ID: 680483
Sample Name: Technical information zip.exe
Cookbook: default.jbs
Time: 17:20:35
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

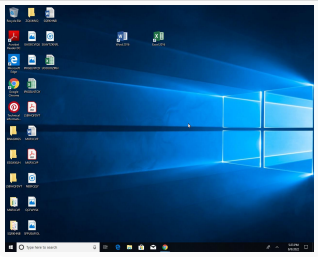
Windows Analysis Report

Technical information zip.exe

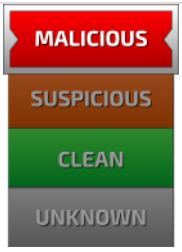
Overview

General Information

Sample Name:	Technical information zip.exe
Analysis ID:	680483
MD5:	ca033c84f5a371…
SHA1:	23f023abfef70de..
SHA256:	bfcb8ee096a65d..
Tags:	exe
Infos:	



Detection



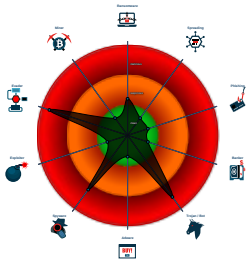
AgentTesla

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

Signatures

- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Snort IDS alert for network traffic
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Yara detected Generic Downloader
- .NET source code contains very larg…
- Queries sensitive network adapter in…
- Tries to harvest and steal browser in…

Classification



Process Tree

- **System is w10x64**
- Technical information zip.exe (PID: 4828 cmdline: "C:\Users\user\Desktop\Technical information zip.exe" MD5: CA033C84F5A37105D613C6961B724E97)
  - Technical information zip.exe (PID: 6128 cmdline: C:\Users\user\Desktop\Technical information zip.exe MD5: CA033C84F5A37105D613C6961B724E97)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "sales@cabletraychina.com",
  "Password": "Jhdq2017#",
  "Host": "mail.cabletraychina.com"
}
```

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
Technical information zip.exe	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.305256005.000000000445B000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.305256005.000000000445B000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.305256005.000000000445B000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x69c26:$a3: MailAccountConfiguration • 0x9fe46:$a3: MailAccountConfiguration • 0xd5e66:$a3: MailAccountConfiguration • 0x69c3f:$a5: SmtpAccountConfiguration • 0x9fe5f:$a5: SmtpAccountConfiguration • 0xd5e7f:$a5: SmtpAccountConfiguration • 0x69c06:$a8: set_BindingAccountConfiguration • 0x9fe26:$a8: set_BindingAccountConfiguration • 0xd5e46:$a8: set_BindingAccountConfiguration • 0x68b66:$a11: get_securityProfile • 0x9ed86:$a11: get_securityProfile • 0xd4da6:$a11: get_securityProfile • 0x68a07:$a12: get_useSeparateFolderTree • 0x9ec27:$a12: get_useSeparateFolderTree • 0xd4c47:$a12: get_useSeparateFolderTree • 0x6a369:$a13: get_DnsResolver • 0xa0589:$a13: get_DnsResolver • 0xd65a9:$a13: get_DnsResolver • 0x68e16:$a14: get_archivingScope • 0x9f036:$a14: get_archivingScope • 0xd5056:$a14: get_archivingScope
00000006.00000000.293840755.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000000.293840755.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Technical information zip.exe.4493998.7.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Technical information zip.exe.4493998.7.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.Technical information zip.exe.4493998.7.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x2ef49:$s1: get_kbok • 0x2f87d:$s2: get_CHoo • 0x304d8:$s3: set_passwordIsSet • 0x2ed4d:$s4: get_enableLog • 0x333f7:$s8: torbrowser • 0x31dd3:$s10: logins • 0x3174b:$s11: credential • 0x2e133:$g1: get_Clipboard • 0x2e141:$g2: get_Keyboard • 0x2e14e:$g3: get_Password • 0x2f72b:$g4: get_CtrlKeyDown • 0x2f73b:$g5: get_ShiftKeyDown • 0x2f74c:$g6: get_AltKeyDown
0.2.Technical information zip.exe.4493998.7.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x2f48e:$a3: MailAccountConfiguration • 0x2f4a7:$a5: SmtpAccountConfiguration • 0x2f46e:$a8: set_BindingAccountConfiguration • 0x2e3ce:$a11: get_securityProfile • 0x2e26f:$a12: get_useSeparateFolderTree • 0x2fbd1:$a13: get_DnsResolver • 0x2e67e:$a14: get_archivingScope • 0x2e4a6:$a15: get_providerName • 0x30bbc:$a17: get_priority • 0x30190:$a18: get_advancedParameters • 0x2f5a8:$a19: get_disabledByRestriction • 0x2e045:$a20: get_LastAccessed • 0x2e718:$a21: get_avatarType • 0x302a7:$a22: get_signaturePresets • 0x2ed4d:$a23: get_enableLog • 0x2e523:$a26: set_accountName • 0x306f2:$a27: set_InternalServerPort • 0x2d984:$a28: set_bindingConfigurationUID • 0x3026d:$a29: set_IdnAddress • 0x30a70:$a30: set_GuidMasterKey • 0x2e57e:$a31: set_username
0.2.Technical information zip.exe.44c9bb8.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 27 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2 - Source IP: 192.168.2.4 - Destination IP: 162.215.255.143

Timestamp:	192.168.2.4162.215.255.143497805872840032 08/08/22-17:23:56.548969
SID:	2840032
Source Port:	49780
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Win32/Agent Tesla SMTP Activity - Source IP: 192.168.2.4 - Destination IP: 162.215.255.143

Timestamp:	192.168.2.4162.215.255.143497805872839723 08/08/22-17:23:56.548892
SID:	2839723
Source Port:	49780
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.4 - Destination IP: 162.215.255.143

Timestamp:	192.168.2.4162.215.255.143497805872851779 08/08/22-17:23:56.548969
SID:	2851779
Source Port:	49780
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.4 - Destination IP: 162.215.255.143

Timestamp:	192.168.2.4162.215.255.143497805872030171 08/08/22-17:23:56.548892
SID:	2030171
Source Port:	49780
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

Networking

Snort IDS alert for network traffic

Yara detected Generic Downloader

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation

.NET source code contains potential unpacker

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 harvest and steal ftp login credentials

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

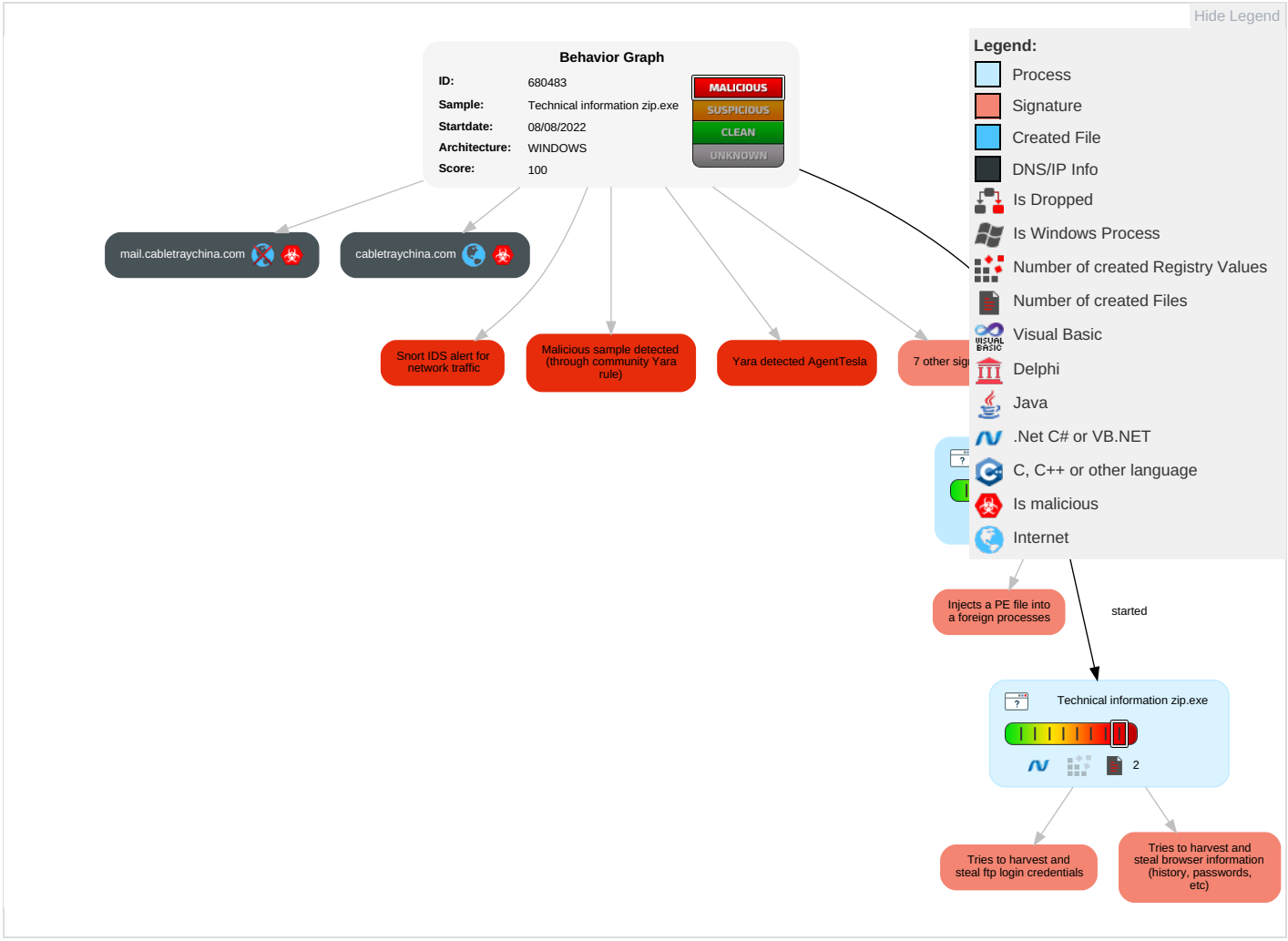
Remote Access Functionality

Yara detected AgentTesla

Mitre Att&ck Matrix

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

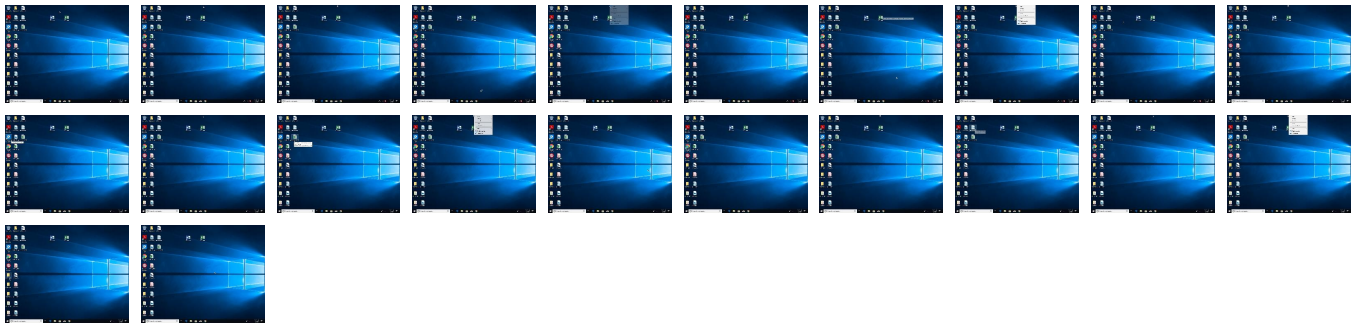
Behavior Graph



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
Technical information zip.exe	10%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.Technical information zip.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	

Source	Detection	Scanner	Label	Link
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	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://www.tiro.com	0%	URL Reputation	safe	
http://https://GQ0wtPGdRTxOSCfi6tDx.net	0%	Avira URL Cloud	safe	
http://cabletraychina.com	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	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://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://YXbeSX.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://boards.4chan.org3Retrieving	0%	Avira URL Cloud	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://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://mail.cabletraychina.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cabletraychina.com	162.215.255.143	true	true		unknown
mail.cabletraychina.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	Technical information zip.exe, 00000006.00000002.527868401.0000000003301000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	Technical information zip.exe, 00000000.00000002.309109555.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Technical information zip.exe, 00000000.00000002.309109555.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	Technical information zip.exe, 00000000.00000002.309109555.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://DynDns.comDynDNS	Technical information zip.exe, 00000006.00000002.527868401.0000000003301000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	Technical information zip.exe, 00000000.00000002.309109555.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Technical information zip.exe, 00000000.00000002.309109555.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	Technical information zip.exe, 00000006.00000002.527868401.0000000003301000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://boards.4chan.org/b/	Technical information zip.exe	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	Technical information zip.exe, 00000000.00000002.309109555.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	Technical information zip.exe, 00000000.00000002.309109555.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Technical information zip.exe, 00000000.00000002.309109555.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://GQ0wtPGdRTxOSCfi6tDx.net	Technical information zip.exe, 00000006.00000002.535012857.0000000003661000.00000004.00000800.00020000.00000000.sdmp, Technical information zip.exe, 00000006.00000002.534899990.000000000364F000.00000004.00000800.00020000.00000000.sdmp, Technical information zip.exe, 00000006.00000002.534929052.000000000365300.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://cabletraychina.com	Technical information zip.exe, 00000006.00000002.534958591.0000000003659000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	Technical information zip.exe, 00000000.00000002.309109555.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	Technical information zip.exe, 00000000.00000002.309109555.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	Technical information zip.exe, 00000000.00000002.309109555.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	Technical information zip.exe, 00000000.00000002.309109555.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Technical information zip.exe, 00000000.00000002.309109555.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Technical information zip.exe, 00000000.00000002.309109555.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Technical information zip.exe, 00000000.00000002.309109555.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Technical information zip.exe, 00000000.00000002.309109555.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Technical information zip.exe, 00000000.00000002.309109555.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	Technical information zip.exe, 00000000.00000002.309109555.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://YXbeSX.com	Technical information zip.exe, 00000006.00000002.527868401.0000000003301000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	Technical information zip.exe, 00000000.00000002.309109555.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Technical information zip.exe, 00000000.00000002.309109555.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Technical information zip.exe, 00000000.00000002.309109555.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://boards.4chan.org3Retrieving	Technical information zip.exe	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	Technical information zip.exe, 00000000.00000002.309109555.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Technical information zip.exe, 00000000.00000002.309109555.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://images.4chan.org/	Technical information zip.exe	false		high
http://www.urwpp.deDPlease	Technical information zip.exe, 00000000.00000002.309109555.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Technical information zip.exe, 00000000.00000002.309109555.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	Technical information zip.exe, 00000000.00000002.309109555.00000000073F2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Technical information zip.exe, 00000000.00000002.305256005.000000000445B000.00000004.00000800.00020000.00000000.sdmp, Technical information zip.exe, 00000006.00000000.293840755.0000000402000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://mail.cabletraychina.com	Technical information zip.exe, 00000006.00000002.534958591.0000000003659000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680483
Start date and time: 08/08/202217:20:35	2022-08-08 17:20:35 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Technical information zip.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:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/1@2/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 52.152.110.14, 20.54.89.106, 40.125.122.176, 20.223.24.244, 52.242.101.226
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, e12564.dspb.akamaiedge.net, rp-consumer-prod-displaycatalog-geomap.trafficmanager.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:21:59	API Interceptor	607x Sleep call for process: Technical information zip.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\Technical information zip.exe.log

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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.803329289885253
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Technical information zip.exe
File size:	1343488
MD5:	ca033c84f5a37105d613c6961b724e97
SHA1:	23f023abfef70de9ee2c909fbef985254b2abe26
SHA256:	bfcb8ee096a65d7ec9201b67df585a7e715aaaa0aa2dcfec2e6ff208b3559498
SHA512:	24efc400092f7fa258e68b2326ad9e075643aa007b7c2de0d50fa0379821e0ea797d2ed771687193e1bc0c3ebd486e59a627743d3094640af859f3e6e47383e2
SSDEEP:	24576:VmZs7cDzhEUKK1j2iU3AMYnC1e9IbUDHDl:Vm67c3xXfU3RYn07U
TLSH:	8A559E17AFA076C8F4B75BB9DC1F68D043F5EC09616AD2692E5078BA1FBA301D401E27
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....c.b.....0..... .....@.. .....@.....

File Icon

Icon Hash:	f0f0ccd6d4c4f0e8

Static PE Info

General

Entrypoint:	0x4edb02
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:	0x62F06317 [Mon Aug 8 01:12:55 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
mov bh, 1Dh
rol dword ptr [esi+ebp*2], 3Bh
or byte ptr [ecx], FFFFFFD9h
inc ebx
or eax, 130476DCh
imul ebp, dword ptr [ebx-3Bh], 17h
mov dl, 4Dh
xchg byte ptr [edx], bl
add eax, B81E4750h
in eax, dx

Instruction
or byte ptr [esi], ah

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xedab0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xf0000	0x5ab5c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x14c000	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	0xece80	0xed000	False	0.747269127439346	data	7.613311750792489	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xf0000	0x5ab5c	0x5ac00	False	0.0600330363292011	data	2.6135874634094827	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x14c000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xf0208	0x42028	data		
RT_ICON	0x132230	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x132698	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x134c40	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x135ce8	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x146510	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0x14a738	0x5a	data		
RT_GROUP_ICON	0x14a794	0x3e	data		
RT_VERSION	0x14a7d4	0x388	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4162.215.255.143497805872840032 08/08/22-17:23:56.548969	TCP	2840032	ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2	49780	587	192.168.2.4	162.215.255.143
192.168.2.4162.215.255.143497805872839723 08/08/22-17:23:56.548892	TCP	2839723	ETPRO TROJAN Win32/Agent Tesla SMTP Activity	49780	587	192.168.2.4	162.215.255.143
192.168.2.4162.215.255.143497805872851779 08/08/22-17:23:56.548969	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49780	587	192.168.2.4	162.215.255.143
192.168.2.4162.215.255.143497805872030171 08/08/22-17:23:56.548892	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49780	587	192.168.2.4	162.215.255.143

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 17:23:54.512552977 CEST	60647	53	192.168.2.4	8.8.8.8
Aug 8, 2022 17:23:54.689174891 CEST	53	60647	8.8.8.8	192.168.2.4
Aug 8, 2022 17:23:54.692245960 CEST	64909	53	192.168.2.4	8.8.8.8
Aug 8, 2022 17:23:54.860028028 CEST	53	64909	8.8.8.8	192.168.2.4

DNS Queries

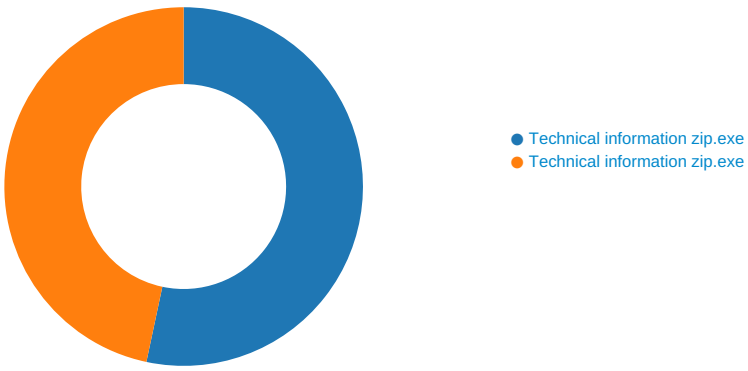
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 17:23:54.512552977 CEST	192.168.2.4	8.8.8.8	0xebe9	Standard query (0)	mail.cabletraychina.com	A (IP address)	IN (0x0001)
Aug 8, 2022 17:23:54.692245960 CEST	192.168.2.4	8.8.8.8	0x8e2a	Standard query (0)	mail.cabletraychina.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 17:23:54.689174891 CEST	8.8.8.8	192.168.2.4	0xebe9	No error (0)	mail.cabletraychina.com	cabletraychina.com		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 17:23:54.689174891 CEST	8.8.8.8	192.168.2.4	0xebe9	No error (0)	cabletraychina.com		162.215.255.143	A (IP address)	IN (0x0001)
Aug 8, 2022 17:23:54.860028028 CEST	8.8.8.8	192.168.2.4	0x8e2a	No error (0)	mail.cabletraychina.com	cabletraychina.com		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 17:23:54.860028028 CEST	8.8.8.8	192.168.2.4	0x8e2a	No error (0)	cabletraychina.com		162.215.255.143	A (IP address)	IN (0x0001)

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Technical information zip.exe PID: **4828**, Parent PID: **3908**

General

Target ID:	0
Start time:	17:21:46
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\Technical information zip.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Technical information zip.exe"
Imagebase:	0xee0000
File size:	1343488 bytes
MD5 hash:	CA033C84F5A37105D613C6961B724E97
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.305256005.000000000445B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.305256005.000000000445B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.305256005.000000000445B000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.304226940.0000000003620000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.299934426.00000000033AB000.00000004.00000800.00020000.00000000.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	6CF2CF06	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	6CF2CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Technical information zip.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D23C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Technical information zip.exe.log	0	1308	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D23C907	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	6CF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CF05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CE603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CF0CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CE603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CE603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CE603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CE603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BD71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BD71B4F	ReadFile

Analysis Process: Technical information zip.exe PID: **6128**, Parent PID: **4828**

General

Target ID:	6
Start time:	17:22:05
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\Technical information zip.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Technical information zip.exe
Imagebase:	0xed0000
File size:	1343488 bytes
MD5 hash:	CA033C84F5A37105D613C6961B724E97
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: 00000006.00000000.293840755.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000000.293840755.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000006.00000000.293840755.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.527868401.0000000003301000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.527868401.0000000003301000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 00000006.00000002.527868401.0000000003301000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CF2CF06	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	6CF2CF06	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	6CF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CF05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CE603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CF0CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CE603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CE603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CE603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CE603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CF05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BD71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BD71B4F	ReadFile

Disassembly

No disassembly