MM.*.....Q.....Q.....aQ.....a.....C.....C.....n.n.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....9o.^....3N>-.~..-.....j.|w.Vu..n..N...#...c.....a...M.$.....n:..m....?..z..1...^_.1.iE..]O.9..|.6.b.E.vVF..h6.i.=|...~.....H.|.^.U.W.@6..}vz..^ON+....M.....{.....2OZ. .=..@w,..c#..`s.A>....O.<.iw9Y....V...Qx_...@6..';Bg.;...J~...2.#.....~.2:..#..0k.6.K...[k.V....>c.98.-..=..Z&...W.:.....

C:\Users\user\AppData\Local\Temp\Unepitomizeds\Indlaansrenter\cavil\Ablativers91\Patronymens.Hov230	
Process:	C:\Users\user\Desktop\SC.028UCCP.exe
File Type:	GTA audio index data (SDT)
Category:	dropped
Size (bytes):	42868
Entropy (8bit):	4.531239376712852
Encrypted:	false
SSDEEP:	768:BmzeD2YSUGt8UN3/hCwqfWCixEmPmXZNIYmhaspQZV:BF9SfyUNvrxEmMAHpQT
MD5:	545F37C048EB23C04FF82F592FB89DEB
SHA1:	9ED7C0D724A7A1C7E38F2A5134D1325B49FCCF25
SHA-256:	DA3CADFEE6D3939C607B6F60B12861931ABD8E7441A2C148C396A38957C7D4DF
SHA-512:	0EB46B15043855818821DD3C60A491E83DF943A30E3BC57E9D37F81AAFF697DFFEF94CE8874A1F61E1E93B7BA2FD740E4FAF7E267BFB1B5B708F1979ED292655
Malicious:	false
Preview:	.....zz.....++.....^^^.....I.....""".R.....6.....ccccccB.....(..}}....>>>>>.B.?.C..J.O..yy.....C.....!!..MMMM.....pp.....P...'.....g.CC...ww.. .....K.....9.;;....X.....W.....6.....%.....+.....ll.....@..CCCC...0.555.....R.....iiii...333.....g..WWW.....M.....D.r.....A.L.[..... 5..,.....P..X.....kkkkk.....w.....VVVV.....?.....+.....gggg.$.....DDDD.??.....m.....r.....`.....; .....bb..ZZ.....z.....O...QQ.....!.....XX.....X.....???.>>>.P.....L....O.{.....v.....ff.....!!!...K....6.....#....eee.....?.....9.....;. .....o.....``.....kkk.....U...;;;.....$.....h....

C:\Users\user\AppData\Local\Temp\nsc7F31.tmp\System.dll	
Process:	C:\Users\user\Desktop\SC.028UCCP.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11264
Entropy (8bit):	5.72460245623286
Encrypted:	false
SSDEEP:	96:3IsUxO9udx4qYp7AJb76BykUbQMtHUOA5Iv+RnsrqeXV+d1g2IW9t2c+cEwF9oug:YVL7ikJb76BQUoUm+RnyXVYO2RvHoug
MD5:	CF85183B87314359488B850F9E97A698
SHA1:	6B6C790037EEC7EBEA4D05590359CB4473F19AEA
SHA-256:	3B6A5CB2A3C091814FCE297C04FB677F72732FB21615102C62A195FDC2E7DFAC
SHA-512:	FE484B3FC89AEED3A6B71B90B90EA11A787697E56BE3077154B6DDC2646850F6C38589ED422FF792E391638A80A778D33F22E891E76B5D65896C6FB4696A2C3E
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....)...m.m.m...k.m.~....j.9..i....I....I.Richm.....PE..L...k..Q.. .....I.....&.....0.....`.....2.....0..P.....P.....0..X.....text..... ..... ..`.rdata..C....0....."".....@..@.data...h....@.....&.....@....reloc..H....P.....(.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.920107350850815
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • 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:	SC.028UCCP.exe
File size:	267392
MD5:	3f8f4a7f43b5627ed45128bb99f0b471
SHA1:	1c1931fe8db9b5df89d39e3121fa72c2a355ded1
SHA256:	0ae741990942bc5b9a51a72dc1cc9f2197b8fe140b76eee9170c3260c00e8656
SHA512:	800a88ff5985f832c73fbada7fa71175531dbe9bd47a93bc8941817e791d8868cfedd4dad2f82604ce06e1e2136821b963d35e23d580edf2d260475eb213ff6f
SSDEEP:	6144:4auq7FPth0P6iM7EFsjSHR58yQlTE1vE1P57hO5FKHJa:HFPr0SirFjC1yP5NO5FKg
TLSH:	AE4412172BE645FFF9D78C72103AEAB3F5BBE6580817144E0B266F7A7D00603092969D
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1p.:u..iu..iu..i...iw..iu..i...i...id..i!2.i...i...it..iRichu..i.....PE..L.....Q.....^.....1.....p....@

