ID: 358341
Sample Name: Zapytanie - 20216470859302.exe
Cookbook: default.jbs
Time: 12:43:18
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

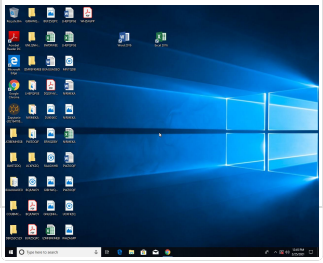
Analysis Report Zapytanie -20216470859302.exe

Overview

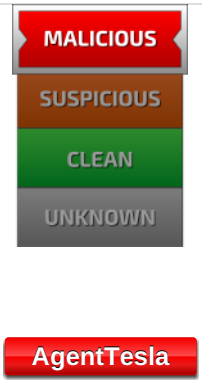
General Information

Sample Name:	Zapytanie -20216470859302.exe
Analysis ID:	358341
MD5:	d78bcccfe9e8e96..
SHA1:	d4b2f340c8df782..
SHA256:	3832cbc966b606..
Tags:	AgentTesla
Infos:	

Most interesting Screenshot:



Detection

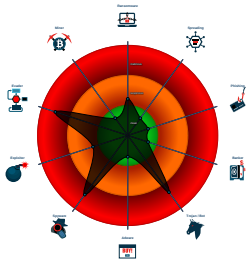


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains very larg…
- .NET source code contains very larg…
- Machine Learning detection for samp…
- May check the online IP address of …
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…

Classification



Startup

- **System is w10x64**
- Zapytanie -20216470859302.exe (PID: 7112 cmdline: 'C:\Users\user\Desktop\Zapytanie -20216470859302.exe' MD5: D78BCCCFE9E8E96D75E488DAB97BA56F)
  - Zapytanie -20216470859302.exe (PID: 2440 cmdline: C:\Users\user\Desktop\Zapytanie -20216470859302.exe MD5: D78BCCCFE9E8E96D75E488DAB97BA56F)
  - Zapytanie -20216470859302.exe (PID: 6340 cmdline: C:\Users\user\Desktop\Zapytanie -20216470859302.exe MD5: D78BCCCFE9E8E96D75E488DAB97BA56F)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "FTP Info": "comercial@fil-net.comFil-2020net+smtp.fil-net.comgreendogman@yandex.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.896326467.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.638964828.000000000311000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000003.00000002.897336626.0000000002B96000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.897276888.0000000002B41000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.897276888.0000000002B41000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Click to see the 5 entries

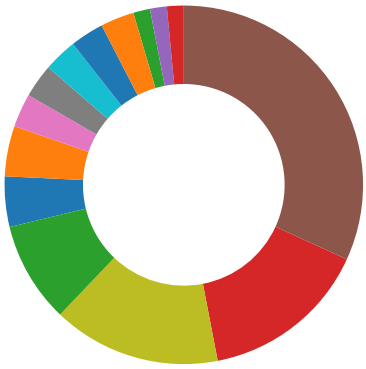
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Zapytanie -20216470859302.exe.43bca80.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.2.Zapytanie -20216470859302.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Zapytanie -20216470859302.exe.43bca80.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Zapytanie -20216470859302.exe.3169490.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0.2.Zapytanie -20216470859302.exe.42643b0.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Uses secure TLS version for HTTPS connections

Contains modern PE file flags such as dynamic base (ASLR) or NX

Networking:

May check the online IP address of the machine

System Summary:

.NET source code contains very large array initializations

.NET source code contains very large strings

Malware Analysis System Evasion:

Yara detected AntiVM_3

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

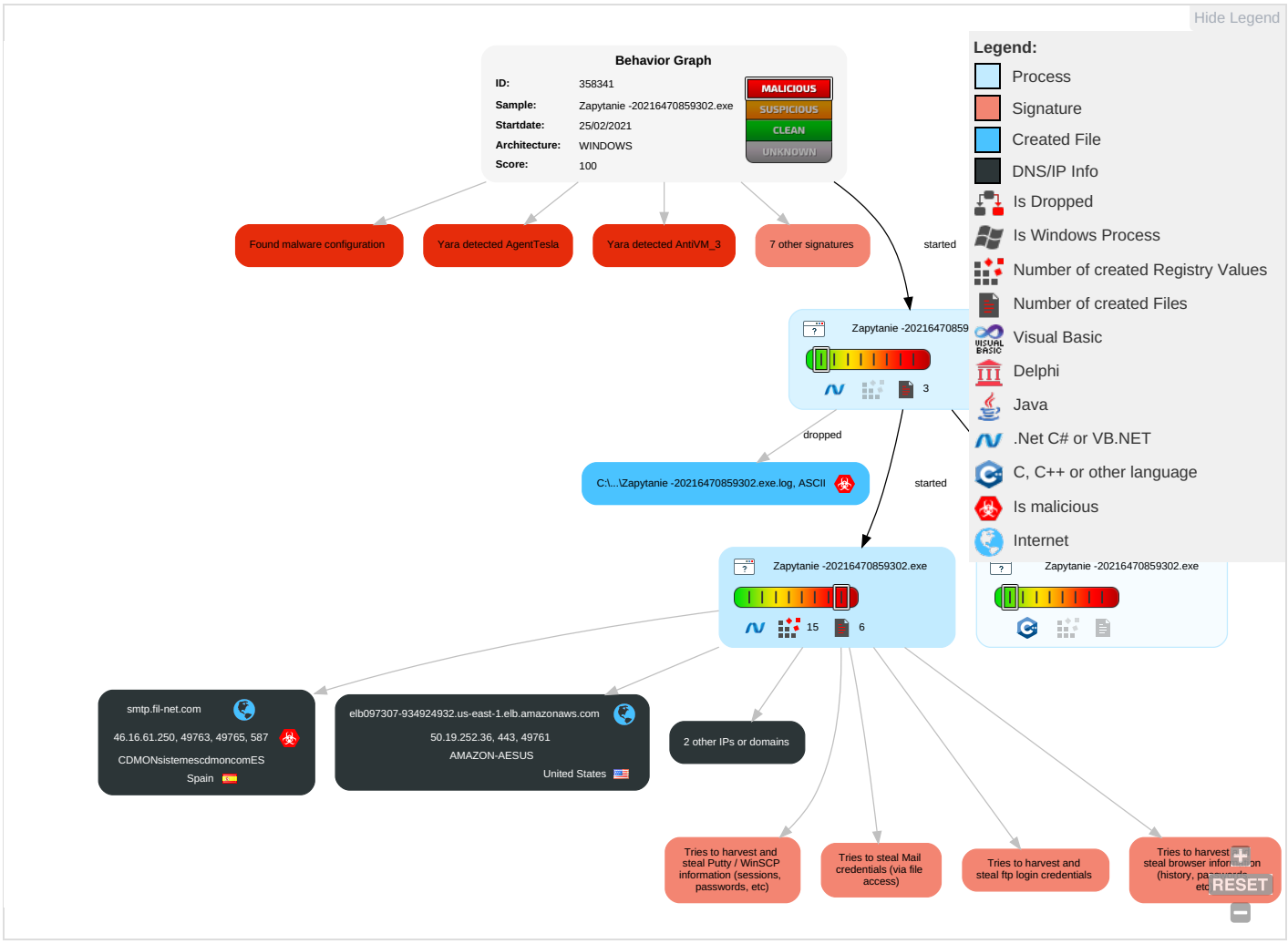
Remote Access Functionality:

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
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1 3	Input Capture 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Credentials in Registry 1	Virtualization/Sandbox Evasion 1 3	SMB/Windows Admin Shares	Archive Collected Data 1 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Application Layer Protocol 1 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2	DCSync	System Network Configuration Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 1 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

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
Zapytanie -20216470859302.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.Zapytanie -20216470859302.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://hqFkeHOniWF1AKH.org	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://umWsex.com	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://smtp.fil-net.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0%	0%	Avira URL Cloud	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

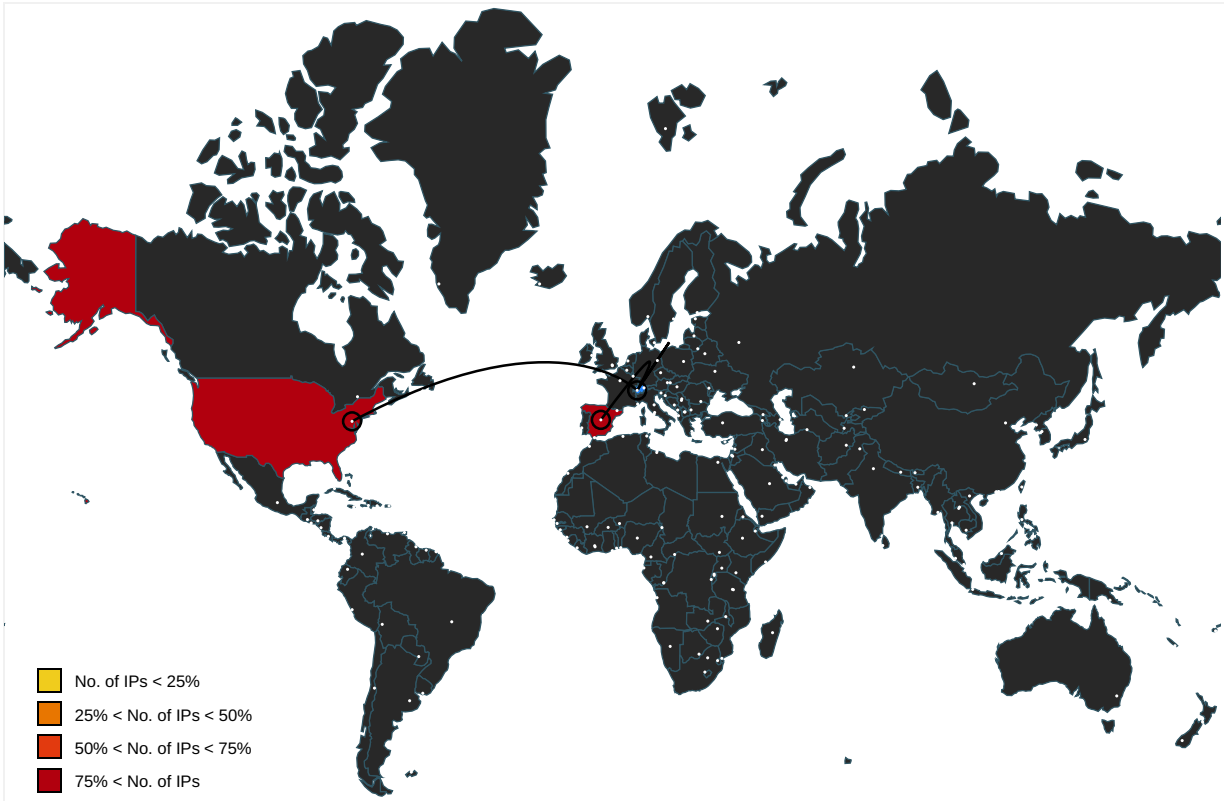
Name	IP	Active	Malicious	Antivirus Detection	Reputation
elb097307-934924932.us-east-1.elb.amazonaws.com	50.19.252.36	true	false		high
smtp.fil-net.com	46.16.61.250	true	true		unknown
api.ipify.org	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://hqFkeHOniWF1AKH.org	Zapytanie -20216470859302.exe, 00000003.00000002.897520193.000000002D95000.00000004.00000001.sdmp, Zapytanie -20216470859302.exe, 00000003.00000002.897579753.0000000002DFB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org/	Zapytanie -20216470859302.exe, 00000003.00000002.897276888.000000002B41000.00000004.00000001.sdmp	false		high
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	Zapytanie -20216470859302.exe, 00000003.00000002.897300872.000000002B7B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	Zapytanie -20216470859302.exe, 00000003.00000002.897276888.0 000000002B41000.00000004.00000 001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.ipify.org	Zapytanie -20216470859302.exe, 00000003.00000002.897276888.0 000000002B41000.00000004.00000 001.sdmp	false		high
http://DynDns.comDynDNS	Zapytanie -20216470859302.exe, 00000003.00000002.897276888.0 000000002B41000.00000004.00000 001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	Zapytanie -20216470859302.exe, 00000003.00000002.897300872.0 000000002B7B000.00000004.00000 001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://umWsex.com	Zapytanie -20216470859302.exe, 00000003.00000002.897276888.0 000000002B41000.00000004.00000 001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.sectigo.com0	Zapytanie -20216470859302.exe, 00000003.00000002.897300872.0 000000002B7B000.00000004.00000 001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.letsencrypt.org0	Zapytanie -20216470859302.exe, 00000003.00000003.842182229.0 0000000068F2000.00000004.00000 