ID: 635165
Sample Name:
DrYFu0WLwMjz5fY.exe
Cookbook: default.jbs
Time: 16:11:08
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

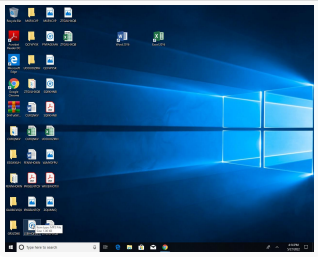
Windows Analysis Report

DrYFu0WLwMjz5fY.exe

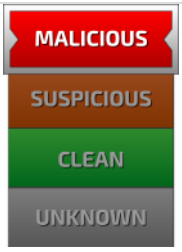
Overview

General Information

Sample Name:	DrYFu0WLwMjz5fY.exe
Analysis ID:	635165
MD5:	a95183abde7096.
SHA1:	21765fad9cec88...
SHA256:	981affe9133f68d..
Tags:	agenttesla exe
Infos:	



Detection



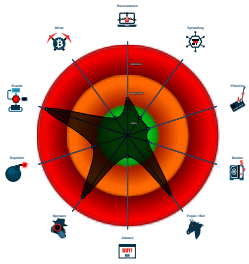
AgentTesla

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 AntiVM3
- Detected unpacking (changes PE se...
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fi...
- Tries to harvest and steal Putty / W...
- Tries to harvest and steal ftp login c...
- Tries to detect sandboxes and other...
- Machine Learning detection for sam...

Classification



Process Tree

- **System is w10x64**
- DrYFu0WLwMjz5fY.exe (PID: 2964 cmdline: "C:\Users\user\Desktop\DrYFu0WLwMjz5fY.exe" MD5: A95183ABDE70960BCCC37B897CCD0699)
  - DrYFu0WLwMjz5fY.exe (PID: 5144 cmdline: C:\Users\user\Desktop\DrYFu0WLwMjz5fY.exe MD5: A95183ABDE70960BCCC37B897CCD0699)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "lewislog@samsung-tv.buzz",
  "Password": "7213575aceACE@#$",
  "Host": "samsung-tv.buzz"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000000.272725067.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000000.272725067.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000004.00000000.267918532.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000000.267918532.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.283159359.000000000462D000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.DrYFu0WLwMjz5fY.exe.4697fd0.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.DrYFu0WLwMjz5fY.exe.4697fd0.8.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.DrYFu0WLwMjz5fY.exe.4697fd0.8.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x30d60:$s10: logins • 0x307c7:$s11: credential • 0x2cdb5:$g1: get_Clipboard • 0x2cdc3:$g2: get_Keyboard • 0x2cdd0:$g3: get_Password • 0x2e0ce:$g4: get_CtrlKeyDown • 0x2e0de:$g5: get_ShiftKeyDown • 0x2e0ef:$g6: get_AltKeyDown
4.0.DrYFu0WLwMjz5fY.exe.400000.12.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.0.DrYFu0WLwMjz5fY.exe.400000.12.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 34 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation

Detected unpacking (changes PE section rights)

Malware Analysis System Evasion

Yara detected AntiVM3
Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)
Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

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)

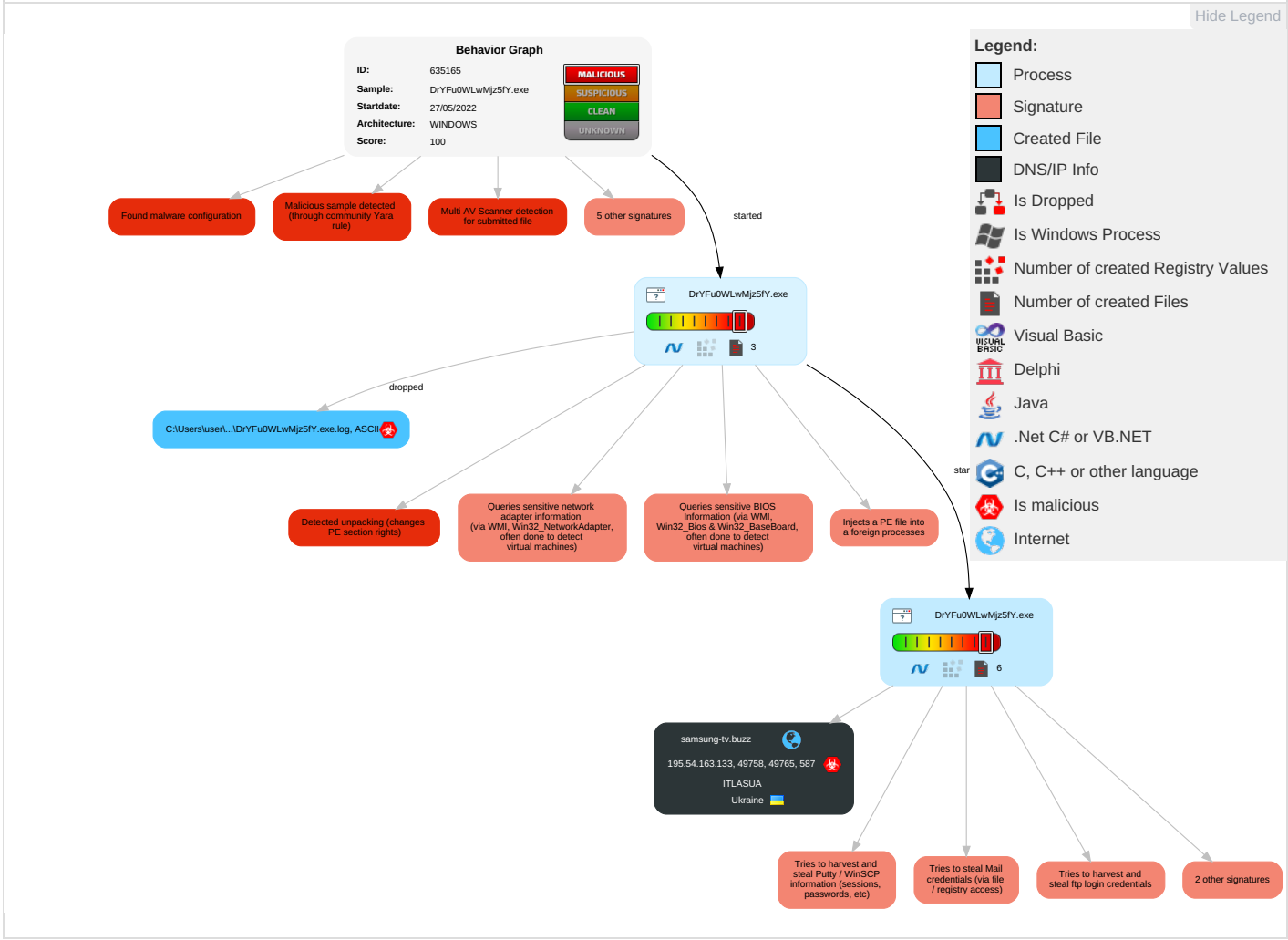
Remote Access Functionality

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	Path Interception	1 1 1 Process Injection	1 1 Disable or Modify Tools	2 OS Credential Dumping	1 1 4 System Information Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Deobfuscate/Decode Files or Information	1 1 Input Capture	1 Query Registry	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 Obfuscated Files or Information	1 Credentials in Registry	2 1 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 3 Software Packing	NTDS	1 Process Discovery	Distributed Component Object Model	1 1 Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	1 3 1 Virtualization/Sandbox Evasion	SSH	1 Clipboard Data	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Modify Registry	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 1 Virtualization/Sandbox Evasion	DCSync	1 Remote System 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