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40310b
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x51E3058F [Sun Jul 14 20:09:51 2013 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:	b40f29cd171eb54c01b1dd2683c9c26b

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=synsmaades@Lakeside.Fo, OU="Virksomhedsledelsens Tensionerne ", O=Draconis, L=Saint-Projet, S=Nouvelle-Aquitaine, C=FR
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 20/08/2022 06:31:00 19/08/2025 06:31:00
Subject Chain	• E=synsmaades@Lakeside.Fo, OU="Virksomhedsledelsens Tensionerne ", O=Draconis, L=Saint-Projet, S=Nouvelle-Aquitaine, C=FR
Version:	3
Thumbprint MD5:	82A2F162C13C97C7C5BD9D1EF5E3E352
Thumbprint SHA-1:	0A4EF0B597133BD21B48A5030DE4541818CB48DA
Thumbprint SHA-256:	9B7EDD84EF52310C29E72A78ED7E0EB44C977D6DE7359675C1845C3D1CD29EBC
Serial:	3E36636B7C2A21B05072BFF828C9540A74C9C941

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push ebp
push esi
xor ebx, ebx
push edi
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 00409190h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [00407034h]
push 00008001h
call dword ptr [004070B0h]
push ebx
call dword ptr [0040728Ch]
push 00000008h
mov dword ptr [0042EC58h], eax
call 00007FC42CBF7708h

Instruction
mov dword ptr [0042EBA4h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 00428FE0h
call dword ptr [00407164h]
push 00409180h
push 0042E3A0h
call 00007FC42CBF73B2h
call dword ptr [0040711Ch]
mov ebp, 00434000h
push eax
push ebp
call 00007FC42CBF73A0h
push ebx
call dword ptr [00407114h]
cmp byte ptr [00434000h], 00000022h
mov dword ptr [0042EBA0h], eax
mov eax, ebp
jne 00007FC42CBF499Ch
mov byte ptr [esp+14h], 00000022h
mov eax, 00434001h
push dword ptr [esp+14h]
push eax
call 00007FC42CBF6E4Dh
push eax
call dword ptr [00407220h]
mov dword ptr [esp+1Ch], eax
jmp 00007FC42CBF4A55h
cmp cl, 00000020h
jne 00007FC42CBF4998h
inc eax
cmp byte ptr [eax], 00000020h
je 00007FC42CBF498Ch