001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/ 9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	Zapytanie -20216470859302.exe, 00000003.00000002.897276888.0 000000002B41000.00000004.00000 001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/	Zapytanie -20216470859302.exe, 00000000.00000002.639307733.0 000000004109000.00000004.00000 001.sdmp, Zapytanie -202164708 59302.exe, 00000003.00000002.8 96326467.0000000000402000.0000 0040.00000001.sdmp	false		high
http://r3.o.lencr.org0	Zapytanie -20216470859302.exe, 00000003.00000003.842182229.0 0000000068F2000.00000004.00000 001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://smtp.fil-net.com	Zapytanie -20216470859302.exe, 00000003.00000002.897562623.0 000000002DE9000.00000004.00000 001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Zapytanie -20216470859302.exe, 00000000.00000002.638964828.0 000000003101000.00000004.00000 001.sdmp, Zapytanie -202164708 59302.exe, 00000003.00000002.8 97276888.0000000002B41000.0000 0004.00000001.sdmp	false		high
http:// https://api.telegram.org/bot%telegramapi%/sendDocumentdoc ument----------x	Zapytanie -20216470859302.exe, 00000003.00000002.897276888.0 000000002B41000.00000004.00000 001.sdmp	false		high
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/ 9.5.3/tor-win32-0.4.3.6.zip	Zapytanie -20216470859302.exe, 00000000.00000002.639307733.0 000000004109000.00000004.00000 001.sdmp, Zapytanie -202164708 59302.exe, 00000003.00000002.8 96326467.0000000000402000.0000 0040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstr ap.min.css	Zapytanie -20216470859302.exe, 00000000.00000002.638964828.0 000000003101000.00000004.00000 001.sdmp	false		high
http://cps.root-x1.letsencrypt.org0	Zapytanie -20216470859302.exe, 00000003.00000003.842182229.0 0000000068F2000.00000004.00000 001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://r3.i.lencr.org/0%	Zapytanie -20216470859302.exe, 00000003.00000003.842182229.0 0000000068F2000.00000004.00000 001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	Zapytanie -20216470859302.exe, 00000003.00000002.897276888.0 000000002B41000.00000004.00000 001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
46.16.61.250	unknown	Spain		197712	CDMONsistemescdmoncom ES	true
50.19.252.36	unknown	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358341
Start date:	25.02.2021
Start time:	12:43:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Zapytanie -20216470859302.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:	15
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@5/2@3/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0% (good quality ratio 0%) • Quality average: 81% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 104.43.139.144, 13.88.21.125, 13.64.90.137, 104.43.193.48, 51.104.139.180, 52.155.217.156, 20.54.26.129, 2.20.142.209, 2.20.142.210, 51.132.208.181, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/358341/sample/Zapytanie -20216470859302.exe

Simulations

Behavior and APIs

Time	Type	Description
12:44:00	API Interceptor	778x Sleep call for process: Zapytanie -20216470859302.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
46.16.61.250	winlog.exe	Get hash	malicious	Browse	
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	
	Nakit Akisi Detaylariniz.exe	Get hash	malicious	Browse	
	S67xSX1MNR.exe	Get hash	malicious	Browse	
50.19.252.36	GTS_21_9018_ORDER_pdf.exe	Get hash	malicious	Browse	• api.ipify.org/
	Hs52qascx.dll	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	0211_38602014674781.doc	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	W0rd.dll	Get hash	malicious	Browse	• api.ipify.org/
	Wh102yYa.dll	Get hash	malicious	Browse	• api.ipify.org/
	gHodcQLJM6.exe	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	Wh102yYa.dll	Get hash	malicious	Browse	• api.ipify.org/
	0112_91448090.doc	Get hash	malicious	Browse	• api.ipify.org/
	0112_1079750132.doc	Get hash	malicious	Browse	• api.ipify.org/
	Our New Order Jan 12 2021 at 2.30_PVV440_PDF.exe	Get hash	malicious	Browse	• api.ipify.org/
	q8yEckmvk1.exe	Get hash	malicious	Browse	• api.ipify.org/
	SecuriteInfo.com.Trojan.PWS.Stealer.29660.11031.exe	Get hash	malicious	Browse	• api.ipify.org/
	vAbH6UC7Hy.exe	Get hash	malicious	Browse	• api.ipify.org/
	sample.exe	Get hash	malicious	Browse	• api.ipify.org/
	BBVA confirming Aviso de pago Eur5780201120.exe	Get hash	malicious	Browse	• api.ipify.org/
	G7APZjNv6i.exe	Get hash	malicious	Browse	• api.ipify.org/
	InquirySW23020KT.com.exe	Get hash	malicious	Browse	• api.ipify.org/
	RFQ.exe	Get hash	malicious	Browse	• api.ipify.org/
	E099874321.exe	Get hash	malicious	Browse	• api.ipify.org/
	BL21157346500MB6ZE1MA.xls.exe	Get hash	malicious	Browse	• api.ipify.org/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
elb097307-934924932.us-east-1.elb.amazonaws.com	0224_13930141056302.doc	Get hash	malicious	Browse	• 54.243.164.148
	RFQ- 978002410.exe	Get hash	malicious	Browse	• 23.21.140.41
	HblVSJaQa1.exe	Get hash	malicious	Browse	• 54.225.214.197
	FspMzSMtYA.exe	Get hash	malicious	Browse	• 23.21.76.253
	0224_11959736734789.doc	Get hash	malicious	Browse	• 54.225.66.103
	New Po #0126733 2021.exe	Get hash	malicious	Browse	• 54.225.129.141
	530000.exe	Get hash	malicious	Browse	• 23.21.252.4
	MT SC GUANGZHOU.exe	Get hash	malicious	Browse	• 54.221.253.252
	MT WOOJIN CHEMS V.2103.exe	Get hash	malicious	Browse	• 54.225.66.103
	GTS_21_9018_ORDER_pdf.exe	Get hash	malicious	Browse	• 50.19.252.36
	Attach_847148466_1889687887.xls	Get hash	malicious	Browse	• 54.221.253.252
	BANK SWIFT- USD 98,712.00.pdf.exe	Get hash	malicious	Browse	• 23.21.126.66
	FAU0000000000.exe	Get hash	malicious	Browse	• 54.235.189.250
	RkoKlvuLh6.exe	Get hash	malicious	Browse	• 50.19.96.218
	i0fOtOV8v0.exe	Get hash	malicious	Browse	• 54.221.253.252
	zLyXzE7WZi.exe	Get hash	malicious	Browse	• 50.19.96.218
	wLy18x5e2o.exe	Get hash	malicious	Browse	• 54.243.164.148
	m32I79J0kJ.exe	Get hash	malicious	Browse	• 54.235.83.248
	QJ2UZbJWDS.exe	Get hash	malicious	Browse	• 23.21.76.253
	jWtClvtYBb.exe	Get hash	malicious	Browse	• 54.235.83.248
smtp.fil-net.com	Nakit Akisi Detaylariniz.exe	Get hash	malicious	Browse	• 46.16.61.250

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	C1 PureQuest PO S1026710.xlsm	Get hash	malicious	Browse	• 100.24.200.179
	C1 PureQuest PO S1026710.xlsm	Get hash	malicious	Browse	• 34.226.34.190
	ibne8SNXWv.exe	Get hash	malicious	Browse	• 3.83.18.241
	ibne8SNXWv.exe	Get hash	malicious	Browse	• 3.83.18.241
	0224_13930141056302.doc	Get hash	malicious	Browse	• 50.19.96.218
	RFQ- 978002410.exe	Get hash	malicious	Browse	• 23.21.140.41
	HblVSJaQa1.exe	Get hash	malicious	Browse	• 54.225.214.197

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	007.docx	Get hash	malicious	Browse	• 18.209.89.50
	007.docx	Get hash	malicious	Browse	• 3.222.126.94
	Malone3388_001.htm	Get hash	malicious	Browse	• 100.24.186.63
	FspMzSMtYA.exe	Get hash	malicious	Browse	• 23.21.76.253
	0224_11959736734789.doc	Get hash	malicious	Browse	• 54.225.66.103
	New Po #0126733 2021.exe	Get hash	malicious	Browse	• 54.225.129.141
	RQP_10378065.exe	Get hash	malicious	Browse	• 3.223.115.185
	Price quotation.exe	Get hash	malicious	Browse	• 100.25.237.136
	a.exe	Get hash	malicious	Browse	• 34.237.10.189
	530000.exe	Get hash	malicious	Browse	• 23.21.252.4
	dwg.exe	Get hash	malicious	Browse	• 3.223.115.185
	MT SC GUANGZHOU.exe	Get hash	malicious	Browse	• 54.221.253.252
	Order List - 022321-xlxs.exe	Get hash	malicious	Browse	• 52.0.217.44
CDMONsistemescdmoncomES	njGJ1eW44wshoMr.exe	Get hash	malicious	Browse	• 46.16.62.134
	3nG9LW7Z21dxUoM.exe	Get hash	malicious	Browse	• 46.16.62.134
	keeFDE9dhCGNNez.exe	Get hash	malicious	Browse	• 46.16.62.134
	74tF1foMeQyUMCh.exe	Get hash	malicious	Browse	• 46.16.62.134
	qm7JU84PFgfqvgs.exe	Get hash	malicious	Browse	• 46.16.62.134
	winlog.exe	Get hash	malicious	Browse	• 46.16.61.250
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 46.16.61.250
	WbGKi8E5OE4eCFG.exe	Get hash	malicious	Browse	• 46.16.62.134
	r9SWnqQlK8PFPEp.exe	Get hash	malicious	Browse	• 46.16.62.134
	L9oOm9x3I7YZFcA.exe	Get hash	malicious	Browse	• 46.16.62.134
	SecuriteInfo.com.Trojan.DownLoader36.34557.26355.exe	Get hash	malicious	Browse	• 134.0.10.35
	jKiL1mzTAVltJ30.exe	Get hash	malicious	Browse	• 46.16.62.134
	09xcuRN2HJmRRCm.exe	Get hash	malicious	Browse	• 46.16.62.134
	57229937-122020-4-7676523.doc	Get hash	malicious	Browse	• 185.66.41.128
	aLjBjGUvWecwGptNRQryBtRBaVCtO.exe	Get hash	malicious	Browse	• 46.16.62.134
	UsU2f18QuIdAe2U.exe	Get hash	malicious	Browse	• 46.16.62.134
	Nakit Akisi Detaylariniz.exe	Get hash	malicious	Browse	• 46.16.61.250
	Archivo_122020_1977149.doc	Get hash	malicious	Browse	• 185.66.41.128
	Doc.doc	Get hash	malicious	Browse	• 185.66.41.127
	JI35907_2020.doc	Get hash	malicious	Browse	• 185.66.41.127

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	kBJlVQuchM.exe	Get hash	malicious	Browse	• 50.19.252.36
	Purchase order.exe	Get hash	malicious	Browse	• 50.19.252.36
	HblVSJaQa1.exe	Get hash	malicious	Browse	• 50.19.252.36
	FspMzSMtYA.exe	Get hash	malicious	Browse	• 50.19.252.36
	New Po #0126733 2021.exe	Get hash	malicious	Browse	• 50.19.252.36
	530000.exe	Get hash	malicious	Browse	• 50.19.252.36
	Bitcoin Mining 2021 Feb.exe	Get hash	malicious	Browse	• 50.19.252.36
	MT SC GUANGZHOU.exe	Get hash	malicious	Browse	• 50.19.252.36
	MT WOOJIN CHEMS V.2103.exe	Get hash	malicious	Browse	• 50.19.252.36
	EOrg2020.exe	Get hash	malicious	Browse	• 50.19.252.36
	Bitcoin Mining 2021 Feb.exe	Get hash	malicious	Browse	• 50.19.252.36
	AZjP1E0nRZ.exe	Get hash	malicious	Browse	• 50.19.252.36
	x0yccMVTIb.exe	Get hash	malicious	Browse	• 50.19.252.36
	WHz0D1UERA.exe	Get hash	malicious	Browse	• 50.19.252.36
	SecuriteInfo.com.Trojan.GenericKD.45754886.17334.exe	Get hash	malicious	Browse	• 50.19.252.36
	1i0Bvmiuqg.exe	Get hash	malicious	Browse	• 50.19.252.36
	SecuriteInfo.com.Variant.Zusy.368685.25375.exe	Get hash	malicious	Browse	• 50.19.252.36
	OC 136584.PDF.exe	Get hash	malicious	Browse	• 50.19.252.36
	Quote_13940007.exe	Get hash	malicious	Browse	• 50.19.252.36
	SecuriteInfo.com.Variant.Zusy.368685.25618.exe	Get hash	malicious	Browse	• 50.19.252.36

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Zapytanie -20216470859302.exe.log	
Process:	C:\Users\user\Desktop\Zapytanie -20216470859302.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a

C:\Users\user\AppData\Roaming\wvbj0rxz.1ql\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\Zapytanie -20216470859302.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Reputation:	moderate, 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):	7.032444091192518
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Zapytanie -20216470859302.exe
File size:	780288
MD5:	d78bcccfe9e8e96d75e488dab97ba56f
SHA1:	d4b2f340c8df782c4ebac3a3dabaab9db19aa28e
SHA256:	3832cbc966b60610c0452b4bfca9648126d7ab20fcd29a413a1b5f88abf7e685

General

SHA512:	cb1ef6c6357cb869343e607fb41a6a6584950fcec81063269a30a5edf3e5bdaddd016883437205db884881decccfe111db81b3eb6a204e56b127e59dcd541594
SSDEEP:	12288:WADfGTIgkG8bfvECBtVUXDU+I/o7TH1uWoOxEJDrDeKo:WUfG+G8b0CBk6GTVuLmF
File Content Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L...9o7`..............P......T........... ....@.. ....@............@................................

File Icon

	
Icon Hash:	e0dad4adc4d2d870

Static PE Info

General

Entrypoint:	0x4bb0b6
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60376F39 [Thu Feb 25 09:34:49 2021 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

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbb064	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbc000	0x51c8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc2000	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	0xb90bc	0xb9200	False	0.603581564399	data	7.04403156947	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xbc000	0x51c8	0x5200	False	0.189500762195	data	4.2360167597	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc2000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xbc100	0x4228	dBase III DBT, version number 0, next free block index 40		
RT_GROUP_ICON	0xc0338	0x14	data		
RT_VERSION	0xc035c	0x340	data		
RT_MANIFEST	0xc06ac	0xb15	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

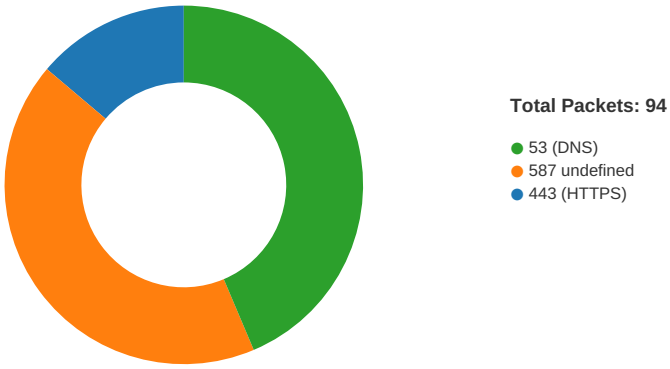
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2014
Assembly Version	3.0.0.0
InternalName	SurrogateKey.exe
FileVersion	3.0.0.0
CompanyName	KTV
LegalTrademarks	
Comments	

Description	Data
ProductName	KTVManagement
ProductVersion	3.0.0.0
FileDescription	KTVManagement
OriginalFilename	SurrogateKey.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 12:45:30.911732912 CET	49761	443	192.168.2.4	50.19.252.36
Feb 25, 2021 12:45:31.039321899 CET	443	49761	50.19.252.36	192.168.2.4
Feb 25, 2021 12:45:31.039460897 CET	49761	443	192.168.2.4	50.19.252.36
Feb 25, 2021 12:45:31.078174114 CET	49761	443	192.168.2.4	50.19.252.36
Feb 25, 2021 12:45:31.205683947 CET	443	49761	50.19.252.36	192.168.2.4
Feb 25, 2021 12:45:31.205743074 CET	443	49761	50.19.252.36	192.168.2.4
Feb 25, 2021 12:45:31.205784082 CET	443	49761	50.19.252.36	192.168.2.4
Feb 25, 2021 12:45:31.205821037 CET	443	49761	50.19.252.36	192.168.2.4
Feb 25, 2021 12:45:31.205848932 CET	443	49761	50.19.252.36	192.168.2.4
Feb 25, 2021 12:45:31.205877066 CET	49761	443	192.168.2.4	50.19.252.36
Feb 25, 2021 12:45:31.205931902 CET	49761	443	192.168.2.4	50.19.252.36
Feb 25, 2021 12:45:31.206959009 CET	443	49761	50.19.252.36	192.168.2.4
Feb 25, 2021 12:45:31.206995010 CET	443	49761	50.19.252.36	192.168.2.4
Feb 25, 2021 12:45:31.207122087 CET	49761	443	192.168.2.4	50.19.252.36
Feb 25, 2021 12:45:31.239533901 CET	49761	443	192.168.2.4	50.19.252.36
Feb 25, 2021 12:45:31.367185116 CET	443	49761	50.19.252.36	192.168.2.4
Feb 25, 2021 12:45:31.415811062 CET	49761	443	192.168.2.4	50.19.252.36
Feb 25, 2021 12:45:31.460108995 CET	49761	443	192.168.2.4	50.19.252.36
Feb 25, 2021 12:45:31.592284918 CET	443	49761	50.19.252.36	192.168.2.4
Feb 25, 2021 12:45:31.634537935 CET	49761	443	192.168.2.4	50.19.252.36
Feb 25, 2021 12:45:35.924237967 CET	49761	443	192.168.2.4	50.19.252.36
Feb 25, 2021 12:45:36.029473066 CET	49763	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:36.051767111 CET	443	49761	50.19.252.36	192.168.2.4
Feb 25, 2021 12:45:36.051805019 CET	443	49761	50.19.252.36	192.168.2.4
Feb 25, 2021 12:45:36.051860094 CET	49761	443	192.168.2.4	50.19.252.36
Feb 25, 2021 12:45:36.051899910 CET	49761	443	192.168.2.4	50.19.252.36
Feb 25, 2021 12:45:36.094329119 CET	587	49763	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:36.094657898 CET	49763	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:36.525538921 CET	587	49763	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:36.530191898 CET	49763	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:36.590604067 CET	587	49763	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:36.591625929 CET	587	49763	46.16.61.250	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 12:45:36.591926098 CET	49763	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:36.653891087 CET	587	49763	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:36.657457113 CET	49763	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:36.722440958 CET	587	49763	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:36.722495079 CET	587	49763	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:36.722518921 CET	587	49763	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:36.722831964 CET	49763	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:36.742218971 CET	49763	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:36.806237936 CET	587	49763	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:36.849023104 CET	49763	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:36.911973953 CET	587	49763	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:36.914171934 CET	49763	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:36.976262093 CET	587	49763	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:36.978008986 CET	49763	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:37.055196047 CET	587	49763	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:37.056329966 CET	49763	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:37.118963957 CET	587	49763	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:37.119790077 CET	49763	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:37.184329987 CET	587	49763	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:37.186240911 CET	49763	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:37.253479958 CET	587	49763	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:37.256767988 CET	49763	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:37.257244110 CET	49763	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:37.257515907 CET	49763	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:37.257700920 CET	49763	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:37.334980965 CET	587	49763	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:37.335048914 CET	587	49763	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:37.422660112 CET	587	49763	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:37.463129997 CET	49763	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:38.440493107 CET	49763	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:38.502240896 CET	587	49763	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:38.502288103 CET	587	49763	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:38.502573013 CET	49763	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:38.503304005 CET	49763	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:38.504842043 CET	49765	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:38.566869974 CET	587	49765	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:38.567148924 CET	49765	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:38.632824898 CET	587	49765	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:38.633137941 CET	49765	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:38.698971033 CET	587	49765	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:38.702189922 CET	587	49765	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:38.702475071 CET	49765	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:38.769692898 CET	587	49765	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:38.770703077 CET	49765	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:38.836992025 CET	587	49765	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:38.837049961 CET	587	49765	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:38.837079048 CET	587	49765	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:38.837338924 CET	49765	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:38.848507881 CET	49765	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:38.910203934 CET	587	49765	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:38.914159060 CET	49765	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:38.990571976 CET	587	49765	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:38.991606951 CET	49765	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:39.055336952 CET	587	49765	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:39.056561947 CET	49765	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:39.132123947 CET	587	49765	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:39.137243986 CET	49765	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:39.202454090 CET	587	49765	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:39.207067966 CET	49765	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:39.270765066 CET	587	49765	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:39.271512032 CET	49765	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:39.335524082 CET	587	49765	46.16.61.250	192.168.2.4
Feb 25, 2021 12:45:39.338957071 CET	49765	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:39.339220047 CET	49765	587	192.168.2.4	46.16.61.250

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 12:45:39.339451075 CET	49765	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:39.339683056 CET	49765	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:39.340048075 CET	49765	587	192.168.2.4	46.16.61.250
Feb 25, 2021 12:45:39.340250015 CET	49765	587	192.168.2.4	46.16.61.250

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 12:43:53.375576019 CET	59123	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:43:53.427099943 CET	53	59123	8.8.8.8	192.168.2.4
Feb 25, 2021 12:43:54.594901085 CET	54531	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:43:54.646500111 CET	53	54531	8.8.8.8	192.168.2.4
Feb 25, 2021 12:43:58.645160913 CET	49714	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:43:58.695830107 CET	53	49714	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:02.122008085 CET	58028	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:02.170808077 CET	53	58028	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:03.323924065 CET	53097	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:03.381195068 CET	53	53097	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:04.302207947 CET	49257	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:04.351104021 CET	53	49257	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:06.038285971 CET	62389	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:06.090027094 CET	53	62389	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:07.000521898 CET	49910	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:07.052772045 CET	53	49910	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:07.950455904 CET	55854	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:08.002602100 CET	53	55854	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:08.905061007 CET	64549	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:08.953980923 CET	53	64549	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:09.861824036 CET	63153	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:09.915024042 CET	53	63153	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:12.387896061 CET	52991	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:12.447180033 CET	53	52991	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:13.363146067 CET	53700	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:13.415047884 CET	53	53700	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:14.324582100 CET	51726	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:14.373701096 CET	53	51726	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:15.494338036 CET	56794	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:15.542990923 CET	53	56794	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:17.933177948 CET	56534	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:17.983107090 CET	53	56534	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:23.220330000 CET	56627	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:23.269114971 CET	53	56627	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:31.034847975 CET	56621	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:31.083744049 CET	53	56621	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:32.009004116 CET	63116	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:32.060801029 CET	53	63116	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:33.079348087 CET	64078	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:33.128216028 CET	53	64078	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:36.036007881 CET	64801	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:36.097470045 CET	53	64801	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:39.499418020 CET	61721	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:39.746045113 CET	53	61721	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:40.264969110 CET	51255	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:40.336627007 CET	53	51255	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:40.943952084 CET	61522	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:41.003189087 CET	53	61522	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:41.017829895 CET	52337	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:41.075126886 CET	53	52337	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:41.448407888 CET	55046	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:41.506658077 CET	53	55046	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:41.976834059 CET	49612	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:42.062493086 CET	53	49612	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:42.605796099 CET	49285	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:42.665215015 CET	53	49285	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 12:44:43.264451027 CET	50601	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:43.324649096 CET	53	50601	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:44.229727030 CET	60875	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:44.305597067 CET	53	60875	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:45.134283066 CET	56448	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:45.191432953 CET	53	56448	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:45.602361917 CET	59172	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:45.660171032 CET	53	59172	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:48.586281061 CET	62420	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:48.648164988 CET	53	62420	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:58.462357998 CET	60579	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:58.511461973 CET	53	60579	8.8.8.8	192.168.2.4
Feb 25, 2021 12:44:58.590760946 CET	50183	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:44:58.658257961 CET	53	50183	8.8.8.8	192.168.2.4
Feb 25, 2021 12:45:00.644224882 CET	61531	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:45:00.707403898 CET	53	61531	8.8.8.8	192.168.2.4
Feb 25, 2021 12:45:30.752023935 CET	49228	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:45:30.800823927 CET	53	49228	8.8.8.8	192.168.2.4
Feb 25, 2021 12:45:30.848331928 CET	59794	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:45:30.897142887 CET	53	59794	8.8.8.8	192.168.2.4
Feb 25, 2021 12:45:33.766820908 CET	55916	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:45:33.815617085 CET	53	55916	8.8.8.8	192.168.2.4
Feb 25, 2021 12:45:35.946440935 CET	52752	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:45:36.026029110 CET	53	52752	8.8.8.8	192.168.2.4
Feb 25, 2021 12:45:36.818815947 CET	60542	53	192.168.2.4	8.8.8.8
Feb 25, 2021 12:45:36.894098997 CET	53	60542	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 12:45:30.752023935 CET	192.168.2.4	8.8.8.8	0xa848	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Feb 25, 2021 12:45:30.848331928 CET	192.168.2.4	8.8.8.8	0xf2c	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Feb 25, 2021 12:45:35.946440935 CET	192.168.2.4	8.8.8.8	0xadd3	Standard query (0)	smtp.fil-net.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 12:45:30.800823927 CET	8.8.8.8	192.168.2.4	0xa848	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 12:45:30.800823927 CET	8.8.8.8	192.168.2.4	0xa848	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 12:45:30.800823927 CET	8.8.8.8	192.168.2.4	0xa848	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)
Feb 25, 2021 12:45:30.800823927 CET	8.8.8.8	192.168.2.4	0xa848	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.66.103	A (IP address)	IN (0x0001)
Feb 25, 2021 12:45:30.800823927 CET	8.8.8.8	192.168.2.4	0xa848	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.214.197	A (IP address)	IN (0x0001)
Feb 25, 2021 12:45:30.800823927 CET	8.8.8.8	192.168.2.4	0xa848	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.96.218	A (IP address)	IN (0x0001)
Feb 25, 2021 12:45:30.800823927 CET	8.8.8.8	192.168.2.4	0xa848	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.164.148	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 12:45:30.800823927 CET	8.8.8.8	192.168.2.4	0xa848	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.48.44	A (IP address)	IN (0x0001)
Feb 25, 2021 12:45:30.800823927 CET	8.8.8.8	192.168.2.4	0xa848	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.129.141	A (IP address)	IN (0x0001)
Feb 25, 2021 12:45:30.800823927 CET	8.8.8.8	192.168.2.4	0xa848	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.140.41	A (IP address)	IN (0x0001)
Feb 25, 2021 12:45:30.897142887 CET	8.8.8.8	192.168.2.4	0xf2c	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 12:45:30.897142887 CET	8.8.8.8	192.168.2.4	0xf2c	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 12:45:30.897142887 CET	8.8.8.8	192.168.2.4	0xf2c	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.214.197	A (IP address)	IN (0x0001)
Feb 25, 2021 12:45:30.897142887 CET	8.8.8.8	192.168.2.4	0xf2c	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.83.248	A (IP address)	IN (0x0001)
Feb 25, 2021 12:45:30.897142887 CET	8.8.8.8	192.168.2.4	0xf2c	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.252.4	A (IP address)	IN (0x0001)
Feb 25, 2021 12:45:30.897142887 CET	8.8.8.8	192.168.2.4	0xf2c	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.189.250	A (IP address)	IN (0x0001)
Feb 25, 2021 12:45:30.897142887 CET	8.8.8.8	192.168.2.4	0xf2c	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.140.41	A (IP address)	IN (0x0001)
Feb 25, 2021 12:45:30.897142887 CET	8.8.8.8	192.168.2.4	0xf2c	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.221.253.252	A (IP address)	IN (0x0001)
Feb 25, 2021 12:45:30.897142887 CET	8.8.8.8	192.168.2.4	0xf2c	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)
Feb 25, 2021 12:45:30.897142887 CET	8.8.8.8	192.168.2.4	0xf2c	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.164.148	A (IP address)	IN (0x0001)
Feb 25, 2021 12:45:36.026029110 CET	8.8.8.8	192.168.2.4	0xadd3	No error (0)	smtp.fil-net.com		46.16.61.250	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 12:45:31.206995010 CET	50.19.252.36	443	192.168.2.4	49761	CN=*.ipify.org CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Jan 19 01:00:00 CET 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Sun Feb 20 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

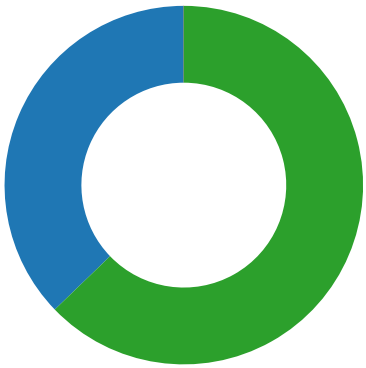
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 25, 2021 12:45:36.525538921 CET	587	49763	46.16.61.250	192.168.2.4	220 vxsys-smtpclusterma-01.srv.cat ESMTP
Feb 25, 2021 12:45:36.530191898 CET	49763	587	192.168.2.4	46.16.61.250	EHLO 114127
Feb 25, 2021 12:45:36.591625929 CET	587	49763	46.16.61.250	192.168.2.4	250-vxsys-smtpclusterma-01.srv.cat 250-PIPELINING 250-SIZE 47185920 250-ETRN 250-STARTTLS 250-AUTH LOGIN PLAIN CRAM-MD5 DIGEST-MD5 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
Feb 25, 2021 12:45:36.591926098 CET	49763	587	192.168.2.4	46.16.61.250	STARTTLS
Feb 25, 2021 12:45:36.653891087 CET	587	49763	46.16.61.250	192.168.2.4	220 2.0.0 Ready to start TLS
Feb 25, 2021 12:45:38.632824898 CET	587	49765	46.16.61.250	192.168.2.4	220 vxsys-smtpclusterma-05.srv.cat ESMTP
Feb 25, 2021 12:45:38.633137941 CET	49765	587	192.168.2.4	46.16.61.250	EHLO 114127
Feb 25, 2021 12:45:38.702189922 CET	587	49765	46.16.61.250	192.168.2.4	250-vxsys-smtpclusterma-05.srv.cat 250-PIPELINING 250-SIZE 47185920 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN CRAM-MD5 DIGEST-MD5 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
Feb 25, 2021 12:45:38.702475071 CET	49765	587	192.168.2.4	46.16.61.250	STARTTLS
Feb 25, 2021 12:45:38.769692898 CET	587	49765	46.16.61.250	192.168.2.4	220 2.0.0 Ready to start TLS

Code Manipulations

Statistics

Behavior



Zapytanie -20216470859302.exe
Zapytanie -20216470859302.exe
Zapytanie -20216470859302.exe

Click to jump to process

System Behavior

Analysis Process: Zapytanie -20216470859302.exe PID: 7112 Parent PID: 4804

General

Start time:	12:43:59
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\Zapytanie -20216470859302.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Zapytanie -20216470859302.exe'
Imagebase:	0xce0000
File size:	780288 bytes
MD5 hash:	D78BCCCFE9E8E96D75E488DAB97BA56F
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: 00000000.00000002.638964828.0000000003101000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.639307733.0000000004109000.00000004.00000001.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	6D38CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D38CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Zapytanie - 20216470859302.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69C78D	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\Zapytanie - 20216470859302.exe.log	unknown	1314	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 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D69C907	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	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile

Analysis Process: Zapytanie -20216470859302.exe PID: 2440 Parent PID: 7112

General

Start time:	12:44:01
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\Zapytanie -20216470859302.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Zapytanie -20216470859302.exe
Imagebase:	0x210000
File size:	780288 bytes
MD5 hash:	D78BCCCFE9E8E96D75E488DAB97BA56F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Zapytanie -20216470859302.exe PID: 6340 Parent PID: 7112

General

Start time:	12:44:01
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\Zapytanie -20216470859302.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Zapytanie -20216470859302.exe
Imagebase:	0x710000
File size:	780288 bytes
MD5 hash:	D78BCCCFE9E8E96D75E488DAB97BA56F
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: 00000003.00000002.896326467.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.897336626.0000000002B96000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.897276888.0000000002B41000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.897276888.0000000002B41000.00000004.00000001.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	6D38CF06	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	6D38CF06	unknown
C:\Users\user\AppData\Roaming\wvbj0rxz.1ql	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C1DBEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\wvbj0rxz.1ql\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	6C1DBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\wvbj0rxz.1ql\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	6C1DBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\wvbj0rxz.1ql\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	6C1DDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\wvbj0rxz.1ql\Chrome\Default\Cookies	success or wait	1	6C1D6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\wvbj0rxz.1ql\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 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 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 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6C1DDD66	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	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\e310657b-14e1-4d73-8ac9-109aafbc6423	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Users\user\AppData\Roaming\wvbj0rxz.1ql\Chrome\Default\Cookies	unknown	16384	success or wait	1	6C1D1B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis