ID: 635212
Sample Name:
6R24hlXGVS56Z6Y.exe
Cookbook: default.jbs
Time: 17:06:05
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

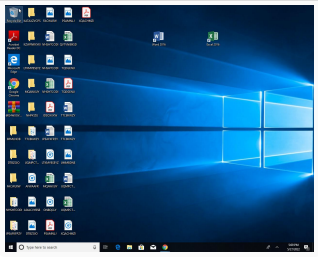
Windows Analysis Report

6R24hlXGVS56Z6Y.exe

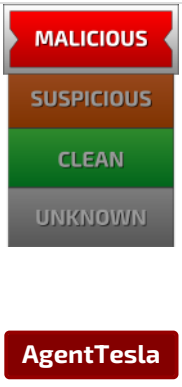
Overview

General Information

Sample Name:	6R24hlXGVS56Z6Y.exe
Analysis ID:	635212
MD5:	a9819b4b8ca61d..
SHA1:	226725a9f34ade..
SHA256:	86a8ba97bde5b0.
Tags:	agenttesla exe
Infos:	



Detection



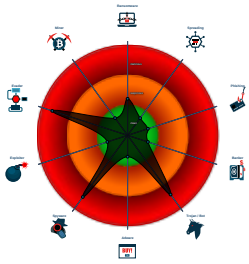
AgentTesla

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
- Antivirus / Scanner detection for sub…
- 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**
- 6R24hlXGVS56Z6Y.exe (PID: 6360 cmdline: "C:\Users\user\Desktop\6R24hlXGVS56Z6Y.exe" MD5: A9819B4B8CA61D132FAA30C59482C10F)
  - 6R24hlXGVS56Z6Y.exe (PID: 6520 cmdline: C:\Users\user\Desktop\6R24hlXGVS56Z6Y.exe MD5: A9819B4B8CA61D132FAA30C59482C10F)
- **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
00000000.00000002.420611463.0000000003784000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.421382198.000000000458A000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.421382198.000000000458A000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000004.00000000.414625419.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000000.414625419.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.6R24hlXGVS56Z6Y.exe.45f54d8.7.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.6R24hlXGVS56Z6Y.exe.45f54d8.7.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.6R24hlXGVS56Z6Y.exe.45f54d8.7.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
4.0.6R24hlXGVS56Z6Y.exe.400000.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.0.6R24hlXGVS56Z6Y.exe.400000.6.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 39 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

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

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)

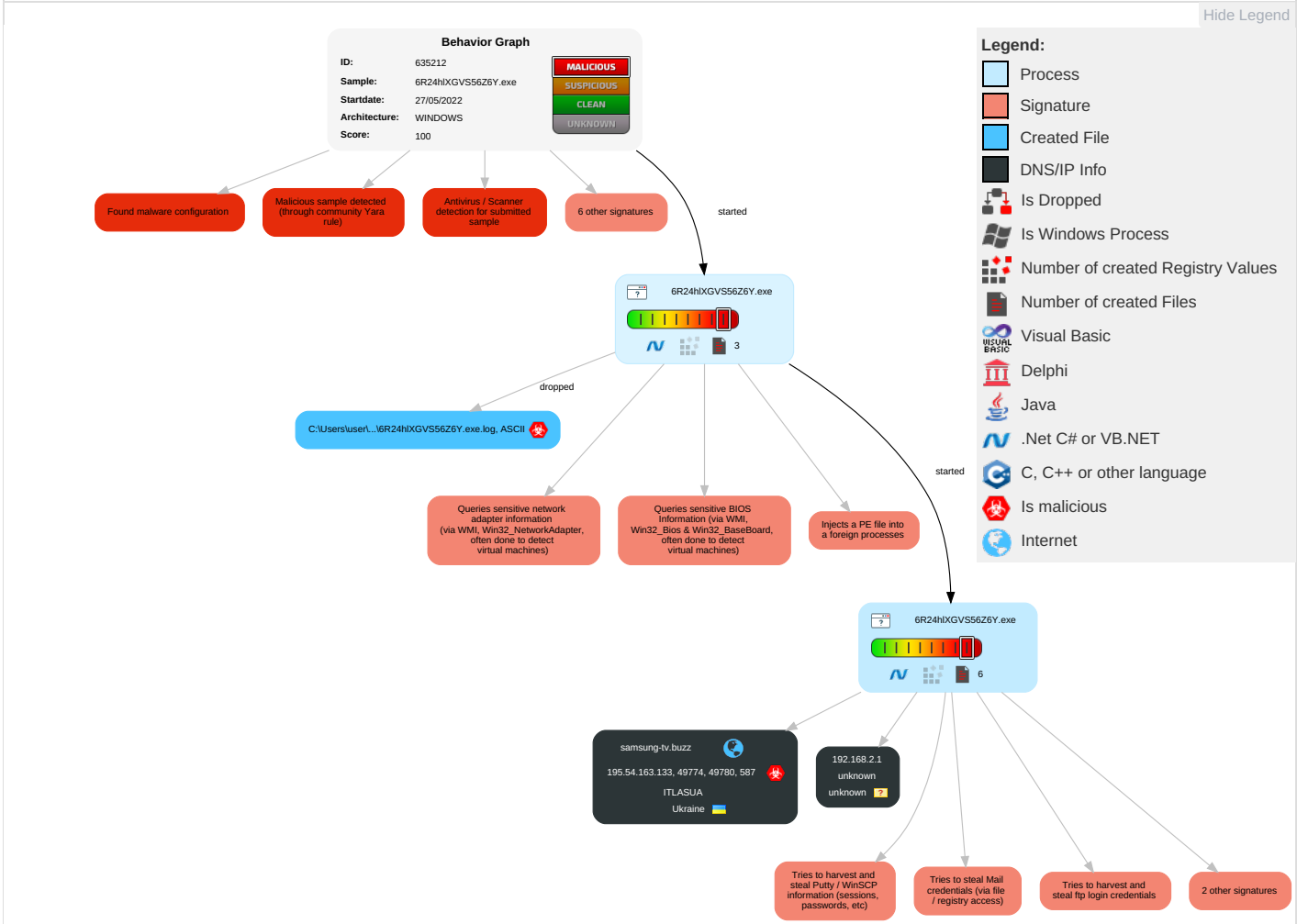
Remote Access Functionality

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 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)	2 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)	3 Software Packing	NTDS	1 Process Discovery	Distributed Component Object Model	1 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

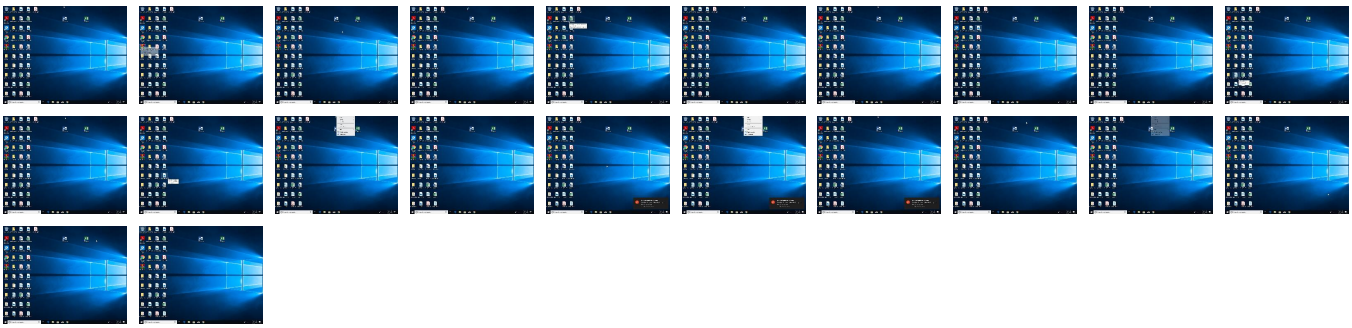
Behavior Graph



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
6R24hlXGVS56Z6Y.exe	37%	Virustotal		Browse
6R24hlXGVS56Z6Y.exe	62%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
6R24hlXGVS56Z6Y.exe	100%	Avira	HEUR/AGEN.1235153	
6R24hlXGVS56Z6Y.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.6R24hlXGVS56Z6Y.exe.600000.1.unpack	100%	Avira	HEUR/AGEN.1235153		Download File
4.0.6R24hlXGVS56Z6Y.exe.600000.11.unpack	100%	Avira	HEUR/AGEN.1235153		Download File
4.0.6R24hlXGVS56Z6Y.exe.600000.7.unpack	100%	Avira	HEUR/AGEN.1235153		Download File
4.0.6R24hlXGVS56Z6Y.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File

Source	Detection	Scanner	Label	Link	Download
4.0.6R24hlXGVS56Z6Y.exe.600000.1.unpack	100%	Avira	HEUR/AGEN.1235153		Download File
4.0.6R24hlXGVS56Z6Y.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
0.2.6R24hlXGVS56Z6Y.exe.fb0000.0.unpack	100%	Avira	HEUR/AGEN.1235153		Download File
4.0.6R24hlXGVS56Z6Y.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.6R24hlXGVS56Z6Y.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.6R24hlXGVS56Z6Y.exe.600000.5.unpack	100%	Avira	HEUR/AGEN.1235153		Download File
4.0.6R24hlXGVS56Z6Y.exe.600000.2.unpack	100%	Avira	HEUR/AGEN.1235153		Download File
4.0.6R24hlXGVS56Z6Y.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.6R24hlXGVS56Z6Y.exe.600000.13.unpack	100%	Avira	HEUR/AGEN.1235153		Download File
0.0.6R24hlXGVS56Z6Y.exe.fb0000.0.unpack	100%	Avira	HEUR/AGEN.1235153		Download File
4.0.6R24hlXGVS56Z6Y.exe.600000.0.unpack	100%	Avira	HEUR/AGEN.1235153		Download File
4.0.6R24hlXGVS56Z6Y.exe.600000.9.unpack	100%	Avira	HEUR/AGEN.1235153		Download File
4.2.6R24hlXGVS56Z6Y.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.0.6R24hlXGVS56Z6Y.exe.600000.3.unpack	100%	Avira	HEUR/AGEN.1235153		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://www.goodfont.co.krom	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://ocsp.suscerte.gob.ve0	0%	URL Reputation	safe	
http://www.sandoll.co.krn-uK	0%	Avira URL Cloud	safe	
http://crl.dhimyotis.com/certignarootca.crl0	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	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://www.fontbureau.comalsF	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.founder.com.cn/cnht	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/dpc0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/8	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.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/$	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://policy.camerfirma.com0	0%	URL Reputation	safe	
http://www.carterandcone.coma	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	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://www.jiyu-kobo.co.jp/P	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://www.jiyu-kobo.co.jp/K	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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.jiyu-kobo.co.jp/B	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://ac.economia.gob.mx/last.crl0G	0%	URL Reputation	safe	
http://www.carterandcone.comof	0%	URL Reputation	safe	
http://https://EEMzZM29crUf0q.org	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/l	0%	URL Reputation	safe	
http://crl.oces.trust2408.com/oces.crl0	0%	URL Reputation	safe	
http://www.fontbureau.comals	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://www.fontbureau.comsivo$	0%	Avira URL Cloud	safe	
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	0%	URL Reputation	safe	
http://www.carterandcone.com$	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ue	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.sandoll.co.krs-c	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	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.urwpp.de	0%	URL Reputation	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.jiyu-kobo.co.jp/wa	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	
http://samsung-tv.buzz	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/LCRacraizv1.crl0	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/va	0%	URL Reputation	safe	
http://crl.defence.gov.au/pki0	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.goodfont.co.krom	6R24hlXGVS56Z6Y.exe, 00000000.00000003.382834582.00000000063BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.455661936.0000000006803000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454554430.0000006803000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3.crl0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454993017.0000000006B44000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.suscerte.gob.ve0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454658986.0000000006C0D000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454993017.0000006B44000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krn-uK	6R24hlXGVS56Z6Y.exe, 00000000.00000003.382834582.00000000063BB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.dhimyotis.com/certignarootca.crl0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454786394.00000000067A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://sertifikati.ca.posta.rs/crl/PostaCARoot.crl0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454993017.0000000006B44000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.chambersign.org1	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454846865.0000000006BD8000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454934585.0000006BE6000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454945162.0000000006BEA000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454868163.0000000006BDD000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454658986.0000000006C0D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://repository.swisssign.com/0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454808555.0000000006BEE000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454835669.0000006BCC000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454993017.0000000006B44000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers	6R24hlXGVS56Z6Y.exe, 00000000.00000002.424564318.00000000076B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454808555.0000000006BEE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.ssc.lt/root-c/cacrl.crl0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454610878.00000000067A8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comalsF	6R24hlXGVS56Z6Y.exe, 00000000.00000003.389936973.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.389669965.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.390078961.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.389700798.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.390236620.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.389756587.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.390181420.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.389842823.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.390014696.00000000063BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ca.disig.sk/ca/crl/ca_disig.crl0	6R24hlXGVS56Z6Y.exe, 00000004.00000002.642919631.0000000006788000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454797413.00000067A5000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.455786336.00000000067A5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnht	6R24hlXGVS56Z6Y.exe, 00000000.00000003.383405212.00000000063BE000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.383502102.00000063C4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.suscerte.gob.ve/dpc0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454658986.0000000006C0D000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454993017.0000000006B44000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/8	6R24hlXGVS56Z6Y.exe, 00000000.00000003.387216615.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387557703.00000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387393990.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387671462.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387511186.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386885596.00000000063C2000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387083177.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387603719.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386706578.00000000063C2000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387338083.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387167162.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387307595.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387434200.00000000063C3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.disig.sk/ca/crl/ca_disig.crl0	6R24hlXGVS56Z6Y.exe, 00000004.00000002.642919631.0000000006788000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454797413.00000067A5000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.455786336.00000000067A5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	6R24hlXGVS56Z6Y.exe, 00000000.00000002.424564318.00000000076B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/Y0	6R24hlXGVS56Z6Y.exe, 00000000.00000003.387216615.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386534111.00000063C0000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387393990.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386490365.00000000063C1000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386885596.00000000063C2000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387083177.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386706578.00000000063C2000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387338083.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387167162.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387307595.00000000063C3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/$	6R24hlXGVS56Z6Y.exe, 00000000.00000003.386534111.00000000063C0000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386490365.00000063C1000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386329788.00000000063C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	6R24hlXGVS56Z6Y.exe, 00000000.00000002.424564318.00000000076B2000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.385016258.00000063BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.como.	6R24hlXGVS56Z6Y.exe, 00000000.00000003.385570624.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.385224109.00000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.385477472.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.385675011.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.385426375.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.385342011.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.385736791.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.385279210.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.385162735.00000000063BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%	6R24hlXGVS56Z6Y.exe, 00000004.00000002.639930761.00000000029C1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://pki.registradores.org/normativa/index.htm0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454610878.00000000067A8000.00000004.00000800.00020000.00000000.sdmp	false		high
http://policy.camerfirma.com0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454846865.0000000006BD8000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454691889.0000006BFF000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454868163.0000000006BDD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.anf.es/es/address-direccion.html	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454808555.0000000006BEE000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.coma	6R24hlXGVS56Z6Y.exe, 00000000.00000003.385224109.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.385426375.00000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.385342011.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.385279210.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.385162735.00000000063BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.anf.es/address/)1(0&	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454993017.0000000006B44000.00000004.00000800.00020000.00000000.sdmp	false		high
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454846865.0000000006BD8000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.455022172.0000000006B60000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454934585.0000000006BE6000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454945162.0000000006BEA000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.466720672.0000000006BC6000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.455216418.0000000006BC0000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454868163.0000000006BDD000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.465548130.0000000006BC3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000002.643882853.0000000006BC6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://cps.letsencrypt.org0	6R24hlXGVS56Z6Y.exe, 00000004.00000002.640954405.0000000002D21000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.465916495.00000067B7000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000002.641105197.0000000002D5F000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000002.642983870.00000000067B8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.ssc.lt/root-b/cacrl.crl0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454691889.0000000006BFF000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454776252.0000000006C05000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.certicamara.com/dpc/0Z	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454993017.0000000006B44000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454846865.0000000006BD8000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454868163.0000000006BDD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.pki.wellsfargo.com/wsprca.crl0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.461073416.0000000006B2E000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.455241825.0000000006B2C000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/P	6R24hlXGVS56Z6Y.exe, 00000000.00000003.386885596.00000000063C2000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386706578.00000000063C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://wwww.certigna.fr/autorites/0m	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454786394.00000000067A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454691889.0000000006BFF000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454825636.0000000C02000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/K	6R24hlXGVS56Z6Y.exe, 00000000.00000003.387216615.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386534111.00000063C0000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386261996.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386490365.00000000063C1000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386199122.00000000063BC000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386885596.00000000063C2000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386167015.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387083177.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386706578.00000000063C2000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387167162.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386329788.00000000063C2000.00000004.00000800.00020000.00000000.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	6R24hlXGVS56Z6Y.exe, 00000004.00000002.639930761.00000000029C1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.anf.es/AC/ANFServerCA.crl0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454993017.0000000006B44000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.globaltrust.info0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454658986.0000000006C0D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/B	6R24hlXGVS56Z6Y.exe, 00000000.00000003.387216615.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386534111.00000063C0000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386261996.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386490365.00000000063C1000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386199122.00000000063BC000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386885596.00000000063C2000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386167015.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387083177.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386706578.00000000063C2000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387167162.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386329788.00000000063C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	6R24hlXGVS56Z6Y.exe, 00000000.00000002.424564318.00000000076B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ac.economia.gob.mx/last.crl0G	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454658986.0000000006C0D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comof	6R24hlXGVS56Z6Y.exe, 00000000.00000003.385224109.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.385342011.00000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.385279210.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.385162735.00000000063BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://EEMzZM29crUf0q.org	6R24hlXGVS56Z6Y.exe, 00000004.00000002.639930761.00000000029C1000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000002.640941183.00000000002D1B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1.crt0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454835669.0000000006BCC000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/l	6R24hlXGVS56Z6Y.exe, 00000000.00000003.387216615.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386534111.00000063C0000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386261996.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387393990.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386490365.00000000063C1000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386885596.00000000063C2000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387083177.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386706578.00000000063C2000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387338083.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387167162.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387307595.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386329788.00000000063C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.oces.trust2408.com/oces.crl0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454808555.0000000006BEE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://eca.hinet.net/repository0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454846865.0000000006BD8000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454868163.0000000006BDD000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comals	6R24hlXGVS56Z6Y.exe, 00000000.00000003.389936973.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.390078961.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.390236620.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.390181420.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.390014696.00000000063BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://certs.oaticerts.com/repository/OATICA2.crl	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454913928.0000000006BFE000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454808555.0000000006BEE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://certs.oati.net/repository/OATICA2.crt0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454691889.0000000006BFF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.accv.es00	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454835669.0000000006BCC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comsivo$	6R24hlXGVS56Z6Y.exe, 00000000.00000003.390359522.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.389936973.00000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.390078961.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.390236620.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.390426618.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.390181420.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.389842823.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.390014696.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.390578615.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.390486046.00000000063BB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_1.pdf0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454808555.0000000006BEE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454846865.0000000006BD8000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454868163.0000000006BDD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com$	6R24hlXGVS56Z6Y.exe, 00000000.00000003.385570624.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.385224109.00000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.385477472.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.385675011.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.385426375.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.385342011.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.385736791.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.385279210.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.385162735.00000000063BB000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.datev.de/zertifikat-policy-int0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454808555.0000000006BEE000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454835669.0000000006BCC000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	6R24hlXGVS56Z6Y.exe, 00000000.00000002.424564318.00000000076B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

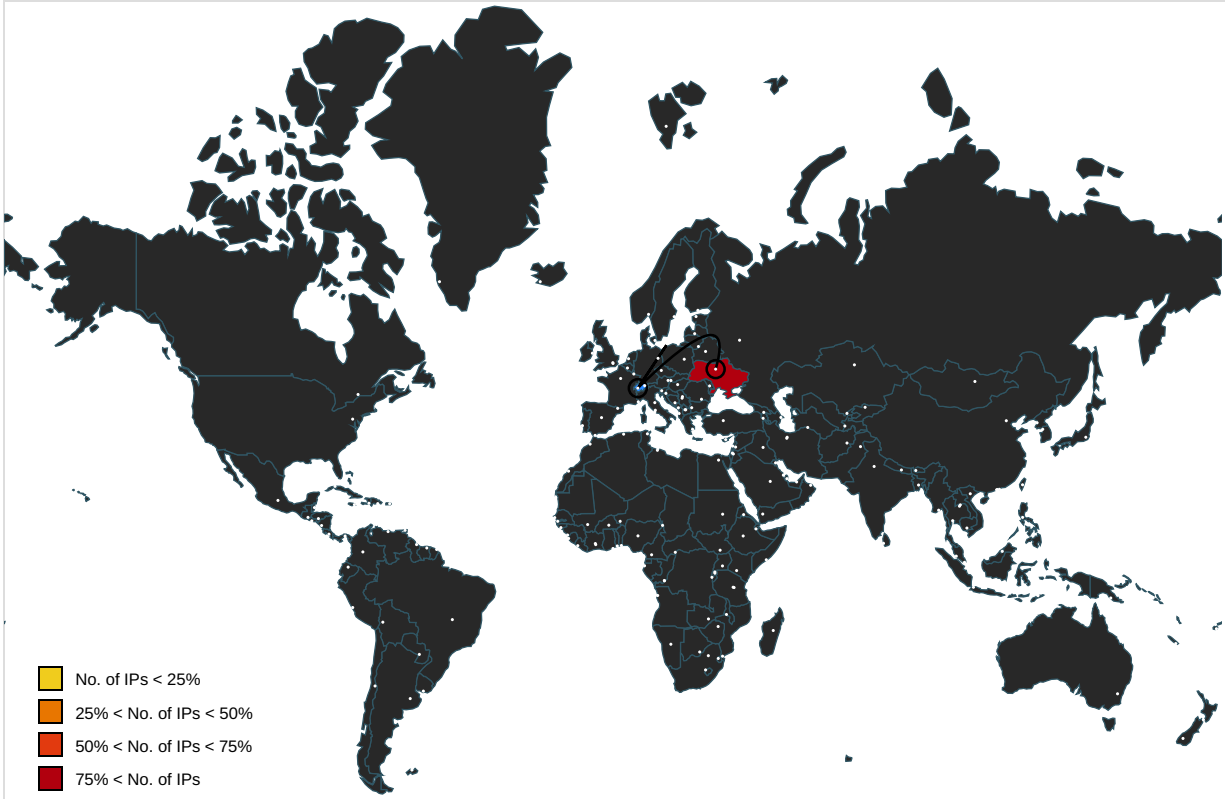
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/ue	6R24hlXGVS56Z6Y.exe, 00000000.00000003.387216615.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386885596.00000000063C2000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387083177.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386706578.00000000063C2000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387167162.00000000063C3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.acabogacia.org0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454868163.0000000006BDD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.firmaprofesional.com/cps0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.455022172.0000000006B60000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.455216418.0000000006BC0000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.ipify.org%%startupfolder%	6R24hlXGVS56Z6Y.exe, 00000004.00000002.639930761.00000000029C1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://crl.securetrust.com/SGCA.crl0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454538794.00000000067F9000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.455625077.00000000067F9000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.460720359.00000000067F9000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.agesic.gub.uy/acrn/acrn.crl0)	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454846865.0000000006BD8000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454868163.0000000006BDD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.rcsc.lt/repository0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454835669.0000000006BCC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krs-c	6R24hlXGVS56Z6Y.exe, 00000000.00000003.382834582.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.382675016.00000000063BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	6R24hlXGVS56Z6Y.exe, 00000000.00000002.424564318.00000000076B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	6R24hlXGVS56Z6Y.exe, 00000000.00000002.424564318.00000000076B2000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.380606284.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.380758503.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.380677591.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.380652171.00000000063BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://web.certicamara.com/marco-legal0Z	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454808555.0000000006BEE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.quovadisglobal.com/cps0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454610878.00000000067A8000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://x1.c.lencr.org/0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.466057935.0000000006803000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000002.640954405.0000002D21000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000002.643187937.000000006803000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000002.641105197.0000000002D5F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://x1.i.lencr.org/0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.466057935.0000000006803000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000002.640954405.0000002D21000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000002.643187937.000000006803000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000002.641105197.0000000002D5F000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	6R24hlXGVS56Z6Y.exe, 00000004.00000002.639930761.00000000029C1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	6R24hlXGVS56Z6Y.exe, 00000000.00000002.424564318.00000000076B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	6R24hlXGVS56Z6Y.exe, 00000000.00000003.382834582.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.382905321.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000002.424564318.00000000076B2000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.382675016.00000000063BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	6R24hlXGVS56Z6Y.exe, 00000000.00000003.388329849.00000000063BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://certs.oaticerts.com/repository/OATICA2.crt08	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454691889.0000000006BFF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://cps.chambersign.org/cps/chambersignroot.html0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454658986.0000000006C0D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.anf.es/AC/RC/ocsp0c	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454993017.0000000006B44000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/wa	6R24hlXGVS56Z6Y.exe, 00000000.00000003.386534111.00000000063C0000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386490365.00000000063C1000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386329788.00000000063C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.oaticerts.com/repository.	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454691889.0000000006BFF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ancert.com/cps0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454610878.00000000067A8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.accv.es0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454835669.0000000006BCC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://acraiz.icpbrasil.gov.br/LCRacraizv2.crl0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.455022172.0000000006B60000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.466720672.0000000006BC6000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.455216418.0000000006BC0000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.465548130.0000000006BC3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000002.643882853.0000000006BC6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.echoworx.com/ca/root2/cps.pdf0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454993017.0000000006B44000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://rca.e-szigno.hu/ocsp0-	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454610878.00000000067A8000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ca.mtin.es/mtin/crl/MTINAutoridadRaiz03	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454808555.0000000006BEE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://samsung-tv.buzz	6R24hlXGVS56Z6Y.exe, 00000004.00000002.640954405.0000000002D21000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000002.641105197.0000000002D5F000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://eca.hinet.net/repository/CRL2/CA.crl0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454846865.0000000006BD8000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454868163.0000000006BDD000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.datev.de/zertifikat-policy-std0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.455022172.0000000006B60000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.455216418.0000000006BC0000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454610878.00000000067A8000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/	6R24hlXGVS56Z6Y.exe, 00000000.00000003.387216615.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386534111.00000000063C0000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387393990.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386490365.00000000063C1000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386885596.00000000063C2000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387083177.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386706578.00000000063C2000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387338083.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387167162.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.387307595.00000000063C3000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://acraiz.icpbrasil.gov.br/LCRacraizv1.crl0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454846865.0000000006BD8000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454934585.0000000006BE6000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454945162.0000000006BEA000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.454868163.0000000006BDD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	6R24hlXGVS56Z6Y.exe, 00000000.00000002.424564318.00000000076B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	6R24hlXGVS56Z6Y.exe, 00000000.00000003.383604980.00000000063BB000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.384160713.00000000063C3000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.384516970.00000000063BB000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/va	6R24hlXGVS56Z6Y.exe, 00000000.00000003.386534111.00000000063C0000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386490365.00000000063C1000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386885596.00000000063C2000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386706578.00000000063C2000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000000.00000003.386329788.00000000063C2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.informatik.admin.ch/PKI/links/CPS_2_16_756_1_17_3_1_0.pdf0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.454610878.00000000067A8000.00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.defence.gov.au/pki0	6R24hlXGVS56Z6Y.exe, 00000004.00000003.455022172.0000000006B60000.00000004.00000800.00020000.00000000.sdmp, 6R24hlXGVS56Z6Y.exe, 00000004.00000003.455216418.0000000006BC0000.00000004.00000800.00020000.00000000.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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635212
Start date and time: 27/05/202217:06:05	2022-05-27 17:06:05 +02:00

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	6R24hlXGVS56Z6Y.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:	20
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@2/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 2.2% (good quality ratio 1.7%) • Quality average: 19.5% • Quality standard deviation: 21.5%
HCA Information:	• Successful, ratio: 100% • 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, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 173.222.108.226, 173.222.108.210, 8.241.9.126, 8.241.79.254, 8.248.131.254, 8.241.9.254, 8.252.5.126
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fg.download.windowsupdate.com.c.footprint.net, fs.microsoft.com, ctldl.windowsupdate.com, a767.dspw65.akamai.net, arc.msn.com, wu-bg-shim.trafficmanager.net, download.windowsupdate.com.edgesuite.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.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
17:07:32	API Interceptor	650x Sleep call for process: 6R24hlXGVS56Z6Y.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\6R24hlXGVS56Z6Y.exe
File Type:	Microsoft Cabinet archive data, 61476 bytes, 1 file
Category:	dropped
Size (bytes):	61476
Entropy (8bit):	**7.995018321729444**
Encrypted:	**true**
SSDEEP:	1536:NATLwfiuePkACih0/8uIwf5CiqGLhk1V/AFnGegJR:N7nePk5gKsoBha/0GTf
MD5:	308336E7F515478969B24C13DED11EDE
SHA1:	8FB0CF42B77DBBEF224A1E5FC38ABC2486320775
SHA-256:	889B832323726A9F10AD03F85562048FDCFE20C9FF6F9D37412CF477B4E92FF9
SHA-512:	61AD97228CD6C3909EF3AC5E4940199971F293BDD0D5EB7916E60469573A44B6287C0FA1E0B6C1389DF35EB6C9A7D2A61FDB318D4A886A3821EF5A9DAB3AC2F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF....$.....,.....I.....w.....Tp. .authroot.stl.H#F..4..CK..<Tk...c_.d....A.F...,.&K..*i.RJJ..J.".%.KY"{n...."{..Lu3.Ln.....y.....M.:...<. v...H..~.#Ov.a0xN....)..C..t.z.,x.00.1``L.....L.\..1.|..2.1.0mD...H1/.....G..UT7!...r.X:....D.0.0...M....I(.-.+..v#...(.r.....z.Y`&hw..Gl+.je.e.j..{.1.....9f=.&.....s.W...L.].+...).f...u.....8....}R...w.X..>.A.Yw...a.x..T8V.e...^.7.q..t^.+....f.q).B.M.....64.<!W(.....D!.0.t "X...l.....D0.....+...A.....0.o..t93.v..O1V x}H.S)....GH.6.I...p2.(4k.....!,.L`.....h:.a]?.....J9.\..Ww.....%.....a4E...q.*...#..a..y..M..R.t..Z2!.T.Ua.k.'O..\./ d.F>.V...3...._.J....."....wI..'..z...j..Ds...qZ...[.....O<.d.K..hH@c1....[w7..z...I....h,.b.....'.w.....bO.i{.....+.-...H..."<...L.Tu}.Y.lB.]3..4..G.3..`E..NF.....{o.h]}p....G..$..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\6R24hlXGVS56Z6Y.exe
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.1008650894945404
Encrypted:	false
SSDEEP:	6:kKbXBmN+SkQlPlEGYRMY9z+4KlDA3RUecl7PG1:PkPlE99SNxAhUecl61
MD5:	73613CA04B78246223E042C2C658801F
SHA1:	1E28BFB3D44CA59265AB73743E70E5142E62345B
SHA-256:	425A28548A28D23A991340FF23F25679B3C6CF61F817A95E20D03271DCAA317B
SHA-512:	638B2416F7D87E6AE24B3D284EE725EE0F72B23C59CBC0174BBA40602A71B798E9CEBB067A702A3B7398407CF22A046D31EDE601358D30BD1BA9B584C54CDA12
Malicious:	false
Reputation:	low
Preview:	p..... .....N..+r..(..... .....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\6R24hlXGVS56Z6Y.exe.log

Process:	C:\Users\user\Desktop\6R24hlXGVS56Z6Y.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\pbnwtogd.e0p\Chrome\Default\Cookies

Process:	C:\Users\user\Desktop\6R24hlXGVS56Z6Y.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	modified
Size (bytes):	20480
Entropy (8bit):	0.6951152985249047
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBopIvJn2QOYiUG3PaVrX:T5LLOpEO5J/Kn7U1uBopIvZXC/alX
MD5:	EA7F9615D77815B5FFF7C15179C6C560
SHA1:	3D1D0BAC6633344E2B6592464EBB957D0D8DD48F
SHA-256:	A5D1ABB57C516F4B3DF3D18950AD1319BA1A63F9A39785F8F0EACE0A482CAB17
SHA-512:	9C818471F69758BD4884FDB9B543211C9E1EE832AC29C2C5A0377C412454E8C745FB3F38FF6E3853AE365D04933C0EC55A46DDA60580D244B308F92C57258C9
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):	7.821023279624439
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	6R24hlXGVS56Z6Y.exe
File size:	670720
MD5:	a9819b4b8ca61d132faa30c59482c10f
SHA1:	226725a9f34ade061c288e6a6faddd944fec8868
SHA256:	86a8ba97bde5b049538c73c0e8fc0484a0883422944eb5b988eec2233d004837
SHA512:	d5f258ced031dfcb55c5b50be6d86029da4ee56a323950ac22c8d39d1f9003f76ef9183694558d2e50041326d96358b4cb3ee0fbffb1572db500a4e8dc0e858f
SSDEEP:	12288:m5lbHo6UHQKywl4DsE84eys2wSO4h0VR81ZnUv3/rWXMnM3jNbazUatGG:qbHoSY+X59O4mVRaVA6XIMz4zUmGG
TLSH:	8EE40119F771A9E6E45C03BE3071183A2F64CB33E5BEE65D68A8711328742C6055BECB
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....L..... ... .@.. .....@.....

File Icon

Icon Hash:	31b1393969391b39

Static PE Info

General

Entrypoint:	0x4a0cce
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x628FCA9D [Thu May 26 18:44:45 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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa0c74	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa2000	0x488c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa8000	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	0x9ecd4	0x9ee00	False	0.89987737264	data	7.84091961833	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa2000	0x488c	0x4a00	False	0.663481841216	data	6.51566732649	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa8000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xa2130	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	0xa6358	0x14	data		
RT_VERSION	0xa636c	0x36c	data		
RT_MANIFEST	0xa66d8	0x1b4	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

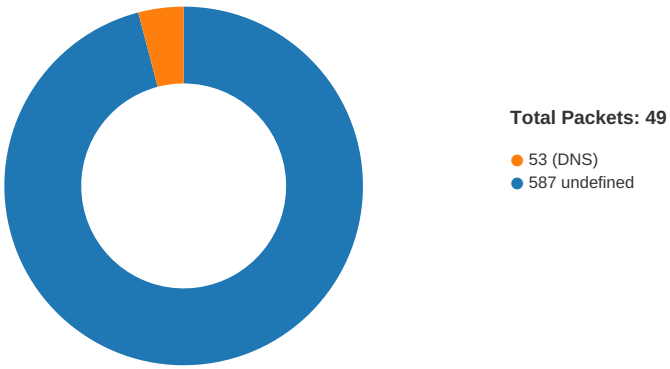
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2017
Assembly Version	1.0.0.0
InternalName	InternalRemotingServi.exe
FileVersion	1.0.0.0
CompanyName	Microsoft
LegalTrademarks	
Comments	

Description	Data
ProductName	BlockGame App
ProductVersion	1.0.0.0
FileDescription	BlockGame App
OriginalFilename	InternalRemotingServi.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 17:07:49.467278957 CEST	49774	587	192.168.2.6	195.54.163.133
May 27, 2022 17:07:49.519980907 CEST	587	49774	195.54.163.133	192.168.2.6
May 27, 2022 17:07:49.520078897 CEST	49774	587	192.168.2.6	195.54.163.133
May 27, 2022 17:07:50.788113117 CEST	587	49774	195.54.163.133	192.168.2.6
May 27, 2022 17:07:50.793912888 CEST	49774	587	192.168.2.6	195.54.163.133
May 27, 2022 17:07:50.846843004 CEST	587	49774	195.54.163.133	192.168.2.6
May 27, 2022 17:07:50.847846031 CEST	49774	587	192.168.2.6	195.54.163.133
May 27, 2022 17:07:50.902426004 CEST	587	49774	195.54.163.133	192.168.2.6
May 27, 2022 17:07:50.975701094 CEST	49774	587	192.168.2.6	195.54.163.133
May 27, 2022 17:07:51.033668041 CEST	587	49774	195.54.163.133	192.168.2.6
May 27, 2022 17:07:51.033704996 CEST	587	49774	195.54.163.133	192.168.2.6
May 27, 2022 17:07:51.033727884 CEST	587	49774	195.54.163.133	192.168.2.6
May 27, 2022 17:07:51.033746958 CEST	587	49774	195.54.163.133	192.168.2.6
May 27, 2022 17:07:51.033838987 CEST	49774	587	192.168.2.6	195.54.163.133
May 27, 2022 17:07:51.033890009 CEST	49774	587	192.168.2.6	195.54.163.133
May 27, 2022 17:07:51.035263062 CEST	587	49774	195.54.163.133	192.168.2.6
May 27, 2022 17:07:51.068314075 CEST	49774	587	192.168.2.6	195.54.163.133
May 27, 2022 17:07:51.123451948 CEST	587	49774	195.54.163.133	192.168.2.6
May 27, 2022 17:07:51.227827072 CEST	49774	587	192.168.2.6	195.54.163.133
May 27, 2022 17:07:58.210067987 CEST	49774	587	192.168.2.6	195.54.163.133
May 27, 2022 17:07:58.262901068 CEST	587	49774	195.54.163.133	192.168.2.6
May 27, 2022 17:07:58.263456106 CEST	49774	587	192.168.2.6	195.54.163.133
May 27, 2022 17:07:58.316687107 CEST	587	49774	195.54.163.133	192.168.2.6
May 27, 2022 17:07:58.317521095 CEST	49774	587	192.168.2.6	195.54.163.133
May 27, 2022 17:07:58.381045103 CEST	587	49774	195.54.163.133	192.168.2.6
May 27, 2022 17:07:58.382733107 CEST	49774	587	192.168.2.6	195.54.163.133
May 27, 2022 17:07:58.437756062 CEST	587	49774	195.54.163.133	192.168.2.6
May 27, 2022 17:07:58.438234091 CEST	49774	587	192.168.2.6	195.54.163.133
May 27, 2022 17:07:58.531240940 CEST	587	49774	195.54.163.133	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 17:07:58.532419920 CEST	49774	587	192.168.2.6	195.54.163.133
May 27, 2022 17:07:58.585324049 CEST	587	49774	195.54.163.133	192.168.2.6
May 27, 2022 17:07:58.586633921 CEST	49774	587	192.168.2.6	195.54.163.133
May 27, 2022 17:07:58.586780071 CEST	49774	587	192.168.2.6	195.54.163.133
May 27, 2022 17:07:58.587353945 CEST	49774	587	192.168.2.6	195.54.163.133
May 27, 2022 17:07:58.587445021 CEST	49774	587	192.168.2.6	195.54.163.133
May 27, 2022 17:07:58.639424086 CEST	587	49774	195.54.163.133	192.168.2.6
May 27, 2022 17:07:58.639447927 CEST	587	49774	195.54.163.133	192.168.2.6
May 27, 2022 17:07:58.639707088 CEST	587	49774	195.54.163.133	192.168.2.6
May 27, 2022 17:07:58.639774084 CEST	587	49774	195.54.163.133	192.168.2.6
May 27, 2022 17:07:58.642030001 CEST	587	49774	195.54.163.133	192.168.2.6
May 27, 2022 17:07:58.737564087 CEST	49774	587	192.168.2.6	195.54.163.133
May 27, 2022 17:08:01.502274036 CEST	49774	587	192.168.2.6	195.54.163.133
May 27, 2022 17:08:01.594315052 CEST	587	49774	195.54.163.133	192.168.2.6
May 27, 2022 17:08:01.831399918 CEST	587	49774	195.54.163.133	192.168.2.6
May 27, 2022 17:08:01.832993984 CEST	49774	587	192.168.2.6	195.54.163.133
May 27, 2022 17:08:01.936984062 CEST	49780	587	192.168.2.6	195.54.163.133
May 27, 2022 17:08:01.989752054 CEST	587	49780	195.54.163.133	192.168.2.6
May 27, 2022 17:08:01.990533113 CEST	49780	587	192.168.2.6	195.54.163.133
May 27, 2022 17:08:02.093596935 CEST	587	49780	195.54.163.133	192.168.2.6
May 27, 2022 17:08:02.093878984 CEST	49780	587	192.168.2.6	195.54.163.133
May 27, 2022 17:08:02.146786928 CEST	587	49780	195.54.163.133	192.168.2.6
May 27, 2022 17:08:02.153640985 CEST	49780	587	192.168.2.6	195.54.163.133
May 27, 2022 17:08:02.209285975 CEST	587	49780	195.54.163.133	192.168.2.6
May 27, 2022 17:08:02.209944010 CEST	49780	587	192.168.2.6	195.54.163.133
May 27, 2022 17:08:02.276432037 CEST	587	49780	195.54.163.133	192.168.2.6
May 27, 2022 17:08:02.276474953 CEST	587	49780	195.54.163.133	192.168.2.6
May 27, 2022 17:08:02.276516914 CEST	587	49780	195.54.163.133	192.168.2.6
May 27, 2022 17:08:02.276531935 CEST	587	49780	195.54.163.133	192.168.2.6
May 27, 2022 17:08:02.276659012 CEST	49780	587	192.168.2.6	195.54.163.133
May 27, 2022 17:08:02.279386044 CEST	587	49780	195.54.163.133	192.168.2.6
May 27, 2022 17:08:02.282840967 CEST	49780	587	192.168.2.6	195.54.163.133
May 27, 2022 17:08:02.336025953 CEST	587	49780	195.54.163.133	192.168.2.6
May 27, 2022 17:08:02.431888103 CEST	49780	587	192.168.2.6	195.54.163.133
May 27, 2022 17:08:03.304214954 CEST	49780	587	192.168.2.6	195.54.163.133
May 27, 2022 17:08:03.356868982 CEST	587	49780	195.54.163.133	192.168.2.6
May 27, 2022 17:08:03.357686043 CEST	49780	587	192.168.2.6	195.54.163.133
May 27, 2022 17:08:03.410973072 CEST	587	49780	195.54.163.133	192.168.2.6
May 27, 2022 17:08:03.412344933 CEST	49780	587	192.168.2.6	195.54.163.133
May 27, 2022 17:08:03.466396093 CEST	587	49780	195.54.163.133	192.168.2.6
May 27, 2022 17:08:03.466887951 CEST	49780	587	192.168.2.6	195.54.163.133
May 27, 2022 17:08:03.519746065 CEST	587	49780	195.54.163.133	192.168.2.6
May 27, 2022 17:08:03.520354986 CEST	49780	587	192.168.2.6	195.54.163.133
May 27, 2022 17:08:03.609772921 CEST	587	49780	195.54.163.133	192.168.2.6
May 27, 2022 17:08:03.610182047 CEST	49780	587	192.168.2.6	195.54.163.133
May 27, 2022 17:08:03.663034916 CEST	587	49780	195.54.163.133	192.168.2.6
May 27, 2022 17:08:03.666685104 CEST	49780	587	192.168.2.6	195.54.163.133
May 27, 2022 17:08:03.666870117 CEST	49780	587	192.168.2.6	195.54.163.133
May 27, 2022 17:08:03.666899920 CEST	49780	587	192.168.2.6	195.54.163.133
May 27, 2022 17:08:03.666997910 CEST	49780	587	192.168.2.6	195.54.163.133
May 27, 2022 17:08:03.667155027 CEST	49780	587	192.168.2.6	195.54.163.133
May 27, 2022 17:08:03.667238951 CEST	49780	587	192.168.2.6	195.54.163.133
May 27, 2022 17:08:03.667314053 CEST	49780	587	192.168.2.6	195.54.163.133
May 27, 2022 17:08:03.667390108 CEST	49780	587	192.168.2.6	195.54.163.133
May 27, 2022 17:08:03.719479084 CEST	587	49780	195.54.163.133	192.168.2.6
May 27, 2022 17:08:03.719531059 CEST	587	49780	195.54.163.133	192.168.2.6
May 27, 2022 17:08:03.719542027 CEST	587	49780	195.54.163.133	192.168.2.6
May 27, 2022 17:08:03.719558001 CEST	587	49780	195.54.163.133	192.168.2.6
May 27, 2022 17:08:03.719616890 CEST	587	49780	195.54.163.133	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 17:08:03.719657898 CEST	587	49780	195.54.163.133	192.168.2.6
May 27, 2022 17:08:03.719672918 CEST	587	49780	195.54.163.133	192.168.2.6
May 27, 2022 17:08:03.719686985 CEST	587	49780	195.54.163.133	192.168.2.6
May 27, 2022 17:08:03.719865084 CEST	587	49780	195.54.163.133	192.168.2.6
May 27, 2022 17:08:03.723057032 CEST	587	49780	195.54.163.133	192.168.2.6
May 27, 2022 17:08:03.822653055 CEST	49780	587	192.168.2.6	195.54.163.133
May 27, 2022 17:09:29.357263088 CEST	49780	587	192.168.2.6	195.54.163.133
May 27, 2022 17:09:29.449362993 CEST	587	49780	195.54.163.133	192.168.2.6
May 27, 2022 17:09:29.683396101 CEST	587	49780	195.54.163.133	192.168.2.6
May 27, 2022 17:09:29.684130907 CEST	49780	587	192.168.2.6	195.54.163.133

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 17:07:49.407982111 CEST	61116	53	192.168.2.6	8.8.8.8
May 27, 2022 17:07:49.438499928 CEST	53	61116	8.8.8.8	192.168.2.6
May 27, 2022 17:08:01.902328968 CEST	50029	53	192.168.2.6	8.8.8.8
May 27, 2022 17:08:01.933845043 CEST	53	50029	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 17:07:49.407982111 CEST	192.168.2.6	8.8.8.8	0x9836	Standard query (0)	samsung-tv.buzz	A (IP address)	IN (0x0001)
May 27, 2022 17:08:01.902328968 CEST	192.168.2.6	8.8.8.8	0x8455	Standard query (0)	samsung-tv.buzz	A (IP address)	IN (0x0001)

DNS Answers

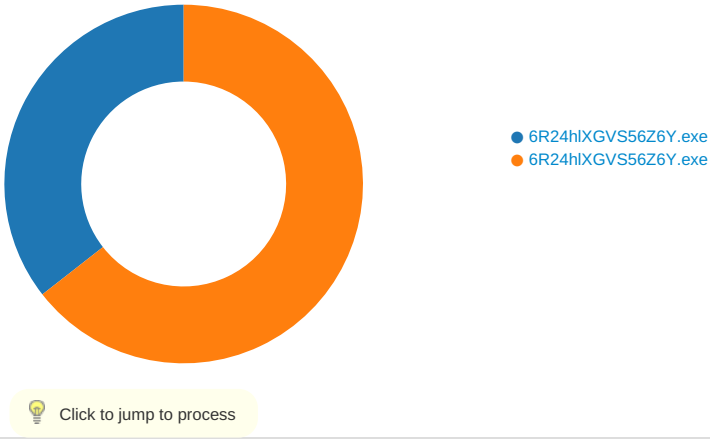
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 17:07:49.438499928 CEST	8.8.8.8	192.168.2.6	0x9836	No error (0)	samsung-tv.buzz		195.54.163.133	A (IP address)	IN (0x0001)
May 27, 2022 17:08:01.933845043 CEST	8.8.8.8	192.168.2.6	0x8455	No error (0)	samsung-tv.buzz		195.54.163.133	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 27, 2022 17:07:50.788113117 CEST	587	49774	195.54.163.133	192.168.2.6	220-cp5ua.hyperhost.ua ESMTP Exim 4.95 #2 Fri, 27 May 2022 18:07:50 +0300 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 27, 2022 17:07:50.793912888 CEST	49774	587	192.168.2.6	195.54.163.133	EHLO 358075
May 27, 2022 17:07:50.846843004 CEST	587	49774	195.54.163.133	192.168.2.6	250-cp5ua.hyperhost.ua Hello 358075 [102.129.143.42] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-STARTTLS 250 HELP
May 27, 2022 17:07:50.847846031 CEST	49774	587	192.168.2.6	195.54.163.133	STARTTLS
May 27, 2022 17:07:50.902426004 CEST	587	49774	195.54.163.133	192.168.2.6	220 TLS go ahead
May 27, 2022 17:08:02.093596935 CEST	587	49780	195.54.163.133	192.168.2.6	220-cp5ua.hyperhost.ua ESMTP Exim 4.95 #2 Fri, 27 May 2022 18:08:01 +0300 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 27, 2022 17:08:02.093878984 CEST	49780	587	192.168.2.6	195.54.163.133	EHLO 358075
May 27, 2022 17:08:02.146786928 CEST	587	49780	195.54.163.133	192.168.2.6	250-cp5ua.hyperhost.ua Hello 358075 [102.129.143.42] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-STARTTLS 250 HELP
May 27, 2022 17:08:02.153640985 CEST	49780	587	192.168.2.6	195.54.163.133	STARTTLS
May 27, 2022 17:08:02.209285975 CEST	587	49780	195.54.163.133	192.168.2.6	220 TLS go ahead

Statistics

Behavior



System Behavior

Analysis Process: 6R24hlXGVS56Z6Y.exe PID: 6360, Parent PID: 5380

General

Target ID:	0
Start time:	17:07:20
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\6R24hlXGVS56Z6Y.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\6R24hlXGVS56Z6Y.exe"
Imagebase:	0xfb0000
File size:	670720 bytes
MD5 hash:	A9819B4B8CA61D132FAA30C59482C10F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.420611463.0000000003784000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.421382198.000000000458A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.421382198.000000000458A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_zgRAT, Description: Detects zgRAT, Source: 00000000.00000002.425573285.0000000007E20000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.419325679.00000000034B1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.422039966.000000000464E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.422039966.000000000464E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6DCCCF06	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	6DCCCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\6R24hlXGVS56Z6Y.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DFDC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\6R24hlXGVS56Z6Y.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 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	6DFDC907	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	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFF1B4F	ReadFile

Analysis Process: 6R24hlXGVS56Z6Y.exe PID: **6520**, Parent PID: **6360**

General	
Target ID:	4
Start time:	17:07:39
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\6R24hlXGVS56Z6Y.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\6R24hlXGVS56Z6Y.exe
Imagebase:	0x600000
File size:	670720 bytes
MD5 hash:	A9819B4B8CA61D132FAA30C59482C10F
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: 00000004.00000000.414625419.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.414625419.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.416014888.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.416014888.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.414120802.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.414120802.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000000.416564680.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.416564680.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.638637561.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.638637561.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.639930761.00000000029C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.639930761.00000000029C1000.00000004.00000800.00020000.00000000.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	6DCCCF06	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	6DCCCF06	unknown
C:\Users\user\AppData\Roaming\pbnwtogd.e0p	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BFFBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\pbnwtogd.e0p\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	6BFFBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\pbnwtogd.e0p\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	6BFFBEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pbnwtogd.e0p\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	6BFFDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pbnwtogd.e0p\Chrome\Default\Cookies	success or wait	1	6BFF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pbnwtogd.e0p\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 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 00 00 00 00 00 00 00	SQLite format 3@ .C g 8	success or wait	1	6BFFDD66	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	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFF1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6BFF1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6BFF1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BFF1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6BFF1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\98bd75d2-ce84-459a-aada-2da99aef3201	unknown	4096	success or wait	1	6BFF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6BFF1B4F	ReadFile
C:\Users\user\AppData\Roaming\pbnwtogd.e0p\Chrome\Default\Cookies	unknown	16384	success or wait	2	6BFF1B4F	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