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	0x74b0	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x44000	0x10b0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x3fc20	0x1860	.ndata
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	0x7000	0x298	.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	0x5de8	0x5e00	False	0.6791057180851063	data	6.503326078284377	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x12da	0x1400	False	0.4388671875	data	5.095966873256735	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x25c98	0x400	False	0.63671875	data	5.037907617207934	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2f000	0x15000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x44000	0x10b0	0x1200	False	0.3513454861111111	data	4.2798158371727295	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x44238	0x368	Device independent bitmap graphic, 96 x 16 x 4, image size 768	English	United States
RT_ICON	0x445a0	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 640	English	United States
RT_DIALOG	0x44888	0x144	data	English	United States
RT_DIALOG	0x449d0	0x13c	data	English	United States
RT_DIALOG	0x44b10	0x100	data	English	United States
RT_DIALOG	0x44c10	0x11c	data	English	United States
RT_DIALOG	0x44d30	0x60	data	English	United States
RT_GROUP_ICON	0x44d90	0x14	data	English	United States
RT_MANIFEST	0x44da8	0x305	XML 1.0 document, ASCII text, with very long lines (773), with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	Sleep, GetShortPathNameA, GetFullPathNameA, MoveFileA, SetCurrentDirectoryA, GetFileAttributesA, GetLastError, CreateDirectoryA, CompareFileTime, SearchPathA, GetTickCount, GetFileSize, GetModuleFileNameA, GetCurrentProcess, CopyFileA, ExitProcess, SetEnvironmentVariableA, GetWindowsDirectoryA, SetFileAttributesA, lstrcmpiA, SetErrorMode, LoadLibraryA, lstrlenA, lstrcpynA, GetDiskFreeSpaceA, GlobalUnlock, GlobalLock, CreateThread, CreateProcessA, RemoveDirectoryA, CreateFileA, GetTempFileNameA, lstrcpyA, lstrcatA, GetSystemDirectoryA, GetVersion, GetProcAddress, WaitForSingleObject, SetFileTime, CloseHandle, GlobalFree, lstrcmpA, ExpandEnvironmentStringsA, GetExitCodeProcess, GlobalAlloc, GetModuleHandleA, LoadLibraryExA, GetCommandLineA, GetTempPathA, FreeLibrary, FindFirstFileA, FindNextFileA, DeleteFileA, SetFilePointer, ReadFile, FindClose, GetPrivateProfileStringA, WritePrivateProfileStringA, MulDiv, WriteFile, MultiByteToWideChar
USER32.dll	CreateWindowExA, EndDialog, ScreenToClient, GetWindowRect, EnableMenuItem, GetSystemMenu, SetClassLongA, IsWindowEnabled, SetWindowPos, GetSysColor, GetWindowLongA, SetCursor, LoadCursorA, CheckDlgButton, GetMessagePos, LoadBitmapA, CallWindowProcA, IsWindowVisible, CloseClipboard, GetDC, SystemParametersInfoA, RegisterClassA, TrackPopupMenu, AppendMenuA, CreatePopupMenu, GetSystemMetrics, SetDlgItemTextA, GetDlgItemTextA, MessageBoxIndirectA, CharPrevA, DispatchMessageA, PeekMessageA, ReleaseDC, EnableWindow, InvalidateRect, SendMessageA, DefWindowProcA, BeginPaint, GetClientRect, FillRect, DrawTextA, GetClassInfoA, DialogBoxParamA, CharNextA, ExitWindowsEx, DestroyWindow, CreateDialogParamA, SetTimer, GetDlgItem, wsprintfA, SetForegroundWindow, ShowWindow, IsWindow, LoadImageA, SetWindowLongA, SetClipboardData, EmptyClipboard, OpenClipboard, EndPaint, PostQuitMessage, FindWindowExA, SendMessageTimeoutA, SetWindowTextA
GDI32.dll	SelectObject, SetBkMode, CreateFontIndirectA, SetTextColor, DeleteObject, GetDeviceCaps, CreateBrushIndirect, SetBkColor
SHELL32.dll	SHGetSpecialFolderLocation, SHGetPathFromIDListA, SHBrowseForFolderA, SHGetFileInfoA, ShellExecuteA, SHFileOperationA
ADVAPI32.dll	RegCloseKey, RegOpenKeyExA, RegDeleteKeyA, RegDeleteValueA, RegEnumValueA, RegCreateKeyExA, RegSetValueExA, RegQueryValueExA, RegEnumKeyA
COMCTL32.dll	ImageList_Create, ImageList_AddMasked, ImageList_Destroy
ole32.dll	CoCreateInstance, CoTaskMemFree, OleInitialize, OleUninitialize
VERSION.dll	GetFileVersionInfoSizeA, GetFileVersionInfoA, VerQueryValueA

Possible Origin

Language of compilation system	Country where language is spoken	Map

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

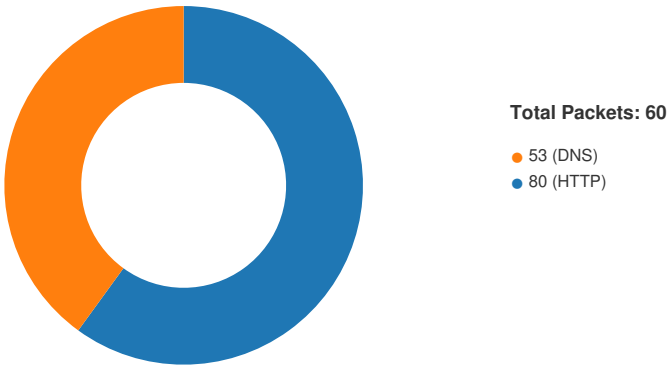
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20188.114.97.349822802031449 03/20/23-09:10:34.025355	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49822	80	192.168.11.20	188.114.97.3
192.168.11.20142.250.186.5149827802031412 03/20/23-09:11:35.414280	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49827	80	192.168.11.20	142.250.186.51
192.168.11.20104.21.39.11449842802031449 03/20/23-09:15:00.044344	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49842	80	192.168.11.20	104.21.39.114
192.168.11.20198.185.159.14449830802031412 03/20/23-09:12:15.932254	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49830	80	192.168.11.20	198.185.159.144
192.168.11.2013.248.157.3249840802031449 03/20/23-09:14:39.545243	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49840	80	192.168.11.20	13.248.157.32
192.168.11.20165.160.15.2049835802031449 03/20/23-09:13:17.988587	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49835	80	192.168.11.20	165.160.15.20
192.168.11.20198.185.159.14449830802031453 03/20/23-09:12:15.932254	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49830	80	192.168.11.20	198.185.159.144
192.168.11.2081.17.29.14749823802031412 03/20/23-09:10:54.265433	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49823	80	192.168.11.20	81.17.29.147
192.168.11.20198.185.159.14449830802031449 03/20/23-09:12:15.932254	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49830	80	192.168.11.20	198.185.159.144
192.168.11.20169.60.232.13949844802031449 03/20/23-09:15:33.016841	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49844	80	192.168.11.20	169.60.232.139
192.168.11.20142.250.186.5149827802031453 03/20/23-09:11:35.414280	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49827	80	192.168.11.20	142.250.186.51
192.168.11.2081.17.29.14749823802031453 03/20/23-09:10:54.265433	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49823	80	192.168.11.20	81.17.29.147
192.168.11.20165.160.15.2049835802031412 03/20/23-09:13:17.988587	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49835	80	192.168.11.20	165.160.15.20
192.168.11.20104.21.39.11449842802031453 03/20/23-09:15:00.044344	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49842	80	192.168.11.20	104.21.39.114
192.168.11.20142.250.186.5149827802031449 03/20/23-09:11:35.414280	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49827	80	192.168.11.20	142.250.186.51