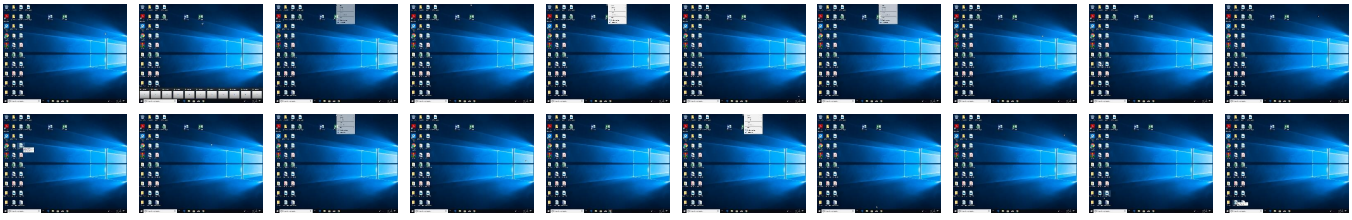
Behavior Graph



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
DrYFu0WLwMjz5fY.exe	34%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
DrYFu0WLwMjz5fY.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.DrYFu0WLwMjz5fY.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.DrYFu0WLwMjz5fY.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.DrYFu0WLwMjz5fY.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.2.DrYFu0WLwMjz5fY.exe.580000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.0.DrYFu0WLwMjz5fY.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.2.DrYFu0WLwMjz5fY.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.DrYFu0WLwMjz5fY.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
samsung-tv.buzz	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://ocsp.suscerte.gob.ve0	0%	URL Reputation	safe	
http://crl.dhimyotis.com/certignarootca.crl0	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnr-tx	0%	Avira URL Cloud	safe	
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/dpc0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://policy.camerfirma.com0	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	0%	URL Reputation	safe	
http://https://wwww.certigna.fr/autorites/0m	0%	URL Reputation	safe	
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.globaltrust.info0	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://ac.economia.gob.mx/last.crl0G	0%	URL Reputation	safe	
http://crl.oces.trust2408.com/oces.crl0	0%	URL Reputation	safe	
http://certs.oaticerts.com/repository/OATICA2.crl	0%	URL Reputation	safe	
http://certs.oati.net/repository/OATICA2.crt0	0%	URL Reputation	safe	
http://www.accv.es00	0%	URL Reputation	safe	
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.acabogacia.org0	0%	URL Reputation	safe	
http://https://api.ipify.org%%startupfolder%	0%	URL Reputation	safe	
http://crl.securetrust.com/SGCA.crl0	0%	URL Reputation	safe	
http://www.agesic.gub.uy/acrn/acrn.crl0)	0%	URL Reputation	safe	
http://www.rcsc.lt/repository0	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comgritaj	0%	Avira URL Cloud	safe	
http://x1.c.lencr.org/0	0%	URL Reputation	safe	
http://x1.i.lencr.org/0	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.comr-tx	0%	Avira URL Cloud	safe	
http://certs.oaticerts.com/repository/OATICA2.crt08	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersignroot.html0	0%	URL Reputation	safe	
http://www.oaticerts.com/repository.	0%	URL Reputation	safe	
http://www.ancert.com/cps0	0%	URL Reputation	safe	
http://ocsp.accv.es0	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/LCRacraizv2.crl0	0%	URL Reputation	safe	
http://www.echoworx.com/ca/root2/cps.pdf0	0%	URL Reputation	safe	
http://ca.mtin.es/mtin/crl/MTINAutoridadRaiz03	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://samsung-tv.buzz	0%	Avira URL Cloud	safe	
http://acraiz.icpbrasil.gov.br/LCRacraizv1.crl0	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://crl.defence.gov.au/pki0	0%	URL Reputation	safe	
http://www.agesic.gub.uy/acrn/cps_acrn.pdf0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignAdvancedSecurityCA.crl0	0%	URL Reputation	safe	
http://https://www.catcert.net/verarrel05	0%	URL Reputation	safe	
http://http.fpki.gov/fcpca/caCertsIssuedByfcpca.p7c0	0%	URL Reputation	safe	
http://www.comsign.co.il/cps0	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://www.postsignum.cz/crl/psrootqca2.crl02	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.htmlE	0%	Avira URL Cloud	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/lcr0#	0%	URL Reputation	safe	
http://postsignum.ttc.cz/crl/psrootqca2.crl0	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://crl1.comsign.co.il/crl/comsignglobalrootca.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
samsung-tv.buzz	195.54.163.133	true	true	• 2%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.certplus.com/CRL/class3.crl0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301730088.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://github.com/dcoetzee/plants-vs-zombies-user-file-editor	DrYFu0WLwMjz5fY.exe	false		high
http://ocsp.suscerte.gob.ve0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.300994237.00000000074DF000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301093390.00000000074EC000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301730088.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.dhimyotis.com/certignarootca.crl0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.300807255.00000000071CA000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://sertifikati.ca.posta.rs/crl/PostaCARoot.crl0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301730088.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.chambersign.org1	DrYFu0WLwMjz5fY.exe, 00000004.00000003.300994237.00000000074DF000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301027805.00000000074CA000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301093390.00000000074EC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cnr-tx	DrYFu0WLwMjz5fY.exe, 00000000.00000003.247385713.0000000007E7A000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000000.00000003.247429001.0000000007E7A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://repository.swisssign.com/0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301070933.00000000074D5000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301027805.00000074CA000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301730088.000000000742200.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301236509.00000000074A8000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers	DrYFu0WLwMjz5fY.exe, 00000000.00000002.286257632.0000000009292000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301027805.00000000074CA000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.ssc.lt/root-c/cacrl.crl0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.300807255.00000000071CA000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ca.disig.sk/ca/crl/ca_disig.crl0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301345594.00000000074A5000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.313665694.00000000074A5000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.313768380.00000000074A5000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.429330402.00000000074A5000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000002.508073762.00000000074A5000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.307999640.00000000074A5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.suscerte.gob.ve/dpc0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.300994237.00000000074DF000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301093390.00000074EC000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301730088.000000000742200.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.disig.sk/ca/crl/ca_disig.crl0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301345594.00000000074A5000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.313665694.00000000074A5000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.313768380.00000000074A5000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.429330402.00000000074A5000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000002.508073762.00000000074A5000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.307999640.00000000074A5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	DrYFu0WLwMjz5fY.exe, 00000000.00000002.286257632.0000000009292000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	DrYFu0WLwMjz5fY.exe, 00000000.00000002.286257632.0000000009292000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000000.00000003.247385713.00000000007E7A000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000000.00000003.247429001.0000000007E7A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%	DrYFu0WLwMjz5fY.exe, 00000004.00000002.505156473.0000000003451000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://pki.registradores.org/normativa/index.htm0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.300807255.00000000071CA000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://policy.camerfirma.com0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.300994237.00000000074DF000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301126397.00000000074C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.anf.es/es/address-direccion.html	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301070933.00000000074D5000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301027805.00000000074CA000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.anf.es/address/)1(0&	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301278276.0000000007435000.00000004.00000800.00020000.00000000.sdmp	false		high
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301027805.00000000074CA000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301236509.00000000074A8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.come	DrYFu0WLwMjz5fY.exe, 00000000.00000003.247705436.0000000007E7A000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000000.00000003.247745863.0000000007E7A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://cps.letsencrypt.org0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.429398254.0000000007272000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000002.506114167.00000000037F3000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000002.505912640.00000000037AF000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000002.507974553.0000000007274000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.ssc.lt/root-b/cacrl.crl0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.300994237.00000000074DF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.certicamara.com/dpc/0Z	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301278276.0000000007435000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301126397.00000000074C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.pki.wellsfargo.com/wsprca.crl0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301730088.0000000007422000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://wwww.certigna.fr/autorites/0m	DrYFu0WLwMjz5fY.exe, 00000004.00000003.300807255.00000000071CA000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.300994237.00000000074DF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	DrYFu0WLwMjz5fY.exe, 00000004.00000002.505156473.0000000003451000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.anf.es/AC/ANFServerCA.crl0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301278276.0000000007435000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.globaltrust.info0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.300994237.00000000074DF000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301093390.00000000074EC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	DrYFu0WLwMjz5fY.exe, 00000000.00000002.286257632.0000000009292000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ac.economia.gob.mx/last.crl0G	DrYFu0WLwMjz5fY.exe, 00000004.00000003.300994237.00000000074DF000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301093390.00000000074EC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

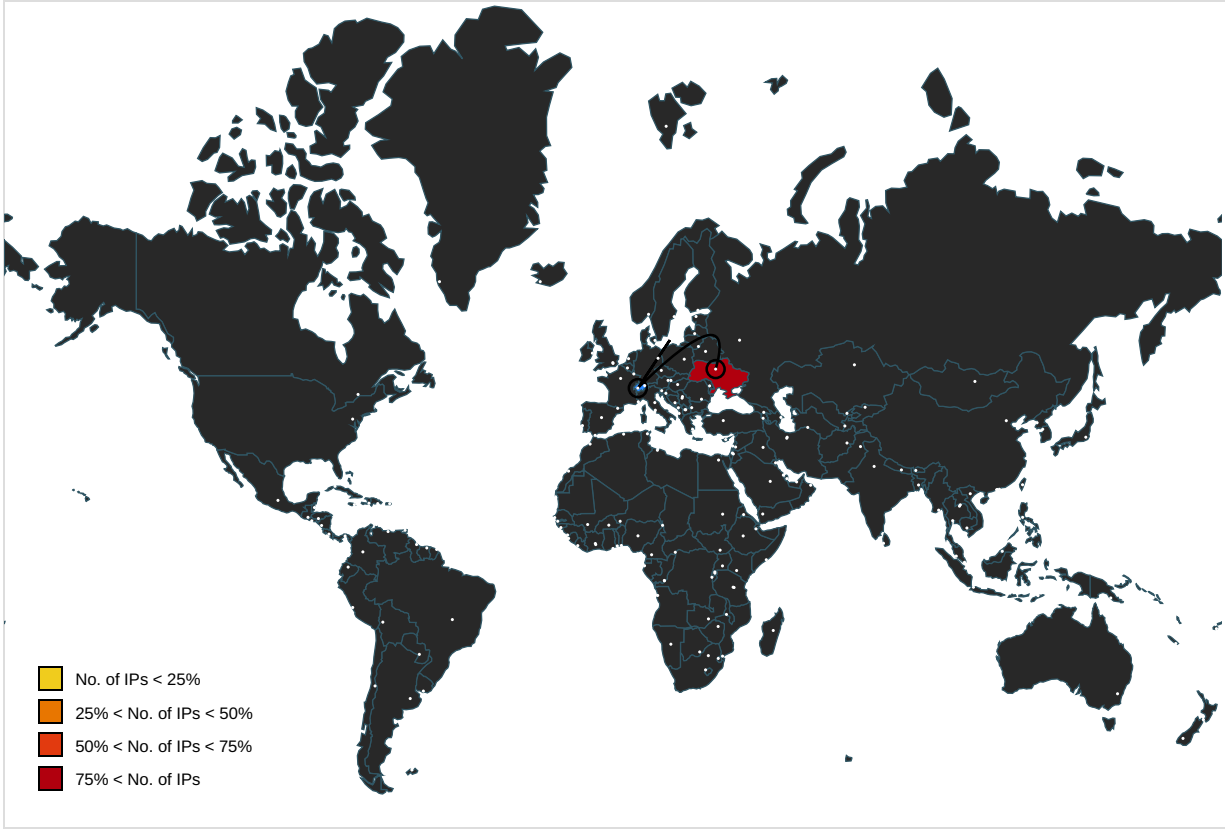
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1.crt0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301879715.00000000074B1000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301236509.00000000074A8000.00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.oces.trust2408.com/oces.crl0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301070933.00000000074D5000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301027805.00000000074CA000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://eca.hinet.net/repository0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301166023.00000000074BC000.00000004.00000800.00020000.00000000.sdmp	false		high
http://certs.oaticerts.com/repository/OATICA2.crl	DrYFu0WLwMjz5fY.exe, 00000004.00000003.300994237.00000000074DF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://certs.oati.net/repository/OATICA2.crt0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.300994237.00000000074DF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.accv.es00	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301879715.00000000074B1000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301236509.00000000074A8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_1.pdf0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301027805.00000000074CA000.00000004.00000800.00020000.00000000.sdmp	false		high
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301166023.00000000074BC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.datev.de/zertifikat-policy-int0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301879715.00000000074B1000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301070933.00000000074D5000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301027805.00000000074CA000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301236509.00000000074A8000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301260375.00000000074B4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	DrYFu0WLwMjz5fY.exe, 00000000.00000002.286257632.0000000009292000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.acabogacia.org0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301126397.00000000074C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.firmaprofesional.com/cps0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301364748.000000000749E000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301278276.0000000007435000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ipify.org%%startupfolder%	DrYFu0WLwMjz5fY.exe, 00000004.00000002.505156473.0000000003451000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://crl.securetrust.com/SGCA.crl0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.429366287.00000000074C5000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301220987.00000000074C5000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301970914.00000000074C5000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301126397.00000000074C2000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.313896786.00000000074C5000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000002.508117984.00000000074C5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.agesic.gub.uy/acrn/acrn.crl0)	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301126397.00000000074C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.rcsc.lt/repository0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301236509.00000000074A8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	DrYFu0WLwMjz5fY.exe, 00000000.00000002.286257632.0000000009292000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	DrYFu0WLwMjz5fY.exe, 00000000.00000002.286257632.0000000009292000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comgritaj	DrYFu0WLwMjz5fY.exe, 00000000.00000002.276898324.0000000001080000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://web.certicamara.com/marco-legal0Z	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301070933.00000000074D5000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301027805.00000000074CA000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.quovadisglobal.com/cps0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.300807255.00000000071CA000.00000004.00000800.00020000.00000000.sdmp	false		high
http://x1.c.lencr.org/0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.429398254.0000000007272000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000002.506114167.00000000037F3000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000002.505912640.00000000037AF000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000002.507974553.0000000007274000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://x1.i.lencr.org/0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.429398254.0000000007272000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000002.506114167.00000000037F3000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000002.505912640.00000000037AF000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000002.507974553.0000000007274000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	DrYFu0WLwMjz5fY.exe, 00000004.00000002.505156473.0000000003451000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	DrYFu0WLwMjz5fY.exe, 00000000.00000002.286257632.0000000009292000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	DrYFu0WLwMjz5fY.exe, 00000000.00000002.286257632.0000000009292000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comr-tx	DrYFu0WLwMjz5fY.exe, 00000000.00000003.247705436.0000000007E7A000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000000.00000003.247745863.0000000007E7A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://certs.oaticerts.com/repository/OATICA2.crt08	DrYFu0WLwMjz5fY.exe, 00000004.00000003.300994237.00000000074DF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://cps.chambersign.org/cps/chambersignroot.html0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.300994237.00000000074DF000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301093390.00000000074EC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.anf.es/AC/RC/ocsp0c	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301278276.0000000007435000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.oaticerts.com/repository.	DrYFu0WLwMjz5fY.exe, 00000004.00000003.300994237.00000000074DF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ancert.com/cps0	DrYFu0WLwMjz5fY.exe, 00000004.00000002.507763236.00000000071D9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.accv.es0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301879715.00000000074B1000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301236509.00000000074A8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://acraiz.icpbrasil.gov.br/LCRacraizv2.crl0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301236509.00000000074A8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.echoworx.com/ca/root2/cps.pdf0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301278276.0000000007435000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://rca.e-szigno.hu/ocsp0-	DrYFu0WLwMjz5fY.exe, 00000004.00000003.300807255.00000000071CA000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ca.mtin.es/mtin/crl/MTINAutoridadRaiz03	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301027805.00000000074CA000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://samsung-tv.buzz	DrYFu0WLwMjz5fY.exe, 00000004.00000002.506114167.00000000037F3000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000002.505912640.00000000037AF000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://eca.hinet.net/repository/CRL2/CA.crl0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301166023.00000000074BC000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.datev.de/zertifikat-policy-std0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.300807255.00000000071CA000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301236509.00000000074A8000.00000004.00000800.00020000.00000000.sdmp	false		high
http://acraiz.icpbrasil.gov.br/LCRacraizv1.crl0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301027805.00000000074CA000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	DrYFu0WLwMjz5fY.exe, 00000000.00000002.286257632.0000000009292000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	DrYFu0WLwMjz5fY.exe, 00000000.00000002.286257632.0000000009292000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.informatik.admin.ch/PKI/links/CPS_2_16_756_1_17_3_1_0.pdf0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.300807255.00000000071CA000.00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.defence.gov.au/pki0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301236509.00000000074A8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.agesic.gub.uy/acrn/cps_acrn.pdf0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301126397.00000000074C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fedir.comsign.co.il/crl/ComSignAdvancedSecurityCA.crl0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301166023.00000000074BC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.catcert.net/verarrel05	DrYFu0WLwMjz5fY.exe, 00000004.00000003.300807255.00000000071CA000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://http.fpki.gov/fcpca/caCertsIssuedByfcpca.p7c0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301236509.00000000074A8000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301260375.00000000074B4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.pki.gva.es/cps0%	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301236509.00000000074A8000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.cert.fnmt.es/dpcs/0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301730088.0000000007422000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301278276.0000000007435000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301403875.000000000743C000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.datev.de/zertifikat-policy-bt0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.300994237.00000000074DF000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301093390.00000074EC000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301730088.000000000742200.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.comsign.co.il/cps0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301166023.00000000074BC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://127.0.0.1:HTTP/1.1	DrYFu0WLwMjz5fY.exe, 00000004.00000002.505156473.0000000003451000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.e-me.lv/repository0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.300807255.00000000071CA000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.300839908.00000071DF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.acabogacia.org/doc0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301730088.0000000007422000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301126397.00000074C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.chambersign.org/chambersroot.crl0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301027805.00000000074CA000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.postsignum.cz/crl/psrootqca2.crl02	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301236509.00000000074A8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.htmlE	DrYFu0WLwMjz5fY.exe, 00000000.00000003.248146714.0000000007EAD000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.pkioverheid.nl/policies/root-policy0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301220987.00000000074C5000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301970914.00000074C5000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301126397.00000000074C2000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.313896786.00000000074C5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.suscerte.gob.ve/lcr0#	DrYFu0WLwMjz5fY.exe, 00000004.00000003.300994237.00000000074DF000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301093390.00000074EC000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301730088.000000000742200.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://postsignum.ttc.cz/crl/psrootqca2.crl0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301236509.00000000074A8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301166023.00000000074BC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl1.comsign.co.il/crl/comsignglobalrootca.crl0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.301364748.000000000749E000.00000004.00000800.00020000.00000000.sdmp, DrYFu0WLwMjz5fY.exe, 00000004.00000003.301278276.00000000007435000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3P.crl0	DrYFu0WLwMjz5fY.exe, 00000004.00000003.300807255.00000000071CA000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
195.54.163.133	samsung-tv.buzz	Ukraine		15626	ITLASUA	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635165
Start date and time: 27/05/202216:11:08	2022-05-27 16:11:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DrYFu0WLwMjz5fY.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/4@2/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 1.4% (good quality ratio 0.8%) • Quality average: 32.1% • Quality standard deviation: 33.6%

HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 173.222.108.226, 173.222.108.210
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, a767.dspw65.akamai.net, arc.msn.com, wu-bg-shim.trafficmanager.net, download.windowsupdate.com.edgesuite.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:12:20	API Interceptor	682x Sleep call for process: DrYFu0WLwMjz5fY.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\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Users\user\Desktop\DrYFu0WLwMjz5fY.exe
File Type:	Microsoft Cabinet archive data, 61476 bytes, 1 file
Category:	dropped
Size (bytes):	61476
Entropy (8bit):	**7.995018321729444**
Encrypted:	**true**

SSDEEP:	1536:NATLwfiuePkACih0/8ulwf5CiqGLhk1V/AFnGegJR:N7nePk5gKsoBha/0GTf
MD5:	308336E7F515478969B24C13DED11EDE
SHA1:	8FB0CF42B77DBBEF224A1E5FC38ABC2486320775
SHA-256:	889B832323726A9F10AD03F85562048FDCFE20C9FF6F9D37412CF477B4E92FF9
SHA-512:	61AD97228CD6C3909EF3AC5E4940199971F293BDD0D5EB7916E60469573A44B6287C0FA1E0B6C1389DF35EB6C9A7D2A61FDB318D4A886A3821EF5A9DAB3AC2F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF....$.....,.....I.....w.....Tp. .authroot.stl.H#F..4..CK..<Tk...c_.d....A.F...,.&K..*i.RJJ..J.".%.KY"{n...."{..Lu3.Ln.....y.....M.:...<. v...H..~.#Ov.a0xN....)..C..t.z.,x.00.1``L.....L.\..1.|..2.1.0mD...H1/.....G..UT7!...r.X:....D.0.0...M....I(.-.+..v#...(.r.....z.Y`&hw..Gl+.je.e.j..{.1.....9f=.&.....s.W...L.].+...).f...u.....8....}R...w.X..>.A.Yw...a.x..T8V.e...^.7.q..t^.+....f.q).B.M.....64.<!W(.....D!.0.t "X...l.....D0.....+...A.....0.o..t93.v..O1V x}H.S)....GH.6.l...p2.(4k....!,.L`.....h:.a]?.....J9.\..Ww.....%.....a4E...q.*...#..a..y..M..R.t..Z2!.T.Ua.k.'O..\./ d.F>.V...3...._.J....".....wI..'..z...j..Ds...qZ...[.....O<.d.K..hH@c1....[w7..z...l....h,.b.....'.w.....bO.i{.....+.-...H..."<...L.Tu}.Y.lB.]3..4..G.3..`E..NF.....{o.h]}p....G..$..4....;..&.O.d....v:Ik.T..ObLq..&.j.j...B9.(..!..\.:K`.....:O..N.....C..jD:.i.....1.....eCo.c..3o.....nN.D..3.7...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Users\user\Desktop\DrYFu0WLwMjz5fY.exe
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.0941585927255777
Encrypted:	false
SSDEEP:	6:kK4HBmN+SkQlPlEGYRMY9z+4KlDA3RUecl7PG1:0TkPlE99SNxAhUecl61
MD5:	497C37EFC97B14D36794F4568369F626
SHA1:	51459B7E1D4DD17D37D0BEDDC04E7306CCC5F72B
SHA-256:	A5A97C249259FBD19FF818CBB716465A9BAFB470CA7F61EAA80A018D99B9372F
SHA-512:	17EA6D7E12C12991B363F72A34B419C4A427BAD77C25F4C25E4B888DBFA9492D0FE06C9B3CE5A1439143C63E76D2DD8A51243C5E95D6DA12D61BBBF2F93025F
Malicious:	false
Reputation:	low
Preview:	p..... ...../....q..(..... .....3f..o.....&.....$...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.3.3.6.6.b.4.9.0.6.f.d.8.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DrYFu0WLwMjz5fY.exe.log

Process:	C:\Users\user\Desktop\DrYFu0WLwMjz5fY.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Roaming\enexldkj.qah\Chrome\Default\Cookies

Process:	C:\Users\user\Desktop\DrYFu0WLwMjz5fY.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ

MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Reputation:	high, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.681430646387277
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	DrYFu0WLwMjz5fY.exe
File size:	909312
MD5:	a95183abde70960bccc37b897ccd0699
SHA1:	21765fad9cec8831ef6e7361076abd779f4bf68c
SHA256:	981affe9133f68da268a562ad4c6f16464b7d00e4a596bae4516e984bfd04cff
SHA512:	f1a9f64a11742877036d13a9f2239d720b44de53b7cab596f1879574f4d43c703deb50695b1ee45bc82d4c6c2cdc9feea03cc0a6ef0dd6fffb329bca108bcd4f
SSDEEP:	24576:732dT2XreSkbHo2xS6OVby2+eIjErm4KUGhwGG:DbuxObtI4rShwGG
TLSH:	6315BFBC31907DDFC817CE7985985C649A202CA6470BE203A01B3DDDAA7DF968F156E3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....%.b.....0.....L..... .....@.. .....@.....@.....

File Icon

Icon Hash:	31b1393969391b39

Static PE Info

General

Entrypoint:	0x4db02e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6290259C [Fri May 27 01:13:00 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xdafd8	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xdc000	0x4860	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe2000	0xc	.reloc
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	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xd9034	0xd9200	False	0.835496725676	data	7.6975939931	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xdc000	0x4860	0x4a00	False	0.662056587838	data	6.42119337389	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe2000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xdc160	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 4294268550, next used block 4294202757		
RT_GROUP_ICON	0xe0388	0x14	data		
RT_GROUP_ICON	0xe039c	0x14	data		
RT_VERSION	0xe03b0	0x2c4	data		
RT_MANIFEST	0xe0674	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

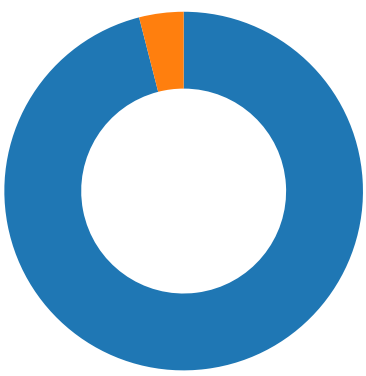
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	
Assembly Version	1.0.0.0
InternalName	SHA.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	
ProductVersion	1.0.0.0
FileDescription	
OriginalFilename	SHA.exe

Network Behavior

Network Port Distribution



Total Packets: 50

- 53 (DNS)
- 587 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 16:12:39.271641016 CEST	49758	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:39.326838017 CEST	587	49758	195.54.163.133	192.168.2.4
May 27, 2022 16:12:39.327167988 CEST	49758	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:39.489639044 CEST	587	49758	195.54.163.133	192.168.2.4
May 27, 2022 16:12:39.490025997 CEST	49758	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:39.545362949 CEST	587	49758	195.54.163.133	192.168.2.4
May 27, 2022 16:12:39.547352076 CEST	49758	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:39.604124069 CEST	587	49758	195.54.163.133	192.168.2.4
May 27, 2022 16:12:39.654772043 CEST	49758	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:39.715156078 CEST	587	49758	195.54.163.133	192.168.2.4
May 27, 2022 16:12:39.715207100 CEST	587	49758	195.54.163.133	192.168.2.4
May 27, 2022 16:12:39.715241909 CEST	587	49758	195.54.163.133	192.168.2.4
May 27, 2022 16:12:39.715267897 CEST	587	49758	195.54.163.133	192.168.2.4
May 27, 2022 16:12:39.715348959 CEST	49758	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:39.715400934 CEST	49758	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:39.716634035 CEST	587	49758	195.54.163.133	192.168.2.4
May 27, 2022 16:12:39.743633032 CEST	49758	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:39.799196959 CEST	587	49758	195.54.163.133	192.168.2.4
May 27, 2022 16:12:39.993288994 CEST	49758	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:43.145391941 CEST	49758	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:43.200733900 CEST	587	49758	195.54.163.133	192.168.2.4
May 27, 2022 16:12:43.202548981 CEST	49758	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:43.258194923 CEST	587	49758	195.54.163.133	192.168.2.4
May 27, 2022 16:12:43.258897066 CEST	49758	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:43.315084934 CEST	587	49758	195.54.163.133	192.168.2.4
May 27, 2022 16:12:43.316406965 CEST	49758	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:43.371669054 CEST	587	49758	195.54.163.133	192.168.2.4
May 27, 2022 16:12:43.372342110 CEST	49758	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:43.467113018 CEST	587	49758	195.54.163.133	192.168.2.4
May 27, 2022 16:12:43.471972942 CEST	587	49758	195.54.163.133	192.168.2.4
May 27, 2022 16:12:43.473081112 CEST	49758	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:43.528278112 CEST	587	49758	195.54.163.133	192.168.2.4
May 27, 2022 16:12:43.528327942 CEST	587	49758	195.54.163.133	192.168.2.4
May 27, 2022 16:12:43.529453993 CEST	49758	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:43.529511929 CEST	49758	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:43.530061007 CEST	49758	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:43.530122995 CEST	49758	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:43.584635973 CEST	587	49758	195.54.163.133	192.168.2.4
May 27, 2022 16:12:43.584683895 CEST	587	49758	195.54.163.133	192.168.2.4
May 27, 2022 16:12:43.584815979 CEST	587	49758	195.54.163.133	192.168.2.4
May 27, 2022 16:12:43.584841967 CEST	587	49758	195.54.163.133	192.168.2.4
May 27, 2022 16:12:43.587070942 CEST	587	49758	195.54.163.133	192.168.2.4
May 27, 2022 16:12:43.681020021 CEST	49758	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:47.460766077 CEST	49758	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:47.555217981 CEST	587	49758	195.54.163.133	192.168.2.4
May 27, 2022 16:12:47.803215027 CEST	587	49758	195.54.163.133	192.168.2.4
May 27, 2022 16:12:47.803838968 CEST	49758	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:47.870364904 CEST	49765	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:47.925909042 CEST	587	49765	195.54.163.133	192.168.2.4
May 27, 2022 16:12:47.926224947 CEST	49765	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:48.019937038 CEST	587	49765	195.54.163.133	192.168.2.4
May 27, 2022 16:12:48.020385027 CEST	49765	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:48.076255083 CEST	587	49765	195.54.163.133	192.168.2.4
May 27, 2022 16:12:48.080271959 CEST	49765	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:48.139369965 CEST	587	49765	195.54.163.133	192.168.2.4
May 27, 2022 16:12:48.140382051 CEST	49765	587	192.168.2.4	195.54.163.133

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 16:12:48.205936909 CEST	587	49765	195.54.163.133	192.168.2.4
May 27, 2022 16:12:48.206037998 CEST	587	49765	195.54.163.133	192.168.2.4
May 27, 2022 16:12:48.206079960 CEST	587	49765	195.54.163.133	192.168.2.4
May 27, 2022 16:12:48.206111908 CEST	587	49765	195.54.163.133	192.168.2.4
May 27, 2022 16:12:48.206182003 CEST	49765	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:48.206254959 CEST	49765	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:48.210211992 CEST	587	49765	195.54.163.133	192.168.2.4
May 27, 2022 16:12:48.212935925 CEST	49765	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:48.268774033 CEST	587	49765	195.54.163.133	192.168.2.4
May 27, 2022 16:12:48.493921995 CEST	49765	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:48.527714968 CEST	587	49765	195.54.163.133	192.168.2.4
May 27, 2022 16:12:48.528364897 CEST	49765	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:48.703119993 CEST	49765	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:48.758764982 CEST	587	49765	195.54.163.133	192.168.2.4
May 27, 2022 16:12:48.759193897 CEST	49765	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:48.815078974 CEST	587	49765	195.54.163.133	192.168.2.4
May 27, 2022 16:12:48.815649033 CEST	49765	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:48.872153044 CEST	587	49765	195.54.163.133	192.168.2.4
May 27, 2022 16:12:48.872580051 CEST	49765	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:48.928091049 CEST	587	49765	195.54.163.133	192.168.2.4
May 27, 2022 16:12:48.928575039 CEST	49765	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:49.020035028 CEST	587	49765	195.54.163.133	192.168.2.4
May 27, 2022 16:12:49.020384073 CEST	49765	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:49.075999975 CEST	587	49765	195.54.163.133	192.168.2.4
May 27, 2022 16:12:49.077652931 CEST	49765	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:49.077888012 CEST	49765	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:49.077908993 CEST	49765	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:49.077979088 CEST	49765	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:49.078180075 CEST	49765	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:49.078322887 CEST	49765	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:49.078340054 CEST	49765	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:49.078419924 CEST	49765	587	192.168.2.4	195.54.163.133
May 27, 2022 16:12:49.133163929 CEST	587	49765	195.54.163.133	192.168.2.4
May 27, 2022 16:12:49.133209944 CEST	587	49765	195.54.163.133	192.168.2.4
May 27, 2022 16:12:49.133236885 CEST	587	49765	195.54.163.133	192.168.2.4
May 27, 2022 16:12:49.133261919 CEST	587	49765	195.54.163.133	192.168.2.4
May 27, 2022 16:12:49.133398056 CEST	587	49765	195.54.163.133	192.168.2.4
May 27, 2022 16:12:49.133425951 CEST	587	49765	195.54.163.133	192.168.2.4
May 27, 2022 16:12:49.133552074 CEST	587	49765	195.54.163.133	192.168.2.4
May 27, 2022 16:12:49.133579969 CEST	587	49765	195.54.163.133	192.168.2.4
May 27, 2022 16:12:49.133605003 CEST	587	49765	195.54.163.133	192.168.2.4
May 27, 2022 16:12:49.137506008 CEST	587	49765	195.54.163.133	192.168.2.4
May 27, 2022 16:12:49.181477070 CEST	49765	587	192.168.2.4	195.54.163.133
May 27, 2022 16:14:19.142858028 CEST	49765	587	192.168.2.4	195.54.163.133

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 16:12:39.221312046 CEST	64454	53	192.168.2.4	8.8.8.8
May 27, 2022 16:12:39.254265070 CEST	53	64454	8.8.8.8	192.168.2.4
May 27, 2022 16:12:47.831768036 CEST	60647	53	192.168.2.4	8.8.8.8
May 27, 2022 16:12:47.866461039 CEST	53	60647	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 16:12:39.221312046 CEST	192.168.2.4	8.8.8.8	0x571d	Standard query (0)	samsung-tv.buzz	A (IP address)	IN (0x0001)
May 27, 2022 16:12:47.831768036 CEST	192.168.2.4	8.8.8.8	0x7e16	Standard query (0)	samsung-tv.buzz	A (IP address)	IN (0x0001)

DNS Answers

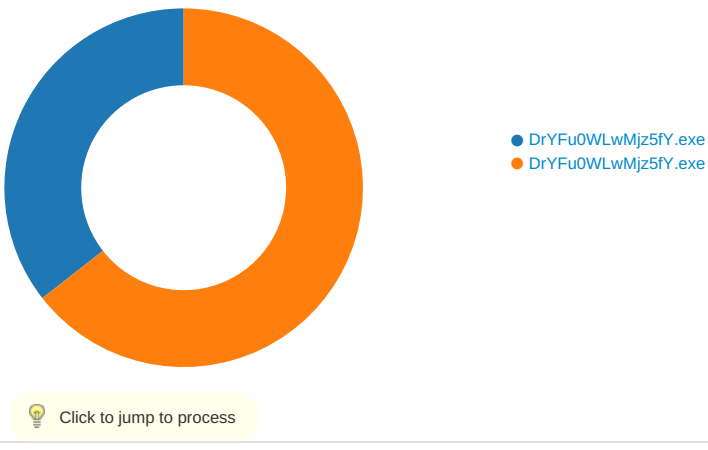
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 16:12:39.254265070 CEST	8.8.8.8	192.168.2.4	0x571d	No error (0)	samsung-tv.buzz		195.54.163.133	A (IP address)	IN (0x0001)
May 27, 2022 16:12:47.866461039 CEST	8.8.8.8	192.168.2.4	0x7e16	No error (0)	samsung-tv.buzz		195.54.163.133	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 27, 2022 16:12:39.489639044 CEST	587	49758	195.54.163.133	192.168.2.4	220-cp5ua.hyperhost.ua ESMTP Exim 4.95 #2 Fri, 27 May 2022 17:12:38 +0300 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 27, 2022 16:12:39.490025997 CEST	49758	587	192.168.2.4	195.54.163.133	EHLO 377142
May 27, 2022 16:12:39.545362949 CEST	587	49758	195.54.163.133	192.168.2.4	250-cp5ua.hyperhost.ua Hello 377142 [102.129.143.42] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-STARTTLS 250 HELP
May 27, 2022 16:12:39.547352076 CEST	49758	587	192.168.2.4	195.54.163.133	STARTTLS
May 27, 2022 16:12:39.604124069 CEST	587	49758	195.54.163.133	192.168.2.4	220 TLS go ahead
May 27, 2022 16:12:48.019937038 CEST	587	49765	195.54.163.133	192.168.2.4	220-cp5ua.hyperhost.ua ESMTP Exim 4.95 #2 Fri, 27 May 2022 17:12:47 +0300 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 27, 2022 16:12:48.020385027 CEST	49765	587	192.168.2.4	195.54.163.133	EHLO 377142
May 27, 2022 16:12:48.076255083 CEST	587	49765	195.54.163.133	192.168.2.4	250-cp5ua.hyperhost.ua Hello 377142 [102.129.143.42] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-STARTTLS 250 HELP
May 27, 2022 16:12:48.080271959 CEST	49765	587	192.168.2.4	195.54.163.133	STARTTLS
May 27, 2022 16:12:48.139369965 CEST	587	49765	195.54.163.133	192.168.2.4	220 TLS go ahead

Statistics

Behavior



System Behavior

Analysis Process: DrYFu0WLwMjz5fY.exe PID: **2964**, Parent PID: **4052**

General

Target ID:	0
Start time:	16:12:09
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\DrYFu0WLwMjz5fY.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\DrYFu0WLwMjz5fY.exe"
Imagebase:	0x580000
File size:	909312 bytes
MD5 hash:	A95183ABDE70960BCCC37B897CCD0699
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.283159359.000000000462D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.283159359.000000000462D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.280654156.0000000002D9E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_zgRAT, Description: Detects zgRAT, Source: 00000000.00000002.286677931.00000000098D0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
Reputation:	low

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	6DD0CF06	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	6DD0CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DrYFu0WLwMjz5fY.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E01C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DrYFu0WLwMjz5fY.exe.log	0	1308	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E01C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB51B4F	ReadFile

Analysis Process: DrYFu0WLwMjz5fY.exe PID: **5144**, Parent PID: **2964**

General

Target ID:	4
Start time:	16:12:22
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\DrYFu0WLwMjz5fY.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DrYFu0WLwMjz5fY.exe
Imagebase:	0xfe0000
File size:	909312 bytes
MD5 hash:	A95183ABDE70960BCCC37B897CCD0699
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.272725067.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.272725067.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.267918532.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.267918532.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.271853258.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.271853258.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.273383724.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.273383724.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.501605400.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.501605400.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.505156473.0000000003451000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.505156473.0000000003451000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

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	6DD0CF06	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	6DD0CF06	unknown
C:\Users\user\AppData\Roaming\enexldkj.qah	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CB5BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\enexldkj.qah\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CB5BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\enexldkj.qah\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CB5BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\enexldkj.qah\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CB5DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\enexldkj.qah\Chrome\Default\Cookies	success or wait	1	6CB56A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\enexldkj.qah\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 fd 0d 0f fd 00 04 0d 20 00 0f 67 0f fd 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3@ .C g 8	success or wait	1	6CB5DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB51B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CB51B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CB51B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CB51B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6CB51B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\d1aef8e4-b864-479c-bf86-f42c63d352b2	unknown	4096	success or wait	1	6CB51B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6CB51B4F	ReadFile
C:\Users\user\AppData\Roaming\enexldkj.qah\Chrome\Default\Cookies	unknown	16384	success or wait	2	6CB51B4F	ReadFile

Registry Activities

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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly