

JoeSandbox Cloud BASIC



ID: 694556

Sample Name: arinzezx.exe

Cookbook: default.jbs

Time: 23:46:48

Date: 31/08/2022

Version: 35.0.0 Citrine

Table of Contents

Table of Contents	2
Windows Analysis Report arinzezx.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Agenttesla	4
Yara Signatures	4
Memory Dumps	4
Unpacked PEs	5
Sigma Signatures	5
Snort Signatures	5
Joe Sandbox Signatures	5
AV Detection	5
Key, Mouse, Clipboard, Microphone and Screen Capturing	6
System Summary	6
Malware Analysis System Evasion	6
HIPS / PFW / Operating System Protection Evasion	6
Stealing of Sensitive Information	6
Remote Access Functionality	6
Mitre Att&ck Matrix	6
Behavior Graph	7
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	9
Contacted Domains	9
Contacted URLs	9
URLs from Memory and Binaries	10
World Map of Contacted IPs	13
Public IPs	13
Private	13
General Information	14
Warnings	14
Simulations	14
Behavior and APIs	14
Joe Sandbox View / Context	14
IPs	14
Domains	15
ASNs	15
JA3 Fingerprints	15
Dropped Files	15
Created / dropped Files	15
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\arinzezx.exe.log	15
C:\Users\user\AppData\Local\Microsoft\Windows\NetCache\IE\B87Z87FM\livestream[1].htm	15
Static File Info	16
General	16
File Icon	16
Static PE Info	16
General	16
Entrypoint Preview	16
Data Directories	18
Sections	18
Resources	19
Imports	19
Network Behavior	19
Network Port Distribution	19
TCP Packets	19
UDP Packets	21
DNS Queries	21
DNS Answers	21
HTTP Request Dependency Graph	22
HTTP Packets	22
HTTPS Proxied Packets	24
SMTP Packets	27
Statistics	27

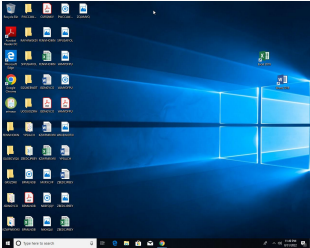
Behavior	27
System Behavior	27
Analysis Process: arinzezx.exePID: 6600, Parent PID: 1424	27
General	27
File Activities	28
File Created	28
File Written	28
File Read	28
Analysis Process: arinzezx.exePID: 6964, Parent PID: 6600	29
General	29
Analysis Process: arinzezx.exePID: 6976, Parent PID: 6600	29
General	29
File Activities	30
File Created	30
File Read	30
Disassembly	30

Windows Analysis Report

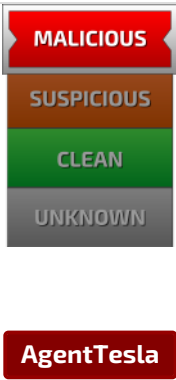
arinzezx.exe

Overview

General Information

Sample Name:	arinzezx.exe
Analysis ID:	694556
MD5:	314c678d85f792..
SHA1:	1a1695ee1411cc..
SHA256:	e5b9cc21b8de77..
Tags:	exe
Infos:	
	

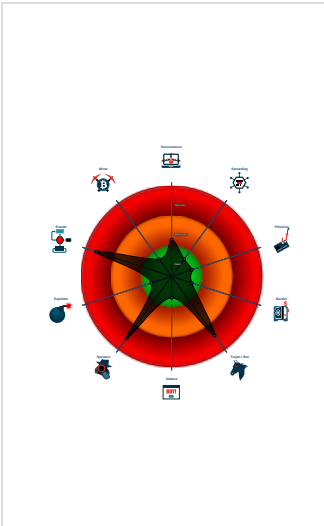
Detection

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

Signatures

Malicious sample detected (through...
Yara detected AgentTesla
Yara detected AntiVM3
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...
Injects a PE file into a foreign proce...
Queries sensitive network adapter in...
Tries to harvest and steal browser in...

Classification



Process Tree

System is w10x64
arinzezx.exe (PID: 6600 cmdline: "C:\Users\user\Desktop\arinzezx.exe" MD5: 314C678D85F7927A42F34797627532E1)
arinzezx.exe (PID: 6964 cmdline: C:\Users\user\Desktop\arinzezx.exe MD5: 314C678D85F7927A42F34797627532E1)
arinzezx.exe (PID: 6976 cmdline: C:\Users\user\Desktop\arinzezx.exe MD5: 314C678D85F7927A42F34797627532E1)
cleanup

Malware Configuration

Threatname: Agenttesla
<pre>{ "Exfil Mode": "SMTP", "Username": "arinzelog@steuler-kch.org", "Password": "7213575aceACE@#\$", "Host": "cp5ua.hyperhost.ua" }</pre>

Yara Signatures

Memory Dumps				
Source	Rule	Description	Author	Strings
00000004.00000000.365108165.0000000000402000.00000400.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000000.365108165.0000000000402000.00000400.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000000.365108165.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	0x300ad:\$a13: get_DnsResolver 0x2e8c7:\$a20: get_LastAccessed 0x30a2b:\$a27: set_InternalServerPort 0x30d47:\$a30: set_GuidMasterKey 0x2e9ce:\$a33: get_Clipboard 0x2e9dc:\$a34: get_Keyboard 0x2fce0:\$a35: get_ShiftKeyDown 0x2fcf1:\$a36: get_AltKeyDown 0x2e9e9:\$a37: get_Password 0x2f490:\$a38: get_PasswordHash 0x304ad:\$a39: get_DefaultCredentials
00000001.00000002.376461043.0000000002F25000.0000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000001.00000002.381932594.0000000004787000.0000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 10 entries				

Unpacked PEs				
Source	Rule	Description	Author	Strings
4.0.arinzezx.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.0.arinzezx.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
4.0.arinzezx.exe.400000.0.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	0x32b5f:\$s10: logins 0x325c6:\$s11: credential 0x2ebce:\$g1: get_Clipboard 0x2ebdc:\$g2: get_Keyboard 0x2ebe9:\$g3: get_Password 0x2fed0:\$g4: get_CtrlKeyDown 0x2fee0:\$g5: get_ShiftKeyDown 0x2fef1:\$g6: get_AltKeyDown
4.0.arinzezx.exe.400000.0.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	0x302ad:\$a13: get_DnsResolver 0x2eac7:\$a20: get_LastAccessed 0x30c2b:\$a27: set_InternalServerPort 0x30f47:\$a30: set_GuidMasterKey 0x2ebce:\$a33: get_Clipboard 0x2ebdc:\$a34: get_Keyboard 0x2fee0:\$a35: get_ShiftKeyDown 0x2fef1:\$a36: get_AltKeyDown 0x2ebe9:\$a37: get_Password 0x2f690:\$a38: get_PasswordHash 0x306ad:\$a39: get_DefaultCredentials
1.2.arinzezx.exe.4787e30.8.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 19 entries				

Sigma Signatures	
No Sigma rule has matched	

Snort Signatures	
No Snort rule has matched	

Joe Sandbox Signatures	
------------------------	--

AV Detection

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)

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	211 Windows Management Instrumentation	Path Interception	111 Process Injection	1 Masquerading	2 OS Credential Dumping	211 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	11 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 Disable or Modify Tools	111 Input Capture	1 Process Discovery	Remote Desktop Protocol	111 Input Capture	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)	131 Virtualization/Sandbox Evasion	1 Credentials in Registry	131 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Archive Collected Data	Automated Exfiltration	3 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	111 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	2 Data from Local System	Scheduled Transfer	3 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	1 Remote System Discovery	SSH	1 Clipboard Data	Data Transfer Size Limits	24 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
arinzezx.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.arinzezx.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://en.wd	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.fonts.comcD	0%	Avira URL Cloud	safe	
http://can-sat.netai.net/livestream/r	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/ConsentHttp/external	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://https://DtM6GM1g5LTIJoVP.org	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://YthClZ.com	0%	Avira URL Cloud	safe	
http://can-sat.netai.net/y	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://can-sat.netai.net/livestream/Hx	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://can-sat.netai.net/livestream/	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNSnamejdpaswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://can-sat.netai.net/livestream/CgC	0%	Avira URL Cloud	safe	
http://can-sat.netai.n	0%	Avira URL Cloud	safe	
http://can-sat.netai.net/livestream/5	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://can-sat.netai.net/livestream/ions.AddInAdapter.v10.0	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://can-sat.netai.net/livestream/tldi	0%	Avira URL Cloud	safe	
http://can-sat.netai.net/5	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.htmlu	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.tiro.comY	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://can-sat.netai.net/livestream/46	0%	Avira URL Cloud	safe	
http://can-sat.netai.net/livestream/e	0%	Avira URL Cloud	safe	
http://can-sat.netai.net/livestream/ll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
can-sat.netai.net	153.92.0.100	true	false		unknown
www.000webhost.com	104.19.184.120	true	false		high
cp5ua.hyperhost.ua	91.235.128.141	true	false		high
consent.google.com	216.58.215.238	true	false		high
maps.google.com	142.250.203.110	true	false		high
www.google.com	142.250.203.100	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.000webhost.com/migrate?static=true	false		high
http://https://consent.google.com/ml?continue=https://www.google.com/maps?saddr%3D31.2087496,29.9091634&gl=GB&m=0&pc=m&uxe=eomtm&hl=de&src=1	false		high
http://https://www.google.com/maps?saddr=31.2087496,29.9091634&z=10	false		high
http://maps.google.com/?saddr=31.2087496,29.9091634&z=10	false		high
http://can-sat.netai.net/livestream/	false	Avira URL Cloud: safe	unknown
http://maps.google.com/maps?saddr=31.2087496,29.9091634&z=10	false		high

URLs from Memory and Binaries

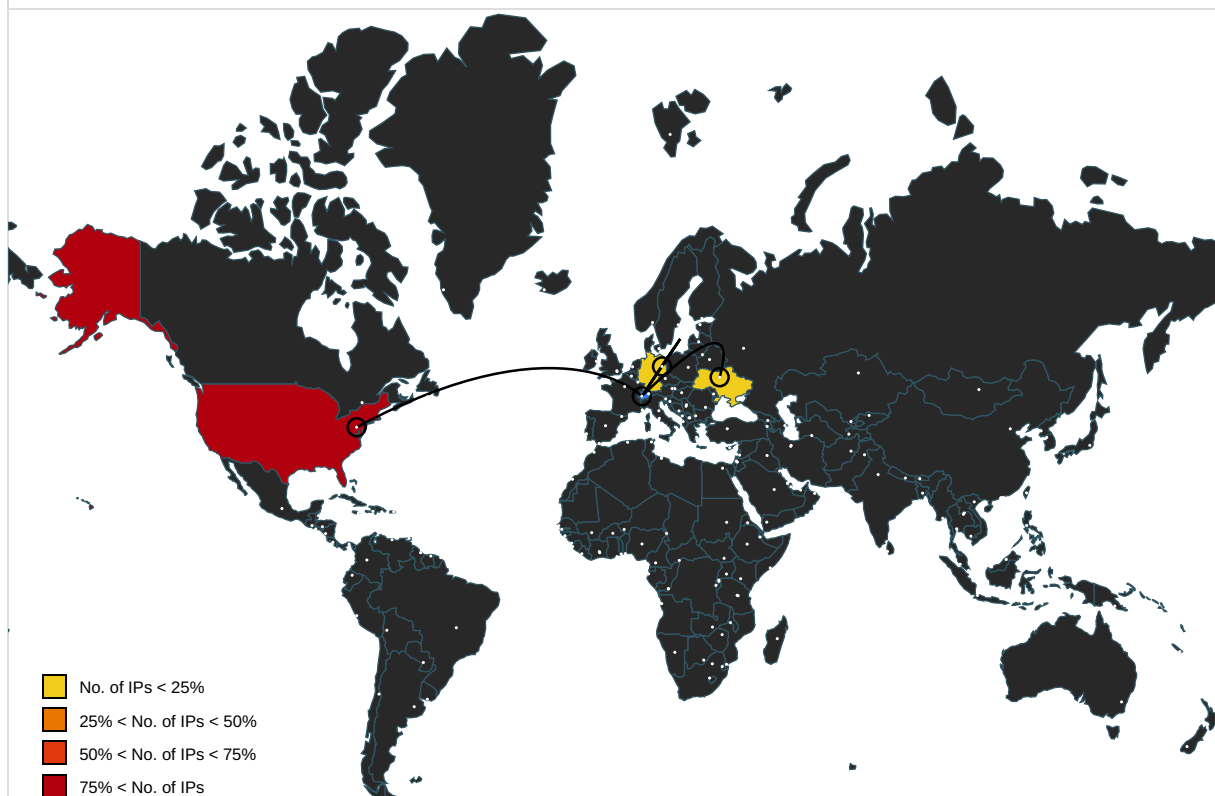
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.000webhost.com/migrate?static=truesl	arinzezx.exe, 00000001.00000002.395742771.000000000AFED000.00000004.00000800.00020000.00000000.sdmp	false		high
http://127.0.0.1:HTTP/1.1	arinzezx.exe, 00000004.00000002.587010252.00000000033F1000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	low
http://en.wD	arinzezx.exe, 00000001.00000003.328011792.0000000008042000.00000004.00000800.00020000.00000000.sdmp, arinzezx.exe, 0000001.00000003.328069691.0000000008044000.00000004.00000800.00020000.00000000.sdmp, arinzezx.exe, 00000001.00000003.327966259.00000008040000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	arinzezx.exe, 00000001.00000002.386131393.0000000009342000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersAny	arinzezx.exe, 00000001.00000003.331202082.0000000008070000.00000004.00000800.00020000.00000000.sdmp, arinzezx.exe, 0000001.00000003.331229601.0000000008070000.00000004.00000800.00020000.00000000.sdmp, arinzezx.exe, 00000001.00000003.331180508.000000008070000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.comcD	arinzezx.exe, 00000001.00000003.324211844.000000000804B000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://can-sat.netai.net/livestream/r	arinzezx.exe, 00000001.00000002.395742771.000000000AFED000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	arinzezx.exe, 00000001.00000002.386131393.0000000009342000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://csp.withgoogle.com/csp/report-to/ConsentHttp/external	arinzezx.exe, 00000001.00000002.392284063.000000000AFCA000.00000004.00000800.00020000.00000000.sdmp, arinzezx.exe, 0000001.00000002.397304814.000000000BAD9000.00000004.00000800.00020000.00000000.sdmp, arinzezx.exe, 00000001.00000003.362398365.00000000BAD9000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/bThe	arinzezx.exe, 00000001.00000002.386131393.0000000009342000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://ocsp.sectigo.com0	arinzezx.exe, 00000004.00000002.590184555.0000000003749000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	arinzezx.exe, 00000001.00000002.386131393.0000000009342000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://DtM6GM1g5LTlJoVP.org	arinzezx.exe, 00000004.00000002.590311251.000000000376C000.00000004.00000800.00020000.00000000.sdmp, arinzezx.exe, 0000004.00000002.589851489.0000000003704000.00000004.00000800.00020000.00000000.sdmp, arinzezx.exe, 00000004.00000002.587010252.0000000033F1000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.tiro.com	arinzezx.exe, 00000001.00000002.386131393.0000000009342000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://cp5ua.hyperhost.ua	arinzezx.exe, 00000004.00000002.590184555.0000000003749000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers	arinzezx.exe, 00000001.00000002.38613139 3.0000000009342000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.goodfont.co.kr	arinzezx.exe, 00000001.00000002.38613139 3.0000000009342000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.000webhost.com/migrate?static=true&M	arinzezx.exe, 00000001.00000002.39180938 1.000000000AFAA000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://maps.google.com/?saddr=31.2087496	arinzezx.exe, 00000001.00000002.37137797 2.0000000002B7B000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://YthClZ.com	arinzezx.exe, 00000004.00000002.58701025 2.00000000033F1000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://can-sat.netai.net/y	arinzezx.exe, 00000001.00000002.39180938 1.000000000AFAA000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://consent.google.com/	arinzezx.exe, 00000001.00000002.39643067 3.000000000B03C000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.sajatypesworks.com	arinzezx.exe, 00000001.00000002.38613139 3.0000000009342000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	arinzezx.exe, 00000001.00000002.38613139 3.0000000009342000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	arinzezx.exe, 00000001.00000002.38613139 3.0000000009342000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	arinzezx.exe, 00000001.00000002.38613139 3.0000000009342000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://can-sat.netai.net/livestream/Hx	arinzezx.exe, 00000001.00000002.39574277 1.000000000AFED000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://fontfabrik.com	arinzezx.exe, 00000001.00000002.38613139 3.0000000009342000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.000webhost.com/migrate?static=true&c	arinzezx.exe, 00000001.00000002.39621193 3.000000000B010000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://DynDns.comDynDNSnamejdpasswordPsi/Psi	arinzezx.exe, 00000004.00000002.58701025 2.00000000033F1000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	arinzezx.exe, 00000001.00000002.38613139 3.0000000009342000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html	arinzezx.exe, 00000001.00000003.32924997 1.0000000008034000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	arinzezx.exe, 00000001.00000003.32425015 5.000000000804B000.00000004.00000800.000 20000.00000000.sdmp, arinzezx.exe, 00000 001.00000002.386131393.0000000009342000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	arinzezx.exe, 00000001.00000002.38613139 3.0000000009342000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	arinzezx.exe, 00000001.00000002.38613139 3.0000000009342000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.000webhost.com/X	arinzezx.exe, 00000001.00000002.39622696 2.000000000B014000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.zhongyicts.com.cn	arinzezx.exe, 00000001.00000002.38613139 3.0000000009342000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	arinzezx.exe, 00000001.00000003.32976567 2.0000000008041000.00000004.00000800.000 20000.00000000.sdmp, arinzezx.exe, 00000 001.00000002.386131393.0000000009342000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://can-sat.netai.net/livestream/CgC	arinzezx.exe, 00000001.00000002.39574277 1.000000000AFED000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://can-sat.netai.n	arinzezx.exe, 00000001.00000002.36830682 3.000000000B74000.00000004.00000010.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://can-sat.netai.net/livestream/5	arinzezx.exe, 00000001.00000002.39228406 3.000000000AFC4000.00000004.00000800.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	arinzezx.exe, 00000004.00000002.59018455 5.0000000003749000.00000004.00000800.000 20000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	arinzezx.exe, 00000001.00000002.38613139 3.0000000009342000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.fontbureau.com	arinzezx.exe, 00000001.00000002.38613139 3.0000000009342000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://sectigo.com/CPS0	arinzezx.exe, 00000004.00000002.59018455 5.0000000003749000.00000004.00000800.000 20000.00000000.sdmp	false	URL Reputation: safe	unknown
http://can-sat.netai.net/livestream/ions.AddInAdapter.v10.0	arinzezx.exe, 00000001.00000002.39228406 3.000000000AFC4000.00000004.00000800.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://https://consent.google.com/ml?continue=https://www.google.com/maps?saddr%3D31.2087496	arinzezx.exe, 00000001.00000002.39616380 9.000000000B009000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	arinzezx.exe, 00000004.00000002.58701025 2.00000000033F1000.00000004.00000800.000 20000.00000000.sdmp	false	URL Reputation: safe	unknown
http://maps.google.com/	arinzezx.exe, 00000001.00000002.39632012 6.000000000B022000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://can-sat.netai.net/livestream/tldi	arinzezx.exe, 00000001.00000002.39228406 3.000000000AFC4000.00000004.00000800.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://can-sat.netai.net/5	arinzezx.exe, 00000001.00000002.36898645 6.000000000E90000.00000004.00000020.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designerse~	arinzezx.exe, 00000001.00000003.33082104 9.0000000008070000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.carterandcone.coml	arinzezx.exe, 00000001.00000002.38613139 3.0000000009342000.00000004.00000800.000 20000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	arinzezx.exe, 00000001.00000002.38613139 3.0000000009342000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.fontbureau.com/designers2~	arinzezx.exe, 00000001.00000003.33181851 4.0000000008070000.00000004.00000800.000 20000.00000000.sdmp, arinzezx.exe, 00000 001.00000003.331395636.000000008070000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://www.ascendercorp.com/typedesigners.htmlu	arinzezx.exe, 00000001.00000003.32924997 1.0000000008034000.00000004.00000800.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	arinzezx.exe, 00000001.00000002.38613139 3.0000000009342000.00000004.00000800.000 20000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	arinzezx.exe, 00000001.00000002.38613139 3.0000000009342000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.tiro.comY	arinzezx.exe, 00000001.00000003.32469381 5.000000000804B000.00000004.00000800.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	arinzezx.exe, 00000001.00000002.38613139 3.0000000009342000.00000004.00000800.000 20000.00000000.sdmp	false	URL Reputation: safe	unknown
http://maps.google.com/maps?saddr=31.2087496	arinzezx.exe, 00000001.00000002.39621193 3.000000000B010000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://www.000webhost.com/	arinzezx.exe, 00000001.00000002.39622696 2.000000000B014000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://can-sat.netai.net/livestream/46	arinzezx.exe, 00000001.00000002.36898645 6.000000000E90000.00000004.00000020.000 20000.00000000.sdmp	false	Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://can-sat.netai.net/livestream/e	arinzezx.exe, 00000001.00000002.39228406 3.000000000AFC000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	arinzezx.exe, 00000001.00000002.38613139 3.0000000009342000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://www.google.com/_	arinzezx.exe, 00000001.00000002.39632012 6.000000000B022000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://can-sat.netai.net/livestream/ll	arinzezx.exe, 00000001.00000002.39228406 3.000000000AFC000.00000004.00000800.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.google.com/	arinzezx.exe, 00000001.00000002.39632012 6.000000000B022000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://www.google.com/maps?saddr=31.2087496	arinzezx.exe, 00000001.00000002.39621193 3.000000000B010000.00000004.00000800.000 20000.00000000.sdmp, arinzezx.exe, 00000 001.00000002.396320126.000000000B022000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.google.com/maps?saddr%3D31.2087496	arinzezx.exe, 00000001.00000002.39173680 8.000000000AFA1000.00000004.00000800.000 20000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.58.215.238	consent.google.com	United States		15169	GOOGLEUS	false
104.19.184.120	www.000webhost.com	United States		13335	CLOUDFLARENETUS	false
142.250.203.100	www.google.com	United States		15169	GOOGLEUS	false
153.92.0.100	can-sat.netai.net	Germany		204915	AWEXUS	false
142.250.203.110	maps.google.com	United States		15169	GOOGLEUS	false
91.235.128.141	cp5ua.hyperhost.ua	Ukraine		15626	ITLASUA	false

Private

IP
192.168.2.1

General Information	
Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	694556
Start date and time:	2022-08-31 23:46:48 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	arinzezx.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	18
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@6/7
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings
• Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded domains from analysis (whitelisted): eudb.ris.api.iris.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com • Not all processes where analyzed, report is missing behavior information • Report creation exceeded maximum time and may have missing d isassembly code 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. • VT rate limit hit for: arinzezx.exe

Simulations		
Behavior and APIs		
Time	Type	Description
23:48:05	API Interceptor	666x Sleep call for process: arinzezx.exe modified

Joe Sandbox View / Context
IPs
 No context

Domains
 No context
ASNs
 No context
JA3 Fingerprints
 No context
Dropped Files
 No context

Created / dropped Files	
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\arinzezx.exe.log 	
Process:	C:\Users\user\Desktop\arinzezx.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1421
Entropy (8bit):	5.3458551807012835
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE49E4184F0:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz8
MD5:	DD8C1D6EF5A3F10AA0CAC71550CF950A
SHA1:	9EBD88472EFFCE6D3CB76038B1F18091D6380083
SHA-256:	A711E30BAC1BD29BF2FFA7FDA00D2F01E1978DA22F2F941E877B5C3A8476F17F
SHA-512:	2130B3804715A279E40B085702552BCB647AA5F0ED39FD1E90A8F963C8EB6D736190CB37147427C1A9CCA1AB0AF30BAB62649E045116334DF52923F0A7406A6F
Malicious:	true
Reputation:	moderate, 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, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72 e6\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\1d8480152e0da9a60ad49c6d16a3b6d\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\S ystem.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b 77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\1b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\B87Z87FM\livestream[1].htm	
Process:	C:\Users\user\Desktop\arinzezx.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	162
Entropy (8bit):	4.43530643106624
Encrypted:	false
SSDEEP:	3:qVoB3IUROGclXqyvXboAcMBXqWSZUXqXIIVLLP61IwcWWGu:q43tSI6kXiMIWSU6XII5LP8lpfGu
MD5:	4F8E702CC244EC5D4DE32740C0ECBD97
SHA1:	3ADB1F02D5B6054DE0046E367C1D687B6CDF7AFF
SHA-256:	9E17CB15DD75BBBD5DBB984EDA674863C3B10AB72613CF8A39A00C3E11A8492A
SHA-512:	21047FEA5269FEE75A2A187AA09316519E35068CB2F276CFAF371E5224445E9D5C98497BD76FB9608D2B73E9DAC1A3F5BFADFDC4623C479D53ECF93D81D3C F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	<html>..<head><title>301 Moved Permanently</title></head>..<body>..<center> 301 Moved Permanently </center>..<hr><center>nginx</center>..</body>.. </html>..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.2761539654732506
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:	arinzezx.exe
File size:	1527808
MD5:	314c678d85f7927a42f34797627532e1
SHA1:	1a1695ee1411cc14754cc92e14a6243ee7af81d1
SHA256:	e5b9cc21b8de77e68e03e202609511b8b57d1ea278d6cd0fe0b7fb454f1d7432
SHA512:	40b9a9373cd8590cb70d8ba289d4fe0d83d5dbff81a6b6c17baf03142f4627fdeee36547a15b5b4d2b77c650ea74001ee10abe98ec6f6ba8333e9cdf57f2ca09
SSDEEP:	24576:H+tsF5jvq3uXN7+ZZ56+ncKxRGXUO+C+O/suliuM:ec5jvt856+ncaO+CV/sa
TLSH:	BD655B9C7650B2AFC817CE76CAA45C24F6A0B56B430BE743A05326ED9D0D69BCF150F2
File Content Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode....\$......PE..L...{l.c.....0..\$....*.....B... ..`.....@..@.....

File Icon



Icon Hash:	f0e4d068c4f4d470
------------	------------------

Static PE Info

General

Entrypoint:	0x57422e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x630F6C7B [Wed Aug 31 14:13:15 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

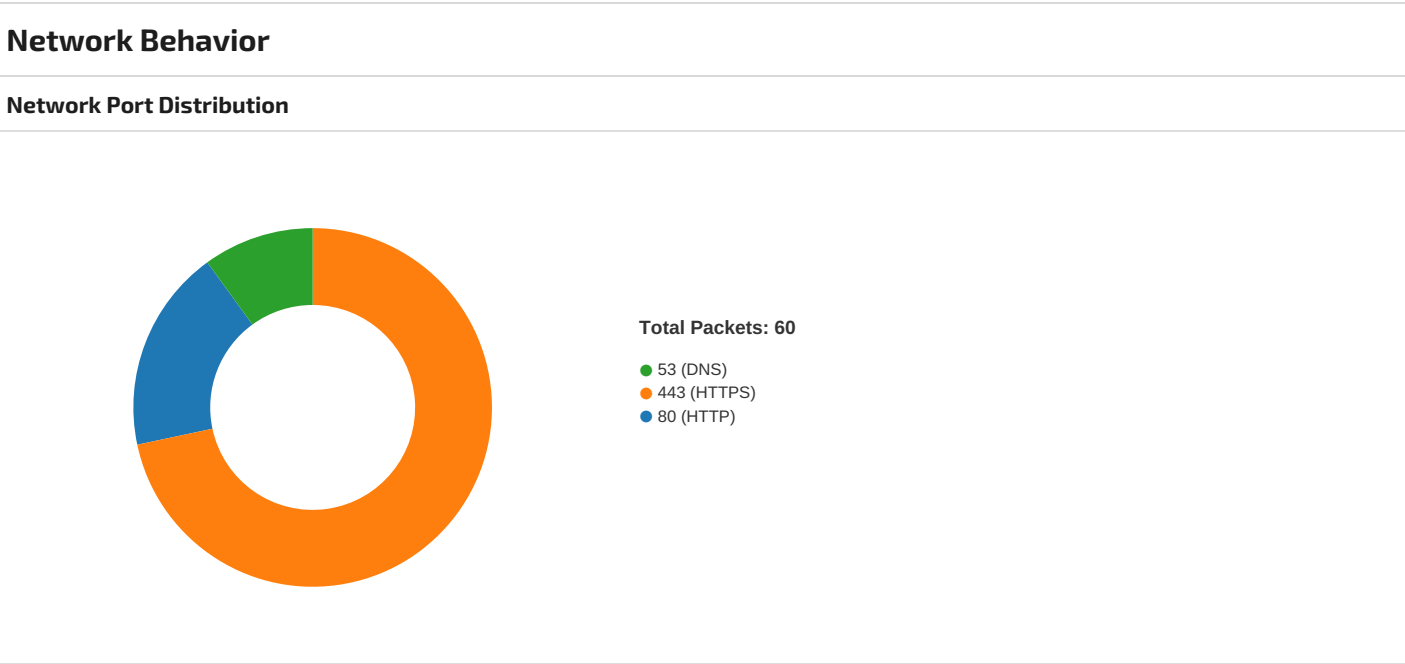
Entrypoint Preview

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
```


Resources					
Name	RVA	Size	Type	Language	Country
RT_ICON	0x176130	0x1fcb	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0x1780fc	0x14	data		
RT_VERSION	0x178110	0x320	data		
RT_MANIFEST	0x178430	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports	
DLL	Import
mscoree.dll	_CorExeMain



TCP Packets				
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:48:04.576775074 CEST	49714	80	192.168.2.5	142.250.203.110
Aug 31, 2022 23:48:04.577162981 CEST	49715	80	192.168.2.5	153.92.0.100
Aug 31, 2022 23:48:04.593622923 CEST	80	49714	142.250.203.110	192.168.2.5
Aug 31, 2022 23:48:04.593744993 CEST	49714	80	192.168.2.5	142.250.203.110
Aug 31, 2022 23:48:04.595390081 CEST	49714	80	192.168.2.5	142.250.203.110
Aug 31, 2022 23:48:04.612171888 CEST	80	49714	142.250.203.110	192.168.2.5
Aug 31, 2022 23:48:04.699640989 CEST	80	49714	142.250.203.110	192.168.2.5
Aug 31, 2022 23:48:04.699734926 CEST	49714	80	192.168.2.5	142.250.203.110
Aug 31, 2022 23:48:04.709311008 CEST	80	49715	153.92.0.100	192.168.2.5
Aug 31, 2022 23:48:04.709398031 CEST	49715	80	192.168.2.5	153.92.0.100
Aug 31, 2022 23:48:04.734621048 CEST	49715	80	192.168.2.5	153.92.0.100
Aug 31, 2022 23:48:04.738118887 CEST	49714	80	192.168.2.5	142.250.203.110
Aug 31, 2022 23:48:04.755947113 CEST	80	49714	142.250.203.110	192.168.2.5
Aug 31, 2022 23:48:04.866863012 CEST	80	49715	153.92.0.100	192.168.2.5
Aug 31, 2022 23:48:04.866895914 CEST	80	49715	153.92.0.100	192.168.2.5
Aug 31, 2022 23:48:04.867017984 CEST	49715	80	192.168.2.5	153.92.0.100
Aug 31, 2022 23:48:06.168876886 CEST	49716	443	192.168.2.5	104.19.184.120
Aug 31, 2022 23:48:06.168926001 CEST	443	49716	104.19.184.120	192.168.2.5
Aug 31, 2022 23:48:06.169018030 CEST	49716	443	192.168.2.5	104.19.184.120
Aug 31, 2022 23:48:06.386010885 CEST	80	49714	142.250.203.110	192.168.2.5
Aug 31, 2022 23:48:06.386142969 CEST	49714	80	192.168.2.5	142.250.203.110
Aug 31, 2022 23:48:06.574127913 CEST	49716	443	192.168.2.5	104.19.184.120

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:48:06.574150085 CEST	443	49716	104.19.184.120	192.168.2.5
Aug 31, 2022 23:48:06.627569914 CEST	443	49716	104.19.184.120	192.168.2.5
Aug 31, 2022 23:48:06.627779961 CEST	49716	443	192.168.2.5	104.19.184.120
Aug 31, 2022 23:48:09.230206966 CEST	49717	443	192.168.2.5	142.250.203.100
Aug 31, 2022 23:48:09.230243921 CEST	443	49717	142.250.203.100	192.168.2.5
Aug 31, 2022 23:48:09.230318069 CEST	49717	443	192.168.2.5	142.250.203.100
Aug 31, 2022 23:48:09.866502047 CEST	80	49715	153.92.0.100	192.168.2.5
Aug 31, 2022 23:48:09.866643906 CEST	49715	80	192.168.2.5	153.92.0.100
Aug 31, 2022 23:48:09.873178959 CEST	49717	443	192.168.2.5	142.250.203.100
Aug 31, 2022 23:48:09.873193979 CEST	443	49717	142.250.203.100	192.168.2.5
Aug 31, 2022 23:48:09.930548906 CEST	443	49717	142.250.203.100	192.168.2.5
Aug 31, 2022 23:48:09.930721998 CEST	49717	443	192.168.2.5	142.250.203.100
Aug 31, 2022 23:48:10.719584942 CEST	49717	443	192.168.2.5	142.250.203.100
Aug 31, 2022 23:48:10.719602108 CEST	443	49717	142.250.203.100	192.168.2.5
Aug 31, 2022 23:48:10.719846010 CEST	49716	443	192.168.2.5	104.19.184.120
Aug 31, 2022 23:48:10.719861984 CEST	443	49717	142.250.203.100	192.168.2.5
Aug 31, 2022 23:48:10.719871998 CEST	443	49716	104.19.184.120	192.168.2.5
Aug 31, 2022 23:48:10.719922066 CEST	49717	443	192.168.2.5	142.250.203.100
Aug 31, 2022 23:48:10.720099926 CEST	443	49716	104.19.184.120	192.168.2.5
Aug 31, 2022 23:48:10.720168114 CEST	49716	443	192.168.2.5	104.19.184.120
Aug 31, 2022 23:48:10.723875046 CEST	49717	443	192.168.2.5	142.250.203.100
Aug 31, 2022 23:48:10.724464893 CEST	49716	443	192.168.2.5	104.19.184.120
Aug 31, 2022 23:48:10.747525930 CEST	443	49716	104.19.184.120	192.168.2.5
Aug 31, 2022 23:48:10.747577906 CEST	443	49716	104.19.184.120	192.168.2.5
Aug 31, 2022 23:48:10.747678041 CEST	49716	443	192.168.2.5	104.19.184.120
Aug 31, 2022 23:48:10.747699022 CEST	49716	443	192.168.2.5	104.19.184.120
Aug 31, 2022 23:48:10.767368078 CEST	443	49717	142.250.203.100	192.168.2.5
Aug 31, 2022 23:48:12.369606972 CEST	443	49717	142.250.203.100	192.168.2.5
Aug 31, 2022 23:48:12.369786978 CEST	49717	443	192.168.2.5	142.250.203.100
Aug 31, 2022 23:48:12.369798899 CEST	443	49717	142.250.203.100	192.168.2.5
Aug 31, 2022 23:48:12.369852066 CEST	49717	443	192.168.2.5	142.250.203.100
Aug 31, 2022 23:48:12.381283998 CEST	443	49717	142.250.203.100	192.168.2.5
Aug 31, 2022 23:48:12.381340981 CEST	443	49717	142.250.203.100	192.168.2.5
Aug 31, 2022 23:48:12.381407976 CEST	49717	443	192.168.2.5	142.250.203.100
Aug 31, 2022 23:48:12.381418943 CEST	49717	443	192.168.2.5	142.250.203.100
Aug 31, 2022 23:48:12.402407885 CEST	49717	443	192.168.2.5	142.250.203.100
Aug 31, 2022 23:48:12.402427912 CEST	443	49717	142.250.203.100	192.168.2.5
Aug 31, 2022 23:48:12.402451038 CEST	49717	443	192.168.2.5	142.250.203.100
Aug 31, 2022 23:48:12.402487993 CEST	49717	443	192.168.2.5	142.250.203.100
Aug 31, 2022 23:48:12.445267916 CEST	49718	443	192.168.2.5	216.58.215.238
Aug 31, 2022 23:48:12.445334911 CEST	443	49718	216.58.215.238	192.168.2.5
Aug 31, 2022 23:48:12.445437908 CEST	49718	443	192.168.2.5	216.58.215.238
Aug 31, 2022 23:48:12.495666981 CEST	49718	443	192.168.2.5	216.58.215.238
Aug 31, 2022 23:48:12.495704889 CEST	443	49718	216.58.215.238	192.168.2.5
Aug 31, 2022 23:48:12.558326006 CEST	443	49718	216.58.215.238	192.168.2.5
Aug 31, 2022 23:48:12.558475971 CEST	49718	443	192.168.2.5	216.58.215.238
Aug 31, 2022 23:48:12.560187101 CEST	443	49718	216.58.215.238	192.168.2.5
Aug 31, 2022 23:48:12.560255051 CEST	49718	443	192.168.2.5	216.58.215.238
Aug 31, 2022 23:48:12.591414928 CEST	49718	443	192.168.2.5	216.58.215.238
Aug 31, 2022 23:48:12.591439009 CEST	443	49718	216.58.215.238	192.168.2.5
Aug 31, 2022 23:48:12.591686964 CEST	443	49718	216.58.215.238	192.168.2.5
Aug 31, 2022 23:48:12.591770887 CEST	49718	443	192.168.2.5	216.58.215.238
Aug 31, 2022 23:48:12.593329906 CEST	49718	443	192.168.2.5	216.58.215.238
Aug 31, 2022 23:48:12.635369062 CEST	443	49718	216.58.215.238	192.168.2.5
Aug 31, 2022 23:48:12.653110981 CEST	443	49718	216.58.215.238	192.168.2.5
Aug 31, 2022 23:48:12.653152943 CEST	443	49718	216.58.215.238	192.168.2.5
Aug 31, 2022 23:48:12.653192043 CEST	49718	443	192.168.2.5	216.58.215.238
Aug 31, 2022 23:48:12.653218031 CEST	443	49718	216.58.215.238	192.168.2.5
Aug 31, 2022 23:48:12.653233051 CEST	49718	443	192.168.2.5	216.58.215.238

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:48:12.653261900 CEST	49718	443	192.168.2.5	216.58.215.238
Aug 31, 2022 23:48:12.654133081 CEST	443	49718	216.58.215.238	192.168.2.5
Aug 31, 2022 23:48:12.654172897 CEST	443	49718	216.58.215.238	192.168.2.5
Aug 31, 2022 23:48:12.654202938 CEST	49718	443	192.168.2.5	216.58.215.238
Aug 31, 2022 23:48:12.654211998 CEST	443	49718	216.58.215.238	192.168.2.5
Aug 31, 2022 23:48:12.654249907 CEST	49718	443	192.168.2.5	216.58.215.238
Aug 31, 2022 23:48:12.654275894 CEST	49718	443	192.168.2.5	216.58.215.238
Aug 31, 2022 23:48:12.655402899 CEST	443	49718	216.58.215.238	192.168.2.5
Aug 31, 2022 23:48:12.655468941 CEST	49718	443	192.168.2.5	216.58.215.238
Aug 31, 2022 23:48:12.655528069 CEST	443	49718	216.58.215.238	192.168.2.5
Aug 31, 2022 23:48:12.655570984 CEST	49718	443	192.168.2.5	216.58.215.238
Aug 31, 2022 23:48:12.656781912 CEST	443	49718	216.58.215.238	192.168.2.5
Aug 31, 2022 23:48:12.656836033 CEST	49718	443	192.168.2.5	216.58.215.238
Aug 31, 2022 23:48:12.656836987 CEST	443	49718	216.58.215.238	192.168.2.5
Aug 31, 2022 23:48:12.656868935 CEST	443	49718	216.58.215.238	192.168.2.5
Aug 31, 2022 23:48:12.656898022 CEST	49718	443	192.168.2.5	216.58.215.238
Aug 31, 2022 23:48:12.656919003 CEST	49718	443	192.168.2.5	216.58.215.238
Aug 31, 2022 23:48:12.657917023 CEST	443	49718	216.58.215.238	192.168.2.5
Aug 31, 2022 23:48:12.657993078 CEST	49718	443	192.168.2.5	216.58.215.238

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 31, 2022 23:48:04.422735929 CEST	49177	53	192.168.2.5	8.8.8.8
Aug 31, 2022 23:48:04.450783968 CEST	53	49177	8.8.8.8	192.168.2.5
Aug 31, 2022 23:48:04.527575016 CEST	61452	53	192.168.2.5	8.8.8.8
Aug 31, 2022 23:48:04.558106899 CEST	53	61452	8.8.8.8	192.168.2.5
Aug 31, 2022 23:48:06.056193113 CEST	65323	53	192.168.2.5	8.8.8.8
Aug 31, 2022 23:48:06.078233957 CEST	53	65323	8.8.8.8	192.168.2.5
Aug 31, 2022 23:48:07.941476107 CEST	51484	53	192.168.2.5	8.8.8.8
Aug 31, 2022 23:48:07.969182014 CEST	53	51484	8.8.8.8	192.168.2.5
Aug 31, 2022 23:48:12.412324905 CEST	63446	53	192.168.2.5	8.8.8.8
Aug 31, 2022 23:48:12.440073013 CEST	53	63446	8.8.8.8	192.168.2.5
Aug 31, 2022 23:48:33.922821045 CEST	60975	53	192.168.2.5	8.8.8.8
Aug 31, 2022 23:48:33.950745106 CEST	53	60975	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 31, 2022 23:48:04.422735929 CEST	192.168.2.5	8.8.8.8	0x7761	Standard query (0)	maps.google.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:04.527575016 CEST	192.168.2.5	8.8.8.8	0xb174	Standard query (0)	can-sat.netai.net	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:06.056193113 CEST	192.168.2.5	8.8.8.8	0x59e3	Standard query (0)	www.000webhost.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:07.941476107 CEST	192.168.2.5	8.8.8.8	0xa65d	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:12.412324905 CEST	192.168.2.5	8.8.8.8	0xf296	Standard query (0)	consent.google.com	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:33.922821045 CEST	192.168.2.5	8.8.8.8	0xe3eb	Standard query (0)	cp5ua.hyperhost.ua	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 31, 2022 23:48:04.450783968 CEST	8.8.8.8	192.168.2.5	0x7761	No error (0)	maps.google.com		142.250.203.110	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:04.558106899 CEST	8.8.8.8	192.168.2.5	0xb174	No error (0)	can-sat.netai.net		153.92.0.100	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:06.078233957 CEST	8.8.8.8	192.168.2.5	0x59e3	No error (0)	www.000webhost.com		104.19.184.120	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:06.078233957 CEST	8.8.8.8	192.168.2.5	0x59e3	No error (0)	www.000webhost.com		104.19.185.120	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 31, 2022 23:48:07.969182014 CEST	8.8.8.8	192.168.2.5	0xa65d	No error (0)	www.google.com		142.250.203.100	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:12.440073013 CEST	8.8.8.8	192.168.2.5	0xf296	No error (0)	consent.google.com		216.58.215.238	A (IP address)	IN (0x0001)
Aug 31, 2022 23:48:33.950745106 CEST	8.8.8.8	192.168.2.5	0xe3eb	No error (0)	cp5ua.hype rhost.ua		91.235.128.141	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.google.com
- www.000webhost.com
- consent.google.com
- maps.google.com
- can-sat.netai.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49717	142.250.203.100	443	C:\Users\user\Desktop\larinzezx.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49716	104.19.184.120	443	C:\Users\user\Desktop\larinzezx.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49718	216.58.215.238	443	C:\Users\user\Desktop\larinzezx.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49714	142.250.203.110	80	C:\Users\user\Desktop\larinzezx.exe

Timestamp	kBytes transferred	Direction	Data
Aug 31, 2022 23:48:04.595390081 CEST	822	OUT	GET /?saddr=31.2087496,29.9091634&z=10 HTTP/1.1 Accept: */* Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: maps.google.com Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 31, 2022 23:48:04.699640989 CEST	823	IN	HTTP/1.1 302 Found Location: http://maps.google.com/maps?saddr=31.2087496,29.9091634&z=10 Cache-Control: private Content-Type: text/html; charset=UTF-8 Date: Wed, 31 Aug 2022 21:48:04 GMT Server: gws Content-Length: 261 X-XSS-Protection: 0 X-Frame-Options: SAMEORIGIN Set-Cookie: AEC=AakniGOUVp4jXHHD5YhzAajOatKevD6jDoHGMxHhgsCt6t1rStwPaLBqLg; expires=Mon, 27-Feb-2023 21:48:04 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax Data Raw: 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 3c 54 49 54 4c 45 3e 33 30 32 20 4d 6f 76 65 64 3c 2f 54 49 54 4c 45 3e 3c 2f 48 45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 33 30 32 20 4d 6f 76 65 64 3c 2f 48 31 3e 0a 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 0a 3c 41 20 48 52 45 46 3d 22 68 74 74 70 3a 2f 2f 6d 61 70 73 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 6d 61 70 73 3f 73 61 64 64 72 3d 33 31 2e 32 30 38 37 34 39 36 2c 32 39 2e 39 30 39 31 36 33 34 26 61 6d 70 3b 7a 3d 31 30 22 3e 68 65 72 65 3c 2f 41 3e 2e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8"><TITLE>302 Moved</TITLE></HEAD><BODY><H1>302 Moved</H1>The document has movedhere.</BODY></HTML>
Aug 31, 2022 23:48:04.738118887 CEST	824	OUT	GET /maps?saddr=31.2087496,29.9091634&z=10 HTTP/1.1 Accept: /* Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: maps.google.com Connection: Keep-Alive
Aug 31, 2022 23:48:06.386010885 CEST	884	IN	HTTP/1.1 302 Found Location: https://www.google.com:443/maps?saddr=31.2087496,29.9091634&z=10 Cache-Control: private Timing-Allow-Origin: https://www.google.com Content-Type: text/html; charset=UTF-8 Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-RbpRlc1wZu3MpKqYcMBkxg' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/maps-tactile Cross-Origin-Opener-Policy: same-origin-allow-popups; report-to="gws" Report-To: {"group":"gws","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/gws/maps-tactile"}]}\nDate: Wed, 31 Aug 2022 21:48:06 GMT\nServer: gws\nContent-Length: 265\nX-XSS-Protection: 0\nX-Frame-Options: SAMEORIGIN\nData Raw: 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 3c 54 49 54 4c 45 3e 33 30 32 20 4d 6f 76 65 64 3c 2f 54 49 54 4c 45 3e 3c 2f 48 45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 33 30 32 20 4d 6f 76 65 64 3c 2f 48 31 3e 0a 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 0a 3c 41 20 48 52 45 46 3d 22 68 74 74 70 3a 2f 2f 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 3a 34 34 33 2f 6d 61 70 73 3f 73 61 64 64 72 3d 33 31 2e 32 30 38 37 34 39 36 2c 32 39 2e 39 30 39 31 36 33 34 26 61 6d 70 3b 7a 3d 31 30 22 3e 68 65 72 65 3c 2f 41 3e 2e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8"><TITLE>302 Moved</TITLE></HEAD><BODY><H1>302 Moved</H1>The document has movedhere.</BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49715	153.92.0.100	80	C:\Users\user\Desktop\larinzezx.exe

Timestamp	kBytes transferred	Direction	Data
Aug 31, 2022 23:48:04.734621048 CEST	824	OUT	GET /livestream/ HTTP/1.1 Accept: /* Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Host: can-sat.netai.net Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Aug 31, 2022 23:48:04.866895914 CEST	836	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 31 Aug 2022 21:48:04 GMT Content-Type: text/html Content-Length: 162 Connection: keep-alive Location: https://www.000webhost.com/migrate?static=true X-Frame-Options: sameorigin X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body><center> 301 Moved Permanently </center><hr><center>nginx</center></body></html>

HTTPS Proxied Packets					
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49717	142.250.203.100	443	C:\Users\user\Desktop\larinzezx.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-31 21:48:10 UTC	0	OUT	GET /maps?saddr=31.2087496,29.9091634&z=10 HTTP/1.1 Accept: */* Accept-Language: en-US Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729) Connection: Keep-Alive Host: www.google.com Cookie: AEC=AakniGOUVp4jXHHD5YhzAajOatKevD6jDoHGMxHhgsCt6t1rStwPaLBqLg
2022-08-31 21:48:12 UTC	1	IN	HTTP/1.1 302 Found Location: https://consent.google.com/ml?continue=https://www.google.com/maps?saddr%3D31.2087496,29.9091634&gl=GB&m=0&pc=m&uxe=eomtm&hl=de&src=1 Cache-Control: private Timing-Allow-Origin: https://www.google.com Content-Type: text/html; charset=UTF-8 Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-eYZYv7vRwthqp9Ru1E-35A' 'strict-dynamic' 'report-sample' 'unsafe-eval' 'unsafe-inline' https: http:;report-uri https://csp.withgoogle.com/csp/gws/maps-tactile Cross-Origin-Opener-Policy: same-origin-allow-popups; report-to="gws" Report-To: {"group":"gws","max_age":2592000,"endpoints":[{"url":"https://csp.withgoogle.com/csp/report-to/gws/maps-tactile"}]}} P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Date: Wed, 31 Aug 2022 21:48:12 GMT Server: gws Content-Length: 354 X-XSS-Protection: 0 X-Frame-Options: SAMEORIGIN Set-Cookie: __Secure-ENID=6.SE=bAHSQtlrQMWxy_tqz0WaDaeFL1W5VOmOKkO5mBuNXISlweN8ghtdM05hF-gECfwTJ28xi6MWi6sNJZJsO8QjQObRoGTdPzM-68Gkxop6bVdx8jKoV8MxbLdPglHJvYSyJREMuxUbqTR9T7NbGnUTXMHWRPSNiDAhrFDcYhFn5sM; expires=Sun, 01-Oct-2023 14:06:30 GMT; path=/; domain=.google.com; Secure; HttpOnly; SameSite=lax Set-Cookie: CONSENT=PENDING+026; expires=Fri, 30-Aug-2024 21:48:10 GMT; path=/; domain=.google.com; Secure Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000,h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43" Connection: close
2022-08-31 21:48:12 UTC	2	IN	Data Raw: 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 3c 54 49 54 4c 45 3e 33 30 32 20 4d 6f 76 65 64 3c 2f 54 49 54 4c 45 3e 3c 2f 48 45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 33 30 32 20 4d 6f 76 65 64 3c 2f 48 31 3e 0a 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 0a 3c 41 20 48 52 45 46 3d 22 68 74 74 70 73 3a 2f 2f 63 6f 6e 73 65 6e 74 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 6d 6c 3f 63 6f 6e 74 69 6e 75 65 3d 68 74 74 70 73 3a 2f 2f 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 6d 61 70 73 3f 73 61 64 64 72 25 33 44 33 31 2e 32 30 38 37 34 39 36 2c 32 Data Ascii: <HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=utf-8"><TITLE>302 Moved</TITLE></HEAD><BODY><H1>302 Moved</H1>The document has moved<A HREF="https://consent.google.com/ml?continue=https://www.google.com/maps?saddr%3D31.2087496,2

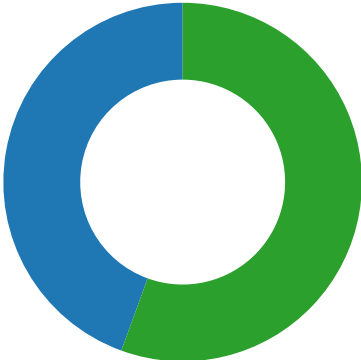
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49716	104.19.184.120	443	C:\Users\user\Desktop\larinzezx.exe

Timestamp	kBytes transferred	Direction	Data
2022-08-31 21:48:12 UTC	18	IN	Data Raw: 22 3e ed 95 9c ea b5 ad ec 96 b4 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 22 6a 61 22 3e e6 97 a5 e6 9c ac e8 aa 9e 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 22 7a 68 2d 43 4e 22 3e e7 ae 80 e4 bd 93 e4 b8 ad e6 96 87 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 22 7a 68 2d 54 57 22 3e e7 b9 81 e9 ab 94 e4 b8 ad e6 96 87 3c 2f 6f 70 74 69 6f 6e 3e 3c 6f 70 74 69 6f 6e 20 76 61 6c 75 65 3d 22 7a 68 2d 48 4b 22 3e e7 b9 81 e9 ab 94 e4 b8 ad e6 96 87 26 6e 62 73 70 3b 28 e9 a6 99 e6 b8 af 29 3c 2f 6f 70 74 69 6f 6e 3e 3c 2f 73 65 6c 65 63 74 3e 3c 69 6e 70 75 74 20 74 79 70 65 3d 22 68 69 64 64 65 6e 22 20 6e 61 6d 65 3d 22 6f 6c 64 68 6c 22 20 76 61 6c 75 65 3d 22 64 65 22 3e 3c Data Ascii: "</option><option value="ja"></option><option value="zh-CN"></option><option value="zh-TW"></option><option value="zh-HK"> ()</option></select><input type="hidden" name="oldhl" value="de"><
2022-08-31 21:48:12 UTC	18	IN	Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

SMTP Packets						
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands	
Aug 31, 2022 23:48:34.138493061 CEST	587	49725	91.235.128.141	192.168.2.5	220-cp5ua.hyperhost.ua ESMTP Exim 4.95 #2 Thu, 01 Sep 2022 00:48:33 +0300 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.	
Aug 31, 2022 23:48:34.138813019 CEST	49725	587	192.168.2.5	91.235.128.141	EHLO 528110	
Aug 31, 2022 23:48:34.191039085 CEST	587	49725	91.235.128.141	192.168.2.5	250-cp5ua.hyperhost.ua Hello 528110 [102.129.143.57] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-STARTTLS 250 HELP	
Aug 31, 2022 23:48:34.191276073 CEST	49725	587	192.168.2.5	91.235.128.141	STARTTLS	
Aug 31, 2022 23:48:34.246081114 CEST	587	49725	91.235.128.141	192.168.2.5	220 TLS go ahead	

Statistics

Behavior



● arinzezx.exe

● arinzezx.exe

● arinzezx.exe

💡 Click to jump to process

System Behavior	
Analysis Process: arinzezx.exe PID: 6600, Parent PID: 1424	
General	
Target ID:	1
Start time:	23:47:52
Start date:	31/08/2022

Path:	C:\Users\user\Desktop\arinzezx.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\arinzezx.exe"
Imagebase:	0x670000
File size:	1527808 bytes
MD5 hash:	314C678D85F7927A42F34797627532E1
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: 00000001.00000002.376461043.0000000002F25000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.381932594.0000000004787000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.381932594.0000000004787000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000001.00000002.381932594.0000000004787000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
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	6CC0CF06	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	6CC0CF06	unknown	
C:\Users\user\AppData\Local\Microsof\CLR_v4.0.32\UsageLogs\arinzezx.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6CF1C78D	CreateFileW	

File Written									
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol	
C:\Users\user\AppData\Local\Microsof\CLR_v4.0.32\UsageLogs\arinzezx.exe.log	0	1421	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	6CF1C907	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	6CBE5705	unknown	

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CBE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CB403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CBECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CB403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CB403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CB403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CB403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CBE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CBE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BA51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BA51B4F	ReadFile

Analysis Process: arinzezx.exe PID: 6964, Parent PID: 6600

General	
Target ID:	3
Start time:	23:48:13
Start date:	31/08/2022
Path:	C:\Users\user\Desktop\arinzezx.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\arinzezx.exe
Imagebase:	0x410000
File size:	1527808 bytes
MD5 hash:	314C678D85F7927A42F34797627532E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: arinzezx.exe PID: 6976, Parent PID: 6600

General	
Target ID:	4
Start time:	23:48:14
Start date:	31/08/2022
Path:	C:\Users\user\Desktop\arinzezx.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\arinzezx.exe
Imagebase:	0xf60000
File size:	1527808 bytes
MD5 hash:	314C678D85F7927A42F34797627532E1
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: 00000004.00000000.365108165.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000000.365108165.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security - Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000004.00000000.365108165.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.587010252.00000000033F1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.587010252.00000000033F1000.00000004.00000800.00020000.00000000.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	6CC0CF06	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	6CC0CF06	unknown

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	6CBE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CBE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CB403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CBECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CB403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CB403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CB403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CB403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CBE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CBE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BA51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BA51B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BA51B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\bfeb4279-08fd-481b-a43b-6bb0808ba818	unknown	4096	success or wait	1	6BA51B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BA51B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6BA51B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6BA51B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default>Login Data	unknown	49152	success or wait	1	6BA51B4F	ReadFile

Disassembly

 No disassembly