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20104.21.39.11449842802031412 03/20/23-09:15:00.044344	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49842	80	192.168.11.20	104.21.39.114
192.168.11.20165.160.15.2049835802031453 03/20/23-09:13:17.988587	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49835	80	192.168.11.20	165.160.15.20
192.168.11.20195.133.40.4649810802018752 03/20/23-09:09:13.434535	TCP	2018752	ET TROJAN Generic .bin download from Dotted Quad	49810	80	192.168.11.20	195.133.40.46
192.168.11.20188.114.97.349822802031412 03/20/23-09:10:34.025355	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49822	80	192.168.11.20	188.114.97.3
192.168.11.2013.248.157.3249840802031453 03/20/23-09:14:39.545243	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49840	80	192.168.11.20	13.248.157.32
192.168.11.20188.114.97.349822802031453 03/20/23-09:10:34.025355	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49822	80	192.168.11.20	188.114.97.3
192.168.11.2013.248.157.3249840802031412 03/20/23-09:14:39.545243	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49840	80	192.168.11.20	13.248.157.32
192.168.11.20169.60.232.13949844802031453 03/20/23-09:15:33.016841	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49844	80	192.168.11.20	169.60.232.139
192.168.11.20169.60.232.13949844802031412 03/20/23-09:15:33.016841	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49844	80	192.168.11.20	169.60.232.139
192.168.11.2081.17.29.14749823802031449 03/20/23-09:10:54.265433	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49823	80	192.168.11.20	81.17.29.147

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 09:09:13.415043116 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.433906078 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.434035063 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.434535027 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.461829901 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.461865902 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.461916924 CET	80	49810	195.133.40.46	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 09:09:13.461976051 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.461987972 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.461999893 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.462011099 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.462033033 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.462148905 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.462148905 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.462148905 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.462148905 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.462148905 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.462148905 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.462156057 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.462157011 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.462286949 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.462486029 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.462655067 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.480679989 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.480778933 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.480791092 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.480807066 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.480822086 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.480833054 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.480844975 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.480881929 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.480894089 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.481041908 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.481046915 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.481046915 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.481046915 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.481046915 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.481046915 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.481046915 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.481054068 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.481067896 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.481082916 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.481095076 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.481220007 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.481228113 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.481229067 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.481230021 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.481230021 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.481355906 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.481355906 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.481369019 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.481369972 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.481525898 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.481694937 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.502079010 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502176046 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502228975 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502242088 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502254963 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502268076 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.502273083 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502286911 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502300024 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502336025 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502350092 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502365112 CET	80	49810	195.133.40.46	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 09:09:13.502382040 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502439022 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502439022 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.502439976 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502440929 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502440929 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502454996 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502470016 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502500057 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502512932 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502612114 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502614021 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502613068 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.502614021 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502613068 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.502614975 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502613068 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.502615929 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502613068 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.502613068 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.502613068 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.502613068 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.502613068 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.502633095 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502640009 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.502640009 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.502640009 CET	49810	80	192.168.11.20	195.133.40.46
Mar 20, 2023 09:09:13.502648115 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502660990 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502677917 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502695084 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502707958 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502723932 CET	80	49810	195.133.40.46	192.168.11.20
Mar 20, 2023 09:09:13.502742052 CET	80	49810	195.133.40.46	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 09:08:23.342824936 CET	61078	53	192.168.11.20	9.9.9.9
Mar 20, 2023 09:08:23.391607046 CET	53	61078	9.9.9.9	192.168.11.20
Mar 20, 2023 09:09:54.924993038 CET	55152	53	192.168.11.20	1.1.1.1
Mar 20, 2023 09:09:55.175930977 CET	53	55152	1.1.1.1	192.168.11.20
Mar 20, 2023 09:10:13.575550079 CET	51847	53	192.168.11.20	1.1.1.1
Mar 20, 2023 09:10:13.629487038 CET	53	51847	1.1.1.1	192.168.11.20
Mar 20, 2023 09:10:33.993092060 CET	63398	53	192.168.11.20	1.1.1.1
Mar 20, 2023 09:10:34.015582085 CET	53	63398	1.1.1.1	192.168.11.20
Mar 20, 2023 09:10:54.194255114 CET	51926	53	192.168.11.20	1.1.1.1
Mar 20, 2023 09:10:54.252357006 CET	53	51926	1.1.1.1	192.168.11.20
Mar 20, 2023 09:11:14.422035933 CET	65472	53	192.168.11.20	1.1.1.1
Mar 20, 2023 09:11:14.789616108 CET	53	65472	1.1.1.1	192.168.11.20
Mar 20, 2023 09:11:14.790040970 CET	65472	53	192.168.11.20	9.9.9.9
Mar 20, 2023 09:11:15.178378105 CET	53	65472	9.9.9.9	192.168.11.20
Mar 20, 2023 09:11:35.339004993 CET	61823	53	192.168.11.20	1.1.1.1
Mar 20, 2023 09:11:35.402036905 CET	53	61823	1.1.1.1	192.168.11.20
Mar 20, 2023 09:11:55.584259987 CET	54486	53	192.168.11.20	1.1.1.1
Mar 20, 2023 09:11:55.599153996 CET	53	54486	1.1.1.1	192.168.11.20
Mar 20, 2023 09:12:15.752722979 CET	51749	53	192.168.11.20	1.1.1.1
Mar 20, 2023 09:12:15.800843000 CET	53	51749	1.1.1.1	192.168.11.20
Mar 20, 2023 09:12:36.216002941 CET	55453	53	192.168.11.20	1.1.1.1

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 09:12:36.538785934 CET	53	55453	1.1.1.1	192.168.11.20
Mar 20, 2023 09:12:57.117762089 CET	60861	53	192.168.11.20	1.1.1.1
Mar 20, 2023 09:12:57.154711008 CET	53	60861	1.1.1.1	192.168.11.20
Mar 20, 2023 09:13:17.816112995 CET	51176	53	192.168.11.20	1.1.1.1
Mar 20, 2023 09:13:17.829958916 CET	53	51176	1.1.1.1	192.168.11.20
Mar 20, 2023 09:13:38.327482939 CET	64989	53	192.168.11.20	1.1.1.1
Mar 20, 2023 09:13:38.744119883 CET	53	64989	1.1.1.1	192.168.11.20
Mar 20, 2023 09:13:38.744478941 CET	64989	53	192.168.11.20	9.9.9.9
Mar 20, 2023 09:13:39.748574018 CET	64989	53	192.168.11.20	9.9.9.9
Mar 20, 2023 09:13:41.763811111 CET	64989	53	192.168.11.20	9.9.9.9
Mar 20, 2023 09:13:42.112545967 CET	53	64989	9.9.9.9	192.168.11.20
Mar 20, 2023 09:13:42.521053076 CET	53	64989	9.9.9.9	192.168.11.20
Mar 20, 2023 09:13:44.021675110 CET	53	64989	9.9.9.9	192.168.11.20
Mar 20, 2023 09:13:58.229331970 CET	57459	53	192.168.11.20	1.1.1.1
Mar 20, 2023 09:13:59.215681076 CET	53	57459	1.1.1.1	192.168.11.20
Mar 20, 2023 09:14:39.517093897 CET	55398	53	192.168.11.20	1.1.1.1
Mar 20, 2023 09:14:39.532558918 CET	53	55398	1.1.1.1	192.168.11.20
Mar 20, 2023 09:14:59.906671047 CET	61744	53	192.168.11.20	1.1.1.1
Mar 20, 2023 09:15:00.032583952 CET	53	61744	1.1.1.1	192.168.11.20
Mar 20, 2023 09:15:32.548209906 CET	58281	53	192.168.11.20	1.1.1.1
Mar 20, 2023 09:15:32.885806084 CET	53	58281	1.1.1.1	192.168.11.20
Mar 20, 2023 09:15:35.157414913 CET	56934	53	192.168.11.20	1.1.1.1
Mar 20, 2023 09:15:35.175795078 CET	53	56934	1.1.1.1	192.168.11.20
Mar 20, 2023 09:15:55.495990992 CET	60148	53	192.168.11.20	1.1.1.1
Mar 20, 2023 09:15:55.980588913 CET	53	60148	1.1.1.1	192.168.11.20
Mar 20, 2023 09:16:37.346389055 CET	53417	53	192.168.11.20	1.1.1.1

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 09:08:23.342824936 CET	192.168.11.20	9.9.9.9	0x5d5e	Standard query (0)	97.97.242.52.in-addr.arpa	PTR (Pointer record)	IN (0x0001)	false
Mar 20, 2023 09:09:54.924993038 CET	192.168.11.20	1.1.1.1	0x11ac	Standard query (0)	www.paparazirestaurant.co.uk	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:13.575550079 CET	192.168.11.20	1.1.1.1	0x8943	Standard query (0)	www.eliteequinewellness.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:33.993092060 CET	192.168.11.20	1.1.1.1	0x421c	Standard query (0)	www.economjchq.space	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:54.194255114 CET	192.168.11.20	1.1.1.1	0xa29e	Standard query (0)	www.friendsofquarepianos.co.uk	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:11:14.422035933 CET	192.168.11.20	1.1.1.1	0xb1a8	Standard query (0)	www.goverifyvin.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:11:14.790040970 CET	192.168.11.20	9.9.9.9	0xb1a8	Standard query (0)	www.goverifyvin.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:11:35.339004993 CET	192.168.11.20	1.1.1.1	0x4097	Standard query (0)	www.arialtnr.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:11:55.584259987 CET	192.168.11.20	1.1.1.1	0x7a1	Standard query (0)	www.eeccu.info	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:12:15.752722979 CET	192.168.11.20	1.1.1.1	0xe5d7	Standard query (0)	www.garageautosainttthomas.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:12:36.216002941 CET	192.168.11.20	1.1.1.1	0xa35d	Standard query (0)	www.hospitalityhsia.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:12:57.117762089 CET	192.168.11.20	1.1.1.1	0xc5dd	Standard query (0)	www.abimpianti.ch	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:13:17.816112995 CET	192.168.11.20	1.1.1.1	0x7d8	Standard query (0)	www.drugtestingservices.co.uk	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:13:38.327482939 CET	192.168.11.20	1.1.1.1	0xa63c	Standard query (0)	www.thinkdev.africa	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:13:38.744478941 CET	192.168.11.20	9.9.9.9	0xa63c	Standard query (0)	www.thinkdev.africa	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 09:13:39.748574018 CET	192.168.11.20	9.9.9.9	0xa63c	Standard query (0)	www.thinkdev.africa	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:13:41.763811111 CET	192.168.11.20	9.9.9.9	0xa63c	Standard query (0)	www.thinkdev.africa	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:13:58.229331970 CET	192.168.11.20	1.1.1.1	0x8fe7	Standard query (0)	www.top-promotion.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:14:39.517093897 CET	192.168.11.20	1.1.1.1	0x68aa	Standard query (0)	www.amyjohnsonrealtor.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:14:59.906671047 CET	192.168.11.20	1.1.1.1	0x3f09	Standard query (0)	www.lists-cellphones.life	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:15:32.548209906 CET	192.168.11.20	1.1.1.1	0xed83	Standard query (0)	www.findyellowfreightjobs.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:15:35.157414913 CET	192.168.11.20	1.1.1.1	0xc133	Standard query (0)	www.conscienciaretroprogresiva.com	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:15:55.495990992 CET	192.168.11.20	1.1.1.1	0xcbb2	Standard query (0)	www.triknblog.net	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:16:37.346389055 CET	192.168.11.20	1.1.1.1	0x67eb	Standard query (0)	www.laposadaapts.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 09:08:23.391607046 CET	9.9.9.9	192.168.11.20	0x5d5e	Name error (3)	97.97.242.52.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)	false
Mar 20, 2023 09:09:55.175930977 CET	1.1.1.1	192.168.11.20	0x11ac	No error (0)	www.paparazirestaurant.co.uk		192.187.111.221	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:13.629487038 CET	1.1.1.1	192.168.11.20	0x8943	No error (0)	www.eliteequinewellness.com	ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 09:10:13.629487038 CET	1.1.1.1	192.168.11.20	0x8943	No error (0)	ghs.googlehosted.com		142.250.185.211	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:34.015582085 CET	1.1.1.1	192.168.11.20	0x421c	No error (0)	www.economjchq.space		188.114.97.3	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:34.015582085 CET	1.1.1.1	192.168.11.20	0x421c	No error (0)	www.economjchq.space		188.114.96.3	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:10:54.252357006 CET	1.1.1.1	192.168.11.20	0xa29e	No error (0)	www.friendsofquarepianos.co.uk		81.17.29.147	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:11:14.789616108 CET	1.1.1.1	192.168.11.20	0xb1a8	Server failure (2)	www.goverifyvin.com	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:11:15.178378105 CET	9.9.9.9	192.168.11.20	0xb1a8	Server failure (2)	www.goverifyvin.com	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:11:35.402036905 CET	1.1.1.1	192.168.11.20	0x4097	No error (0)	www.arialttnr.com	ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 09:11:35.402036905 CET	1.1.1.1	192.168.11.20	0x4097	No error (0)	ghs.googlehosted.com		142.250.186.51	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:11:55.599153996 CET	1.1.1.1	192.168.11.20	0x7a1	Name error (3)	www.eeccu.info	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:12:15.800843000 CET	1.1.1.1	192.168.11.20	0xe5d7	No error (0)	www.garageautosainttthomas.com	ext-sq.squarespace.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 09:12:15.800843000 CET	1.1.1.1	192.168.11.20	0xe5d7	No error (0)	ext-sq.squarespace.com		198.185.159.144	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:12:15.800843000 CET	1.1.1.1	192.168.11.20	0xe5d7	No error (0)	ext-sq.squarespace.com		198.49.23.145	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:12:15.800843000 CET	1.1.1.1	192.168.11.20	0xe5d7	No error (0)	ext-sq.squarespace.com		198.185.159.145	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 09:12:15.800843000 CET	1.1.1.1	192.168.11.20	0xe5d7	No error (0)	ext-sq.squarespace.com		198.49.23.144	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:12:36.538785934 CET	1.1.1.1	192.168.11.20	0xa35d	No error (0)	www.hospitalityhsia.com		206.233.207.174	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:12:57.154711008 CET	1.1.1.1	192.168.11.20	0xc5dd	No error (0)	www.abimpianti.ch		217.26.48.101	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:13:17.829958916 CET	1.1.1.1	192.168.11.20	0x7d8	No error (0)	www.drugtestingservices.co.uk		165.160.15.20	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:13:17.829958916 CET	1.1.1.1	192.168.11.20	0x7d8	No error (0)	www.drugtestingservices.co.uk		165.160.13.20	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:13:38.744119883 CET	1.1.1.1	192.168.11.20	0xa63c	Server failure (2)	www.thinkdev.africa	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:13:42.112545967 CET	9.9.9.9	192.168.11.20	0xa63c	Server failure (2)	www.thinkdev.africa	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:13:42.521053076 CET	9.9.9.9	192.168.11.20	0xa63c	Server failure (2)	www.thinkdev.africa	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:13:44.021675110 CET	9.9.9.9	192.168.11.20	0xa63c	Server failure (2)	www.thinkdev.africa	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:13:59.215681076 CET	1.1.1.1	192.168.11.20	0x8fe7	Name error (3)	www.top-promotion.net	none	none	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:14:39.532558918 CET	1.1.1.1	192.168.11.20	0x68aa	No error (0)	www.amyjohnsonrealtor.com	amyjohnsonrealtor.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 09:14:39.532558918 CET	1.1.1.1	192.168.11.20	0x68aa	No error (0)	amyjohnsonrealtor.com		13.248.157.32	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:15:00.032583952 CET	1.1.1.1	192.168.11.20	0x3f09	No error (0)	www.lists-cellphones.life		104.21.39.114	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:15:00.032583952 CET	1.1.1.1	192.168.11.20	0x3f09	No error (0)	www.lists-cellphones.life		172.67.144.224	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:15:32.885806084 CET	1.1.1.1	192.168.11.20	0xed83	No error (0)	www.findyellowfreightjobs.com		169.60.232.139	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:15:32.885806084 CET	1.1.1.1	192.168.11.20	0xed83	No error (0)	www.findyellowfreightjobs.com		169.60.232.138	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:15:35.175795078 CET	1.1.1.1	192.168.11.20	0xc133	No error (0)	www.conscienciaretroprogresiva.com	conscienciaretroprogresiva.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 09:15:35.175795078 CET	1.1.1.1	192.168.11.20	0xc133	No error (0)	conscienciaretroprogresiva.com		34.102.136.180	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:15:55.980588913 CET	1.1.1.1	192.168.11.20	0xcbb2	No error (0)	www.triknblog.net		183.181.96.18	A (IP address)	IN (0x0001)	false
Mar 20, 2023 09:16:37.623399973 CET	1.1.1.1	192.168.11.20	0x67eb	No error (0)	www.laposadaapts.com	www-laposadaapts-com.rentcafecn.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 09:16:37.623399973 CET	1.1.1.1	192.168.11.20	0x67eb	No error (0)	www-laposadaapts-com.rentcafecn.com	www.rentcafecloudflarecn.com		CNAME (Canonical name)	IN (0x0001)	false
Mar 20, 2023 09:16:37.623399973 CET	1.1.1.1	192.168.11.20	0x67eb	No error (0)	www.rentcafecloudflarecn.com	www.rentcafecloudflarecn.com.cdn.cloudflare.net		CNAME (Canonical name)	IN (0x0001)	false

