ID: 404252
Sample Name: ashleyx.exe
Cookbook: default.jbs
Time: 20:49:34
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

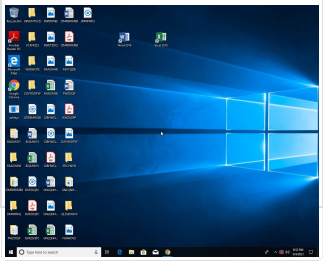
Analysis Report ashleyx.exe

Overview

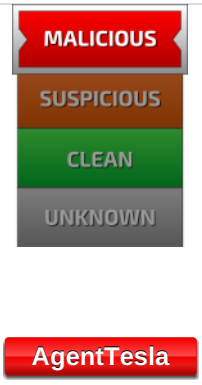
General Information

Sample Name:	ashleyx.exe
Analysis ID:	404252
MD5:	34d4452c1b3446..
SHA1:	bb42e71329d2ad..
SHA256:	65e210b78d7314..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection



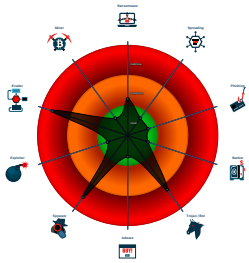
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**
- ashleyx.exe (PID: 7048 cmdline: 'C:\Users\user\Desktop\ashleyx.exe' MD5: 34D4452C1B344685E3F5FD7D0E9640A1)
  - ashleyx.exe (PID: 2204 cmdline: {path} MD5: 34D4452C1B344685E3F5FD7D0E9640A1)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "logs@phuboatrading-vn.comof2ZCW1li4ipTfyEsmtp.phuboatrading-vn.commylogs@phuboatrading-vn.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.911793295.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.683944483.0000000004D15000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.913258103.000000000325 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.913258103.000000000325 1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.680319941.00000000040C9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 4 entries

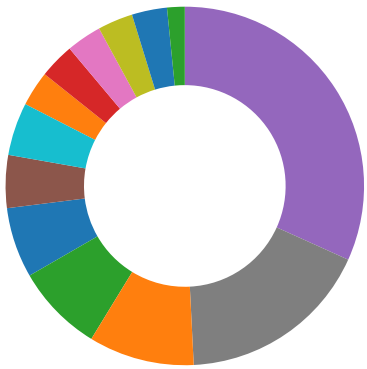
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.ashleyx.exe.4d757b8.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.ashleyx.exe.4d15598.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.ashleyx.exe.43c7e50.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.ashleyx.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.ashleyx.exe.4d757b8.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

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)

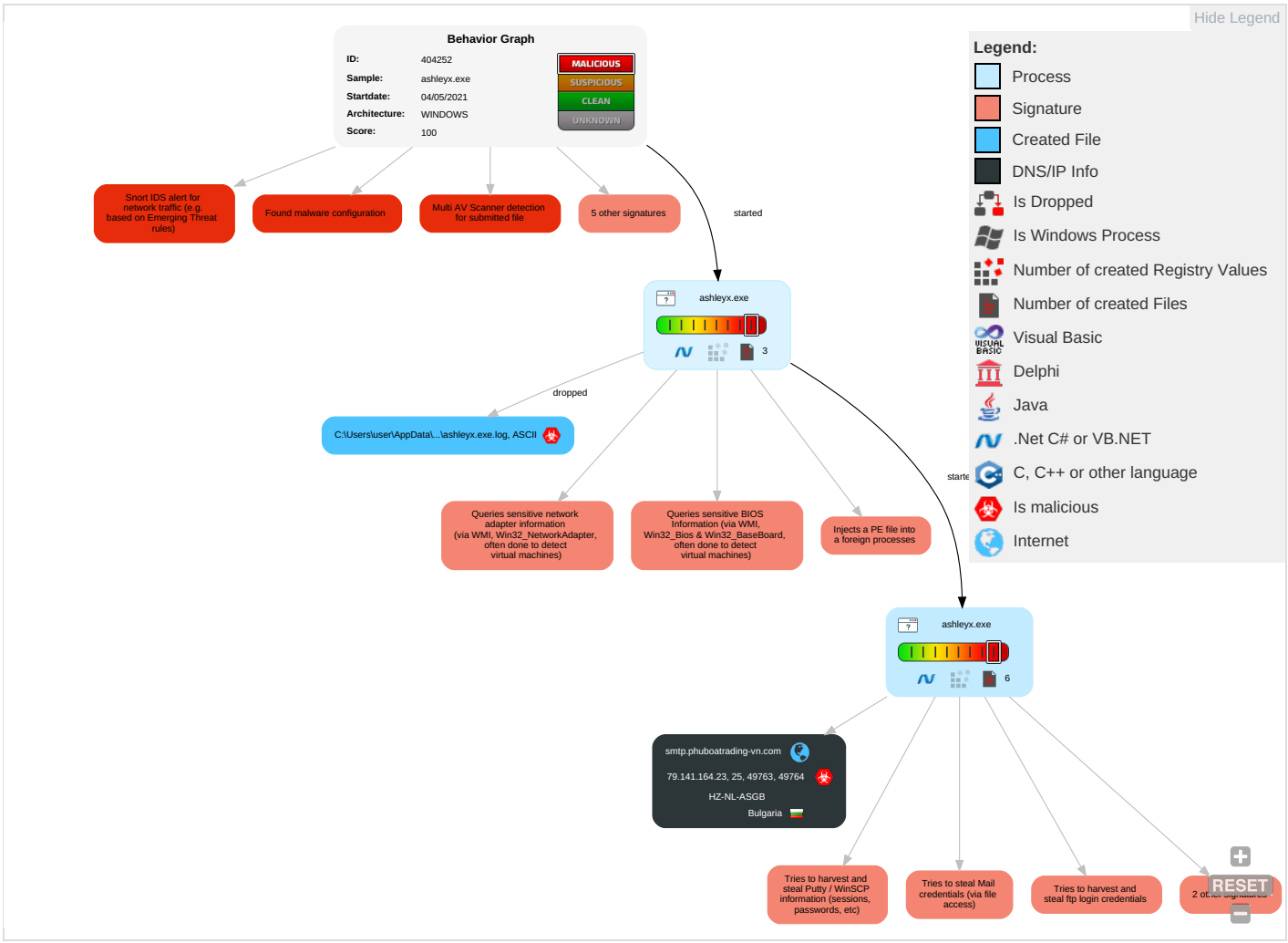
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

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

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
ashleyx.exe	30%	Virustotal		Browse
ashleyx.exe	40%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
ashleyx.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/DK	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnN	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://fl3gHqcqlp4Nk7qizX.net	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://www.jiyu-kobo.co.jp/a-d	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/a-d	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/a-d	0%	URL Reputation	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.carterandcone.com3	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.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/8	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/-cz	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-cz	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-cz	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.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.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.founder.com.cn/cnp	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/8	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/8	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/8	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0YK	0%	Avira URL Cloud	safe	
http://www.fontbureau.comocK	0%	Avira URL Cloud	safe	
http://www.urwpp.de.gd	0%	Avira URL Cloud	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.carterandcone.comC	0%	URL Reputation	safe	
http://www.carterandcone.comC	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.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/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	

Source	Detection	Scanner	Label	Link
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.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.carterandcone.comS	0%	Avira URL Cloud	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	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://www.founder.com.cn/cnd	0%	URL Reputation	safe	
http://www.founder.com.cn/cnd	0%	URL Reputation	safe	
http://www.founder.com.cn/cnd	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/nt	0%	Avira URL Cloud	safe	
http://www.tiro.coms	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtp.phuboatrading-vn.com	79.141.164.23	true	true		unknown

URLs from Memory and Binaries

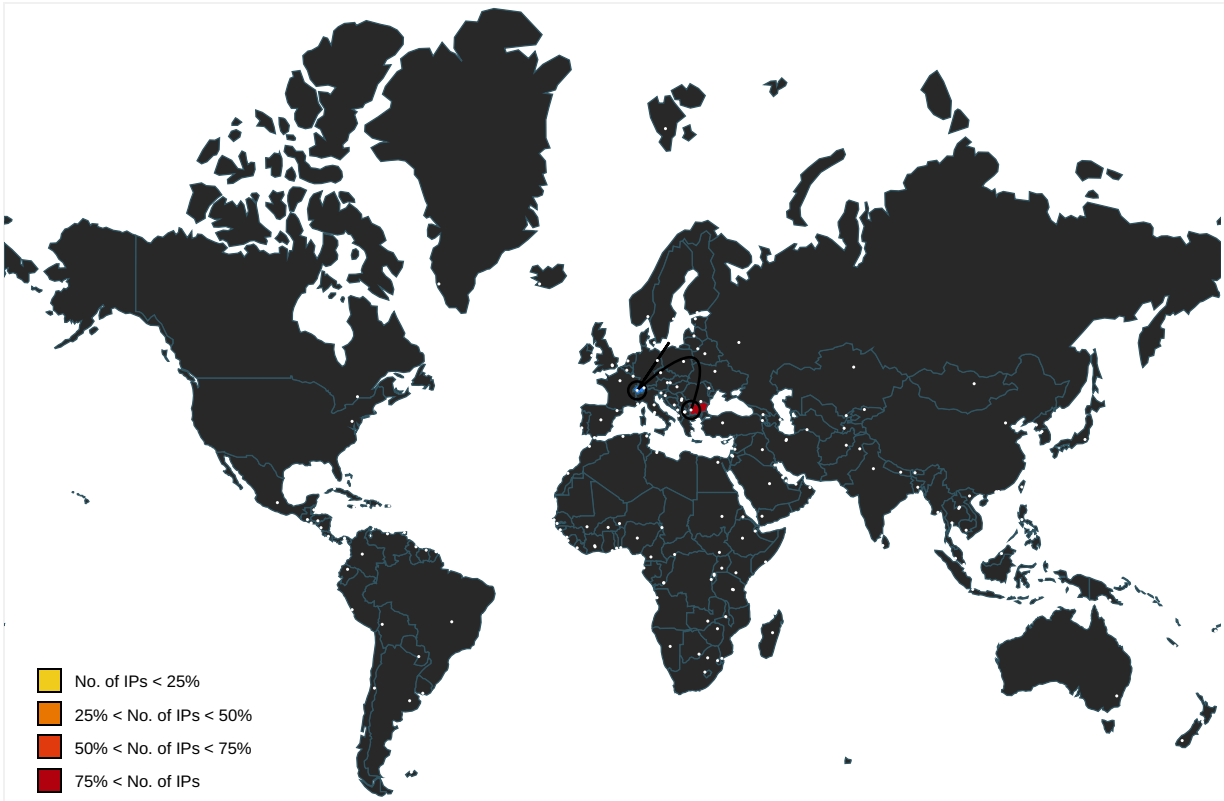
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/DK	ashleyx.exe, 00000000.00000003.651812477.0000000006095000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnN	ashleyx.exe, 00000000.00000003.651004266.00000000060BE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	ashleyx.exe, 00000004.00000002.913258103.0000000003251000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	ashleyx.exe, 00000000.00000002.685132707.0000000006180000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://fl3gHqcqlp4Nk7qizX.net	ashleyx.exe, 00000004.00000002.913258103.0000000003251000.00000004.00000001.sdmp, ashleyx.exe, 00000004.00000002.913746975.00000000035CC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	ashleyx.exe, 00000000.00000002.685132707.0000000006180000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	ashleyx.exe, 00000000.00000002.685132707.0000000006180000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	ashleyx.exe, 00000000.00000002.685132707.0000000006180000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/a-d	ashleyx.exe, 00000000.00000003.651812477.0000000006095000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.com	ashleyx.exe, 00000000.00000002.685132707.0000000006180000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	ashleyx.exe, 00000000.00000002.685132707.0000000006180000.00000002.00000001.sdmp, ashleyx.exe, 00000000.00000003.655202893.00000000060C0000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersivf	ashleyx.exe, 00000000.00000003.661342053.00000000060C0000.00000004.00000001.sdmp	false		high
http://www.carterandcone.com3	ashleyx.exe, 00000000.00000003.651354790.00000000060BF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	ashleyx.exe, 00000000.00000002.685132707.0000000006180000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	ashleyx.exe, 00000000.00000003.651354790.00000000060BF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/8	ashleyx.exe, 00000000.00000003.652217428.0000000006098000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/-cz	ashleyx.exe, 00000000.00000003.651812477.0000000006095000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	ashleyx.exe, 00000000.00000002.685132707.0000000006180000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	ashleyx.exe, 00000000.00000002.685132707.0000000006180000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	ashleyx.exe, 00000000.00000002.685132707.0000000006180000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	ashleyx.exe, 00000000.00000002.685132707.0000000006180000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	ashleyx.exe, 00000000.00000002.685132707.0000000006180000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersf	ashleyx.exe, 00000000.00000003.653569256.00000000060BF000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comgrita	ashleyx.exe, 00000000.00000002.685099190.0000000006090000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnp	ashleyx.exe, 00000000.00000003.651004266.00000000060BE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/8	ashleyx.exe, 00000000.00000003.651990337.000000000609B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0YK	ashleyx.exe, 00000000.00000003.651990337.000000000609B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comocK	ashleyx.exe, 00000000.00000002.685099190.0000000006090000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.de.gd	ashleyx.exe, 00000000.00000003.655452602.00000000060C0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersk	ashleyx.exe, 00000000.00000003.655147245.00000000060C0000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comC	ashleyx.exe, 00000000.00000003.651354790.00000000060BF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp//	ashleyx.exe, 00000000.00000003.651812477.0000000006095000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/-	ashleyx.exe, 00000000.00000003.652217428.0000000006098000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersb	ashleyx.exe, 00000000.00000003.655202893.00000000060C0000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	ashleyx.exe, 00000000.00000002.685132707.0000000006180000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	ashleyx.exe, 00000000.00000003.651812477.0000000006095000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	ashleyx.exe, 00000004.00000002.913258103.0000000003251000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.ascendercorp.com/typedesigners.html	ashleyx.exe, 00000000.00000003.652269015.00000000060BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	ashleyx.exe, 00000000.00000002.685132707.0000000006180000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	ashleyx.exe, 00000000.00000002.685132707.0000000006180000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	ashleyx.exe, 00000000.00000002.685132707.0000000006180000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comS	ashleyx.exe, 00000000.00000003.651354790.00000000060BF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.de	ashleyx.exe, 00000000.00000003.653067561.00000000060BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	ashleyx.exe, 00000000.00000002.685132707.0000000006180000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	ashleyx.exe, 00000000.00000002.685132707.0000000006180000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	ashleyx.exe, 00000000.00000002.683944483.0000000004D15000.00000004.00000001.sdmp, ashleyx.exe, 00000004.00000002.911793295.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designerst	ashleyx.exe, 00000000.00000003.653448509.00000000060BF000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnd	ashleyx.exe, 00000000.00000003.651004266.00000000060BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	ashleyx.exe, 00000000.00000002.685132707.0000000006180000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	ashleyx.exe, 00000000.00000002.685132707.0000000006180000.00000002.00000001.sdmp	false		high
http://DynDns.comDynDNS	ashleyx.exe, 00000004.00000002.913258103.0000000003251000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/nt	ashleyx.exe, 00000000.00000003.651812477.0000000006095000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.coms	ashleyx.exe, 00000000.00000003.651493647.00000000060C0000.00000004.00000001.sdmp	false	• Avira URL Cloud: 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%tordir%%ha	ashleyx.exe, 00000004.00000002.913258103.0000000003251000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fl3gHqcqlp4Nk7qizX.net853321935-2125563209-4053062332-1002_Classes	ashleyx.exe, 00000004.00000003.884379101.0000000001494000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/jp/	ashleyx.exe, 00000000.00000003.652217428.0000000006098000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0Al	ashleyx.exe, 00000000.00000003.652217428.0000000006098000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comn	ashleyx.exe, 00000000.00000003.651354790.00000000060BF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htmu	ashleyx.exe, 00000000.00000003.656978899.00000000060C0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%$	ashleyx.exe, 00000004.00000002.913258103.0000000003251000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.coml	ashleyx.exe, 00000000.00000002.685132707.0000000006180000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	ashleyx.exe, 00000000.00000002.685132707.0000000006180000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers&	ashleyx.exe, 00000000.00000003.653202861.00000000060BE000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn	ashleyx.exe, 00000000.00000003.651004266.00000000060BE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://smtp.phuboatrading-vn.com	ashleyx.exe, 00000004.00000002.913712228.00000000035BF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comIta	ashleyx.exe, 00000000.00000003.651354790.00000000060BF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	ashleyx.exe, 00000000.00000002.685132707.0000000006180000.00000002.00000001.sdmp, ashleyx.exe, 00000000.00000003.653796968.00000000060BF000.00000004.00000001.sdmp, ashleyx.exe, 00000000.00000003.653743073.00000000060BF000.00000004.00000001.sdmp	false		high
http://wcmZQs.com	ashleyx.exe, 00000004.00000002.913258103.0000000003251000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	ashleyx.exe, 00000000.00000003.654413827.00000000060C0000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	ashleyx.exe, 00000000.00000002.685132707.0000000006180000.00000002.00000001.sdmp, ashleyx.exe, 00000000.00000003.651990337.000000000609B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers0._	ashleyx.exe, 00000000.00000003.654739623.00000000060C0000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers8	ashleyx.exe, 00000000.00000002.685132707.0000000006180000.00000002.00000001.sdmp, ashleyx.exe, 00000000.00000003.653796968.00000000060BF000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/VK	ashleyx.exe, 00000000.00000003.651812477.0000000006095000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comic	ashleyx.exe, 00000000.00000003.651493647.00000000060C0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/	ashleyx.exe, 00000000.00000003.653135407.00000000060BE000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.141.164.23	smtp.phuboatrading-vn.com	Bulgaria		59711	HZ-NL-ASGB	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404252
Start date:	04.05.2021
Start time:	20:49:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ashleyx.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@3/2@2/1
EGA Information:	Failed
HDC Information:	Failed
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 • Excluded IPs from analysis (whitelisted): 104.42.151.234, 184.87.213.153, 13.88.21.125, 104.43.139.144, 20.82.210.154, 92.122.213.247, 92.122.213.194, 2.20.142.209, 2.20.142.210, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.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
20:50:33	API Interceptor	720x Sleep call for process: ashleyx.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.141.164.23	Purchase Inquiry 040521.exe	Get hash	malicious	Browse	
	PO_001412.doc	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
smtp.phuboatrading-vn.com	PO_001412.doc	Get hash	malicious	Browse	• 79.141.164.23

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HZ-NL-ASGB	Purchase Inquiry 040521.exe	Get hash	malicious	Browse	• 79.141.164.23
	PO_001412.doc	Get hash	malicious	Browse	• 79.141.164.23
	DgWRWQ2oYs.exe	Get hash	malicious	Browse	• 5.149.255.204
	Sirus.exe	Get hash	malicious	Browse	• 5.149.255.204
	tskhoni.exe	Get hash	malicious	Browse	• 185.81.115.14
	6IGbftBsBg.exe	Get hash	malicious	Browse	• 5.149.255.204
	ikoAImKWvI.exe	Get hash	malicious	Browse	• 5.149.255.204
	yPkfbflyoh.exe	Get hash	malicious	Browse	• 5.149.255.204
	SecuriteInfo.com.Heur.24862.exe	Get hash	malicious	Browse	• 185.81.114.183
	JYDy1dAHdW.exe	Get hash	malicious	Browse	• 5.149.255.204
	EppTbowa74.exe	Get hash	malicious	Browse	• 5.149.255.204
	5rmW4DWq66.exe	Get hash	malicious	Browse	• 5.149.255.204
	886t3PbVKb.apk	Get hash	malicious	Browse	• 5.149.249.226
	PO_07712.doc	Get hash	malicious	Browse	• 79.141.165.38
	IMG_00671.doc	Get hash	malicious	Browse	• 79.141.165.38
	Purchase Order.doc	Get hash	malicious	Browse	• 79.141.165.38
	sample new order.doc	Get hash	malicious	Browse	• 79.141.165.38
	IMG_144907.doc	Get hash	malicious	Browse	• 79.141.165.38
	IMG_497927.doc	Get hash	malicious	Browse	• 79.141.165.38
	9oUx9PzdSA.exe	Get hash	malicious	Browse	• 79.141.164.163

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\ashleyx.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Roaming\tmpjcm5c.fha\Chrome\Default\Cookies

Process:	C:\Users\user\Desktop\ashleyx.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785

C:\Users\user\AppData\Roaming\tmpjcm5c.fha\Chrome\Default\Cookies	
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):	7.27303210920636
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	ashleyx.exe
File size:	1000960
MD5:	34d4452c1b344685e3f5fd7d0e9640a1
SHA1:	bb42e71329d2ad4baff54600020eb7053cc53026
SHA256:	65e210b78d73141c61b7087dce60499ca6c225e1b028d3951589c93baa8f0668
SHA512:	516b564b12a80d67cd4437af8ca86acd65b3ad8536786da3e6851cbbf8ffad33f47ca1f0c9dcd8e83002d4c1dc6d387aa6dc5759be04da782e8d1e99b0b1fde9
SSDEEP:	12288:MrloLLoS60/K7yh07qG3wBrCFfzTmjDjZLSMRoRf/mq4C6K+mgEie4Qi/lbm+OFO:qoLA75wppvZy39uKhgEiQiga+OF
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...O.X.....0..<.....Z... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4f5aae
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:	0x9C58D04F [Thu Feb 13 13:29:51 2053 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4

General

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xf5a58	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xf6000	0x5c0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xf8000	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	0xf3ab4	0xf3c00	False	0.648625801282	data	7.27698416733	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xf6000	0x5c0	0x600	False	0.426432291667	data	4.14428356853	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xf8000	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_VERSION	0xf60a0	0x334	data		
RT_MANIFEST	0xf63d4	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
Assembly Version	1.0.0.0
InternalName	RZVF0aMBAABaAKZ.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Interface
ProductVersion	1.0.0.0
FileDescription	Interface
OriginalFilename	RZVF0aMBAABaAKZ.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-20:52:19.790611	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49763	25	192.168.2.4	79.141.164.23
05/04/21-20:52:22.215980	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49764	25	192.168.2.4	79.141.164.23

Network Port Distribution

Total Packets: 71

- 53 (DNS)
- 25 (SMTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:52:19.288433075 CEST	49763	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:19.338658094 CEST	25	49763	79.141.164.23	192.168.2.4
May 4, 2021 20:52:19.338845968 CEST	49763	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:19.471122026 CEST	25	49763	79.141.164.23	192.168.2.4
May 4, 2021 20:52:19.471648932 CEST	49763	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:19.522794962 CEST	25	49763	79.141.164.23	192.168.2.4
May 4, 2021 20:52:19.522828102 CEST	25	49763	79.141.164.23	192.168.2.4
May 4, 2021 20:52:19.524703979 CEST	49763	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:19.577527046 CEST	25	49763	79.141.164.23	192.168.2.4
May 4, 2021 20:52:19.578166962 CEST	49763	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:19.629369974 CEST	25	49763	79.141.164.23	192.168.2.4
May 4, 2021 20:52:19.630331039 CEST	49763	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:19.683577061 CEST	25	49763	79.141.164.23	192.168.2.4
May 4, 2021 20:52:19.684187889 CEST	49763	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:19.737844944 CEST	25	49763	79.141.164.23	192.168.2.4
May 4, 2021 20:52:19.738210917 CEST	49763	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:19.788660049 CEST	25	49763	79.141.164.23	192.168.2.4
May 4, 2021 20:52:19.790611029 CEST	49763	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:19.790805101 CEST	49763	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:19.791933060 CEST	49763	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:19.792140961 CEST	49763	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:19.842776060 CEST	25	49763	79.141.164.23	192.168.2.4
May 4, 2021 20:52:19.844707966 CEST	25	49763	79.141.164.23	192.168.2.4
May 4, 2021 20:52:19.849090099 CEST	25	49763	79.141.164.23	192.168.2.4
May 4, 2021 20:52:19.889420033 CEST	49763	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:21.306401014 CEST	49763	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:21.356863022 CEST	25	49763	79.141.164.23	192.168.2.4
May 4, 2021 20:52:21.356889963 CEST	25	49763	79.141.164.23	192.168.2.4
May 4, 2021 20:52:21.357558012 CEST	49763	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:21.357758999 CEST	49763	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:21.407876015 CEST	25	49763	79.141.164.23	192.168.2.4
May 4, 2021 20:52:21.776424885 CEST	49764	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:21.826559067 CEST	25	49764	79.141.164.23	192.168.2.4
May 4, 2021 20:52:21.826730967 CEST	49764	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:21.899658918 CEST	25	49764	79.141.164.23	192.168.2.4
May 4, 2021 20:52:21.900046110 CEST	49764	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:21.950335979 CEST	25	49764	79.141.164.23	192.168.2.4
May 4, 2021 20:52:21.950547934 CEST	25	49764	79.141.164.23	192.168.2.4
May 4, 2021 20:52:21.950968027 CEST	49764	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:22.002002001 CEST	25	49764	79.141.164.23	192.168.2.4
May 4, 2021 20:52:22.002566099 CEST	49764	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:22.053567886 CEST	25	49764	79.141.164.23	192.168.2.4
May 4, 2021 20:52:22.056337118 CEST	49764	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:22.107652903 CEST	25	49764	79.141.164.23	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:52:22.108443022 CEST	49764	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:22.163306952 CEST	25	49764	79.141.164.23	192.168.2.4
May 4, 2021 20:52:22.163737059 CEST	49764	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:22.213977098 CEST	25	49764	79.141.164.23	192.168.2.4
May 4, 2021 20:52:22.215795040 CEST	49764	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:22.215980053 CEST	49764	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:22.216200113 CEST	49764	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:22.216372967 CEST	49764	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:22.216578960 CEST	49764	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:22.216739893 CEST	49764	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:22.216830015 CEST	49764	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:22.216959000 CEST	49764	25	192.168.2.4	79.141.164.23
May 4, 2021 20:52:22.266311884 CEST	25	49764	79.141.164.23	192.168.2.4
May 4, 2021 20:52:22.266505003 CEST	25	49764	79.141.164.23	192.168.2.4
May 4, 2021 20:52:22.266741991 CEST	25	49764	79.141.164.23	192.168.2.4
May 4, 2021 20:52:22.266904116 CEST	25	49764	79.141.164.23	192.168.2.4
May 4, 2021 20:52:22.270330906 CEST	25	49764	79.141.164.23	192.168.2.4
May 4, 2021 20:52:22.311584949 CEST	49764	25	192.168.2.4	79.141.164.23

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:50:15.009428024 CEST	49714	53	192.168.2.4	8.8.8.8
May 4, 2021 20:50:15.068043947 CEST	53	49714	8.8.8.8	192.168.2.4
May 4, 2021 20:50:16.546878099 CEST	58028	53	192.168.2.4	8.8.8.8
May 4, 2021 20:50:16.598330975 CEST	53	58028	8.8.8.8	192.168.2.4
May 4, 2021 20:50:17.661214113 CEST	53097	53	192.168.2.4	8.8.8.8
May 4, 2021 20:50:17.710062027 CEST	53	53097	8.8.8.8	192.168.2.4
May 4, 2021 20:50:17.882200956 CEST	49257	53	192.168.2.4	8.8.8.8
May 4, 2021 20:50:17.940947056 CEST	53	49257	8.8.8.8	192.168.2.4
May 4, 2021 20:50:19.328146935 CEST	62389	53	192.168.2.4	8.8.8.8
May 4, 2021 20:50:19.376792908 CEST	53	62389	8.8.8.8	192.168.2.4
May 4, 2021 20:50:20.544532061 CEST	49910	53	192.168.2.4	8.8.8.8
May 4, 2021 20:50:20.597779989 CEST	53	49910	8.8.8.8	192.168.2.4
May 4, 2021 20:50:21.797899008 CEST	55854	53	192.168.2.4	8.8.8.8
May 4, 2021 20:50:21.851433992 CEST	53	55854	8.8.8.8	192.168.2.4
May 4, 2021 20:50:23.599337101 CEST	64549	53	192.168.2.4	8.8.8.8
May 4, 2021 20:50:23.648137093 CEST	53	64549	8.8.8.8	192.168.2.4
May 4, 2021 20:50:24.804491997 CEST	63153	53	192.168.2.4	8.8.8.8
May 4, 2021 20:50:24.853121042 CEST	53	63153	8.8.8.8	192.168.2.4
May 4, 2021 20:50:26.100614071 CEST	52991	53	192.168.2.4	8.8.8.8
May 4, 2021 20:50:26.152251005 CEST	53	52991	8.8.8.8	192.168.2.4
May 4, 2021 20:50:27.316915035 CEST	53700	53	192.168.2.4	8.8.8.8
May 4, 2021 20:50:27.365577936 CEST	53	53700	8.8.8.8	192.168.2.4
May 4, 2021 20:50:28.476697922 CEST	51726	53	192.168.2.4	8.8.8.8
May 4, 2021 20:50:28.529735088 CEST	53	51726	8.8.8.8	192.168.2.4
May 4, 2021 20:50:29.604787111 CEST	56794	53	192.168.2.4	8.8.8.8
May 4, 2021 20:50:29.653872013 CEST	53	56794	8.8.8.8	192.168.2.4
May 4, 2021 20:50:30.989475965 CEST	56534	53	192.168.2.4	8.8.8.8
May 4, 2021 20:50:31.039660931 CEST	53	56534	8.8.8.8	192.168.2.4
May 4, 2021 20:50:32.685702085 CEST	56627	53	192.168.2.4	8.8.8.8
May 4, 2021 20:50:32.739552021 CEST	53	56627	8.8.8.8	192.168.2.4
May 4, 2021 20:50:33.894110918 CEST	56621	53	192.168.2.4	8.8.8.8
May 4, 2021 20:50:33.942657948 CEST	53	56621	8.8.8.8	192.168.2.4
May 4, 2021 20:50:35.082353115 CEST	63116	53	192.168.2.4	8.8.8.8
May 4, 2021 20:50:35.133270979 CEST	53	63116	8.8.8.8	192.168.2.4
May 4, 2021 20:50:36.161096096 CEST	64078	53	192.168.2.4	8.8.8.8
May 4, 2021 20:50:36.220890999 CEST	53	64078	8.8.8.8	192.168.2.4
May 4, 2021 20:50:38.801924944 CEST	64801	53	192.168.2.4	8.8.8.8
May 4, 2021 20:50:38.851711035 CEST	53	64801	8.8.8.8	192.168.2.4
May 4, 2021 20:50:48.271702051 CEST	61721	53	192.168.2.4	8.8.8.8
May 4, 2021 20:50:48.320451021 CEST	53	61721	8.8.8.8	192.168.2.4
May 4, 2021 20:50:52.639288902 CEST	51255	53	192.168.2.4	8.8.8.8
May 4, 2021 20:50:52.701081038 CEST	53	51255	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:51:09.072490931 CEST	61522	53	192.168.2.4	8.8.8.8
May 4, 2021 20:51:09.134953976 CEST	53	61522	8.8.8.8	192.168.2.4
May 4, 2021 20:51:09.481513977 CEST	52337	53	192.168.2.4	8.8.8.8
May 4, 2021 20:51:09.609930992 CEST	53	52337	8.8.8.8	192.168.2.4
May 4, 2021 20:51:10.272124052 CEST	55046	53	192.168.2.4	8.8.8.8
May 4, 2021 20:51:10.558665991 CEST	53	55046	8.8.8.8	192.168.2.4
May 4, 2021 20:51:11.211080074 CEST	49612	53	192.168.2.4	8.8.8.8
May 4, 2021 20:51:11.346826077 CEST	53	49612	8.8.8.8	192.168.2.4
May 4, 2021 20:51:11.583136082 CEST	49285	53	192.168.2.4	8.8.8.8
May 4, 2021 20:51:11.658024073 CEST	53	49285	8.8.8.8	192.168.2.4
May 4, 2021 20:51:11.788130045 CEST	50601	53	192.168.2.4	8.8.8.8
May 4, 2021 20:51:12.046248913 CEST	53	50601	8.8.8.8	192.168.2.4
May 4, 2021 20:51:12.632498980 CEST	60875	53	192.168.2.4	8.8.8.8
May 4, 2021 20:51:12.692610025 CEST	53	60875	8.8.8.8	192.168.2.4
May 4, 2021 20:51:13.356338024 CEST	56448	53	192.168.2.4	8.8.8.8
May 4, 2021 20:51:13.413548946 CEST	53	56448	8.8.8.8	192.168.2.4
May 4, 2021 20:51:14.240776062 CEST	59172	53	192.168.2.4	8.8.8.8
May 4, 2021 20:51:14.297679901 CEST	53	59172	8.8.8.8	192.168.2.4
May 4, 2021 20:51:16.911333084 CEST	62420	53	192.168.2.4	8.8.8.8
May 4, 2021 20:51:16.968554020 CEST	53	62420	8.8.8.8	192.168.2.4
May 4, 2021 20:51:18.042967081 CEST	60579	53	192.168.2.4	8.8.8.8
May 4, 2021 20:51:18.100119114 CEST	53	60579	8.8.8.8	192.168.2.4
May 4, 2021 20:51:19.161361933 CEST	50183	53	192.168.2.4	8.8.8.8
May 4, 2021 20:51:19.221544981 CEST	53	50183	8.8.8.8	192.168.2.4
May 4, 2021 20:51:25.160984039 CEST	61531	53	192.168.2.4	8.8.8.8
May 4, 2021 20:51:25.220212936 CEST	53	61531	8.8.8.8	192.168.2.4
May 4, 2021 20:51:57.859030008 CEST	49228	53	192.168.2.4	8.8.8.8
May 4, 2021 20:51:57.907628059 CEST	53	49228	8.8.8.8	192.168.2.4
May 4, 2021 20:51:59.716505051 CEST	59794	53	192.168.2.4	8.8.8.8
May 4, 2021 20:51:59.774081945 CEST	53	59794	8.8.8.8	192.168.2.4
May 4, 2021 20:52:19.106405020 CEST	55916	53	192.168.2.4	8.8.8.8
May 4, 2021 20:52:19.160440922 CEST	53	55916	8.8.8.8	192.168.2.4
May 4, 2021 20:52:21.710552931 CEST	52752	53	192.168.2.4	8.8.8.8
May 4, 2021 20:52:21.774441004 CEST	53	52752	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 20:52:19.106405020 CEST	192.168.2.4	8.8.8.8	0xdf8f	Standard query (0)	smtp.phubo atrading-vn.com	A (IP address)	IN (0x0001)
May 4, 2021 20:52:21.710552931 CEST	192.168.2.4	8.8.8.8	0x6486	Standard query (0)	smtp.phubo atrading-vn.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 20:52:19.160440922 CEST	8.8.8.8	192.168.2.4	0xdf8f	No error (0)	smtp.phubo atrading-vn.com		79.141.164.23	A (IP address)	IN (0x0001)
May 4, 2021 20:52:21.774441004 CEST	8.8.8.8	192.168.2.4	0x6486	No error (0)	smtp.phubo atrading-vn.com		79.141.164.23	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 4, 2021 20:52:19.471122026 CEST	25	49763	79.141.164.23	192.168.2.4	220 smtp.phuboatrading-vn.com ESMTP
May 4, 2021 20:52:19.471648932 CEST	49763	25	192.168.2.4	79.141.164.23	EHLO 305090
May 4, 2021 20:52:19.522828102 CEST	25	49763	79.141.164.23	192.168.2.4	250-smtp.phuboatrading-vn.com 250-PIPELINING 250-SIZE 20480000 250-ETRN 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
May 4, 2021 20:52:19.524703979 CEST	49763	25	192.168.2.4	79.141.164.23	AUTH login bG9nc0BwaHVib2F0cmFkaW5nLXZuLmNvbQ==

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 4, 2021 20:52:19.577527046 CEST	25	49763	79.141.164.23	192.168.2.4	334 UGFzc3dvcmQ6
May 4, 2021 20:52:19.629369974 CEST	25	49763	79.141.164.23	192.168.2.4	235 2.7.0 Authentication successful
May 4, 2021 20:52:19.630331039 CEST	49763	25	192.168.2.4	79.141.164.23	MAIL FROM:<logs@phuboatrading-vn.com>
May 4, 2021 20:52:19.683577061 CEST	25	49763	79.141.164.23	192.168.2.4	250 2.1.0 Ok
May 4, 2021 20:52:19.684187889 CEST	49763	25	192.168.2.4	79.141.164.23	RCPT TO:<mylogs@phuboatrading-vn.com>
May 4, 2021 20:52:19.737844944 CEST	25	49763	79.141.164.23	192.168.2.4	250 2.1.5 Ok
May 4, 2021 20:52:19.738210917 CEST	49763	25	192.168.2.4	79.141.164.23	DATA
May 4, 2021 20:52:19.788660049 CEST	25	49763	79.141.164.23	192.168.2.4	354 End data with <CR><LF>.<CR><LF>
May 4, 2021 20:52:19.792140961 CEST	49763	25	192.168.2.4	79.141.164.23	.
May 4, 2021 20:52:19.849090099 CEST	25	49763	79.141.164.23	192.168.2.4	250 2.0.0 Ok: queued as B04A9429A0
May 4, 2021 20:52:21.306401014 CEST	49763	25	192.168.2.4	79.141.164.23	QUIT
May 4, 2021 20:52:21.356863022 CEST	25	49763	79.141.164.23	192.168.2.4	221 2.0.0 Bye
May 4, 2021 20:52:21.899658918 CEST	25	49764	79.141.164.23	192.168.2.4	220 smtp.phuboatrading-vn.com ESMTP
May 4, 2021 20:52:21.900046110 CEST	49764	25	192.168.2.4	79.141.164.23	EHLO 305090
May 4, 2021 20:52:21.950547934 CEST	25	49764	79.141.164.23	192.168.2.4	250-smtp.phuboatrading-vn.com 250-PIPELINING 250-SIZE 20480000 250-ETRN 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
May 4, 2021 20:52:21.950968027 CEST	49764	25	192.168.2.4	79.141.164.23	AUTH login bG9nc0BwaHVib2F0cmFkaW5nLXZuLmNvbQ==
May 4, 2021 20:52:22.002002001 CEST	25	49764	79.141.164.23	192.168.2.4	334 UGFzc3dvcmQ6
May 4, 2021 20:52:22.053567886 CEST	25	49764	79.141.164.23	192.168.2.4	235 2.7.0 Authentication successful
May 4, 2021 20:52:22.056337118 CEST	49764	25	192.168.2.4	79.141.164.23	MAIL FROM:<logs@phuboatrading-vn.com>
May 4, 2021 20:52:22.107652903 CEST	25	49764	79.141.164.23	192.168.2.4	250 2.1.0 Ok
May 4, 2021 20:52:22.108443022 CEST	49764	25	192.168.2.4	79.141.164.23	RCPT TO:<mylogs@phuboatrading-vn.com>
May 4, 2021 20:52:22.163306952 CEST	25	49764	79.141.164.23	192.168.2.4	250 2.1.5 Ok
May 4, 2021 20:52:22.163737059 CEST	49764	25	192.168.2.4	79.141.164.23	DATA
May 4, 2021 20:52:22.213977098 CEST	25	49764	79.141.164.23	192.168.2.4	354 End data with <CR><LF>.<CR><LF>
May 4, 2021 20:52:22.216959000 CEST	49764	25	192.168.2.4	79.141.164.23	.
May 4, 2021 20:52:22.270330906 CEST	25	49764	79.141.164.23	192.168.2.4	250 2.0.0 Ok: queued as 23E1F429A0

Code Manipulations

Statistics

Behavior

System Behavior

Analysis Process: ashleyx.exe PID: 7048 Parent PID: 5940

General

Start time:	20:50:22
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\ashleyx.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ashleyx.exe'
Imagebase:	0xd40000
File size:	1000960 bytes
MD5 hash:	34D4452C1B344685E3F5FD7D0E9640A1
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: 00000000.00000002.683944483.0000000004D15000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.680319941.00000000040C9000.00000004.00000001.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	6D19CF06	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	6D19CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ashleyx.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D4AC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ashleyx.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",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_v4.0.3	success or wait	1	6D4AC907	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	6D175705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D175705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D17CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D175705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D175705	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: ashleyx.exe PID: 2204 Parent PID: 7048

General

Start time:	20:50:34
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\ashleyx.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xec0000
File size:	1000960 bytes
MD5 hash:	34D4452C1B344685E3F5FD7D0E9640A1
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: 00000004.00000002.911793295.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.913258103.0000000003251000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.913258103.0000000003251000.00000004.00000001.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	6D19CF06	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	6D19CF06	unknown
C:\Users\user\AppData\Roaming\tmpjcm5c.fha	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\tmpjcm5c.fha\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	6BFEBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\tmpjcm5c.fha\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	6BFEBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\tmpjcm5c.fha\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	6BFEDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\tmpjcm5c.fha\Chrome\Default\Cookies	success or wait	1	6BFE6A95	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\ tmpjcm5c.fha\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6BFEDD66	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	6D175705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D175705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D17CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D175705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D175705	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\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:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6BFE1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6BFE1B4F	ReadFile
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	10960	success or wait	1	6BFE1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\c51a91d0-39d9-48ba-a63c-ca2a9e8a1bd3	unknown	4096	success or wait	1	6BFE1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6BFE1B4F	ReadFile
C:\Users\user\AppData\Roaming\tmpjcm5c.fha\Chrome\Default\Cookies	unknown	16384	success or wait	1	6BFE1B4F	ReadFile

Disassembly

Code Analysis

Code Analysis