HTTP Request Dependency Graph

- 195.133.40.46
- www.paparazirestaurant.co.uk
- www.eliteequinewellness.com
- www.economjchq.space
- www.friendsofquarepianos.co.uk
- www.arialttnr.com
- www.garageautosaintthomas.com
- www.hospitalityhsia.com
- www.abimpianti.ch
- www.drugtestingservices.co.uk
- www.amyjohnsonrealtor.com
- www.lists-cellphones.life
- www.findyellowfreightjobs.com
- www.conscienciaretroprogresiva.com
- www.triknblog.net

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

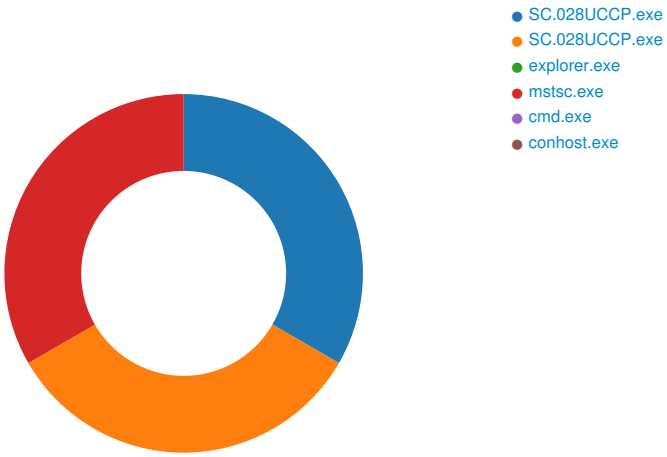
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE9
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE9
GetMessageW	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE9
GetMessageA	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE9

Statistics

Behavior



System Behavior

Analysis Process: SC.028UCCP.exe PID: 6716, Parent PID: 4768

General

Target ID:	0
Start time:	09:08:25
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\SC.028UCCP.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SC.028UCCP.exe
Imagebase:	0x400000
File size:	267392 bytes
MD5 hash:	3F8F4A7F43B5627ED45128BB99F0B471
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_5, Description: Yara detected GuLoader, Source: 00000000.00000002.2936860727.0000000002C10000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.2936860727.000000000411D000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: SC.028UCCP.exe PID: 2704, Parent PID: 6716

General

Target ID:	6
Start time:	09:09:00
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\SC.028UCCP.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SC.028UCCP.exe

Imagebase:	0x400000
File size:	267392 bytes
MD5 hash:	3F8F4A7F43B5627ED45128BB99F0B471
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_5, Description: Yara detected GuLoader, Source: 00000006.00000002.2969977740.0000000001660000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000006.00000002.2969631128.00000000000A0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.2969631128.00000000000A0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2969631128.00000000000A0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2969631128.00000000000A0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000006.00000002.2969631128.00000000000A0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000006.00000002.3048431353.0000000034AC0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.3048431353.0000000034AC0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.3048431353.0000000034AC0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.3048431353.0000000034AC0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000006.00000002.3048431353.0000000034AC0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown
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:\Windows\SysWOW64\ntdll.dll	0	1696752	success or wait	1	41A457	NtReadFile

Analysis Process: explorer.exe PID: **4768**, Parent PID: **2704**

General

Target ID:	7
Start time:	09:09:14
Start date:	20/03/2023
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6a8130000
File size:	4849904 bytes
MD5 hash:	5EA66FF5AE5612F921BC9DA23BAC95F7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Formbook_772cc62d, Description: unknown, Source: 00000007.00000002.7461101436.000000000AD28000.00000040.80000000.00040000.00000000.sdmp, Author: unknown
Reputation:	moderate

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	Completion	Count	Source Address	Symbol

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: mstsc.exe PID: **1800**, Parent PID: **4768**

General

Target ID:	8
Start time:	09:09:19
Start date:	20/03/2023
Path:	C:\Windows\SysWOW64\mstsc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\mstsc.exe
Imagebase:	0x870000
File size:	1264640 bytes
MD5 hash:	B038F39C887BE2A810E20B08613F3B84
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: 00000008.00000002.7446412536.0000000004940000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.7446412536.0000000004940000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.7446412536.0000000004940000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.7446412536.0000000004940000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000008.00000002.7446412536.0000000004940000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000008.00000002.7445956463.0000000004910000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.7445956463.0000000004910000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.7445956463.0000000004910000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.7445956463.0000000004910000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000008.00000002.7445956463.0000000004910000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook_1, Description: Yara detected FormBook, Source: 00000008.00000002.7444154369.0000000002C00000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.7444154369.0000000002C00000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.7444154369.0000000002C00000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.7444154369.0000000002C00000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000008.00000002.7444154369.0000000002C00000.00000040.80000000.00040000.00000000.sdmp, Author: unknown
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1696752	success or wait	1	2C1A457	NtReadFile

Analysis Process: cmd.exe PID: **2296**, Parent PID: **1800**

General

Target ID:	9
Start time:	09:09:23
Start date:	20/03/2023
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\SC.028UCCP.exe"
Imagebase:	0x4f0000
File size:	236544 bytes
MD5 hash:	D0FCE3AFA6AA1D58CE9FA336CC2B675B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **4136**, Parent PID: **2296**

General

Target ID:	10
Start time:	09:09:24
Start date:	20/03/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7259f0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly