ID: 404235
Sample Name: Sample Order.exe
Cookbook: default.jbs
Time: 20:29:26
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

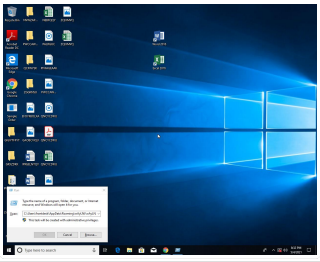
Analysis Report Sample Order.exe

Overview

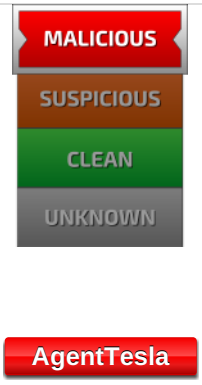
General Information

Sample Name:	Sample Order.exe
Analysis ID:	404235
MD5:	72d643819882ba..
SHA1:	edc461e732f56ca..
SHA256:	c590c197137574..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

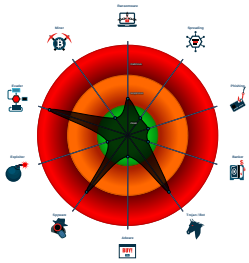


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected AgentTesla
- Yara detected AntiVM3
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- May check the online IP address of …
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…
- Tries to steal Mail credentials (via fil…
- Uses schtasks.exe or at.exe to add …

Classification



Startup

- **System is w10x64**
- Sample Order.exe (PID: 5488 cmdline: 'C:\Users\user\Desktop\Sample Order.exe' MD5: 72D643819882BAF6C48246024D4755D1)
  - schtasks.exe (PID: 5828 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\OnUeAYnP' /XML 'C:\Users\user\AppData\Local\Temp\tmp8100.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5784 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Sample Order.exe (PID: 4452 cmdline: {path} MD5: 72D643819882BAF6C48246024D4755D1)
- wAyLNJ.exe (PID: 6420 cmdline: 'C:\Users\user\AppData\Roaming\wAyLNJ\wAyLNJ.exe' MD5: 72D643819882BAF6C48246024D4755D1)
  - schtasks.exe (PID: 6616 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\OnUeAYnP' /XML 'C:\Users\user\AppData\Local\Temp\tmp3F4E.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6632 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - wAyLNJ.exe (PID: 6668 cmdline: {path} MD5: 72D643819882BAF6C48246024D4755D1)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "alvank6@earthlink.netsoLution16@smtpauth.earthlink.netspe1759@gmail.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000018.00000002.500770724.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Copyright Joe Security LLC 2021

Source	Rule	Description	Author	Strings
00000008.00000002.508711336.000000000315 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000002.508711336.000000000315 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
00000014.00000002.380533904.0000000003C5 F000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000008.00000002.500306866.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 11 entries				

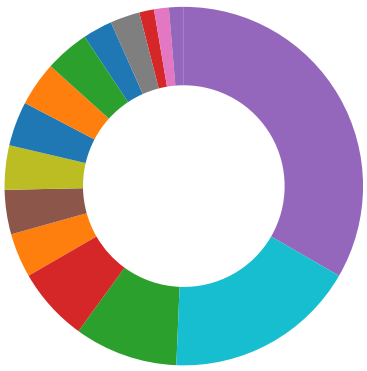
Unpacked PEs

Source	Rule	Description	Author	Strings
20.2.wAyLNJ.exe.3d01858.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
20.2.wAyLNJ.exe.3d01858.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Sample Order.exe.3ca1858.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
24.2.wAyLNJ.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Sample Order.exe.3ca1858.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 2 entries				

Sigma Overview

No Sigma rule has matched

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

Networking:

May check the online IP address of the machine

System Summary:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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 steal Mail credentials (via file access)

Remote Access Functionality:

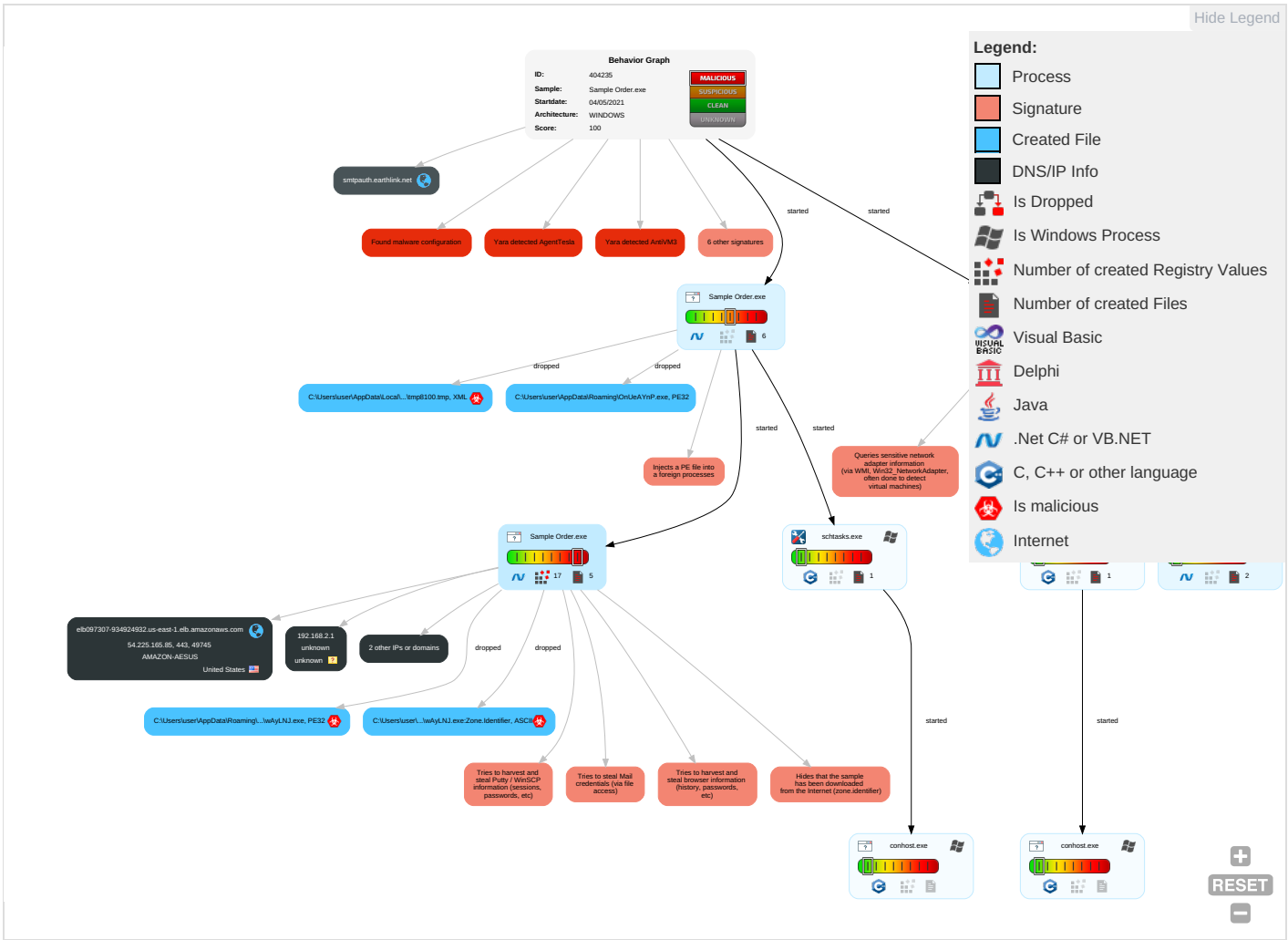
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 1	Account Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium
Default Accounts	Command and Scripting Interpreter 2	Registry Run Keys / Startup Folder 1	Scheduled Task/Job 1	Obfuscated Files or Information 2	Credentials in Registry 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Software Packing 2	Security Account Manager	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)	Timestomp 1	NTDS	Query Registry 1	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 2 2 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4 1	Cached Domain Credentials	Process Discovery 2	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	Virtualization/Sandbox Evasion 1 4 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	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
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	System Network Configuration Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium

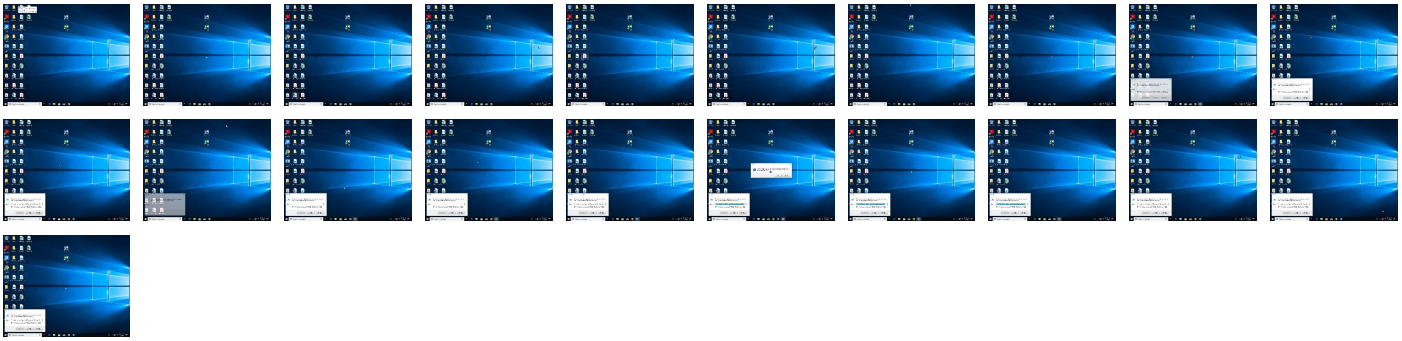
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

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

Source	Detection	Scanner	Label	Link	Download
8.2.Sample Order.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	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.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	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://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://DVEXLL.com	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.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.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	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.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/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
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.fontbureau.comf37x	0%	Avira URL Cloud	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.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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
elb097307-934924932.us-east-1.elb.amazonaws.com	54.225.165.85	true	false		high
smtpauth.earthlink.net	207.69.189.209	true	false		high
api.ipify.org	unknown	unknown	false		high

URLs from Memory and Binaries

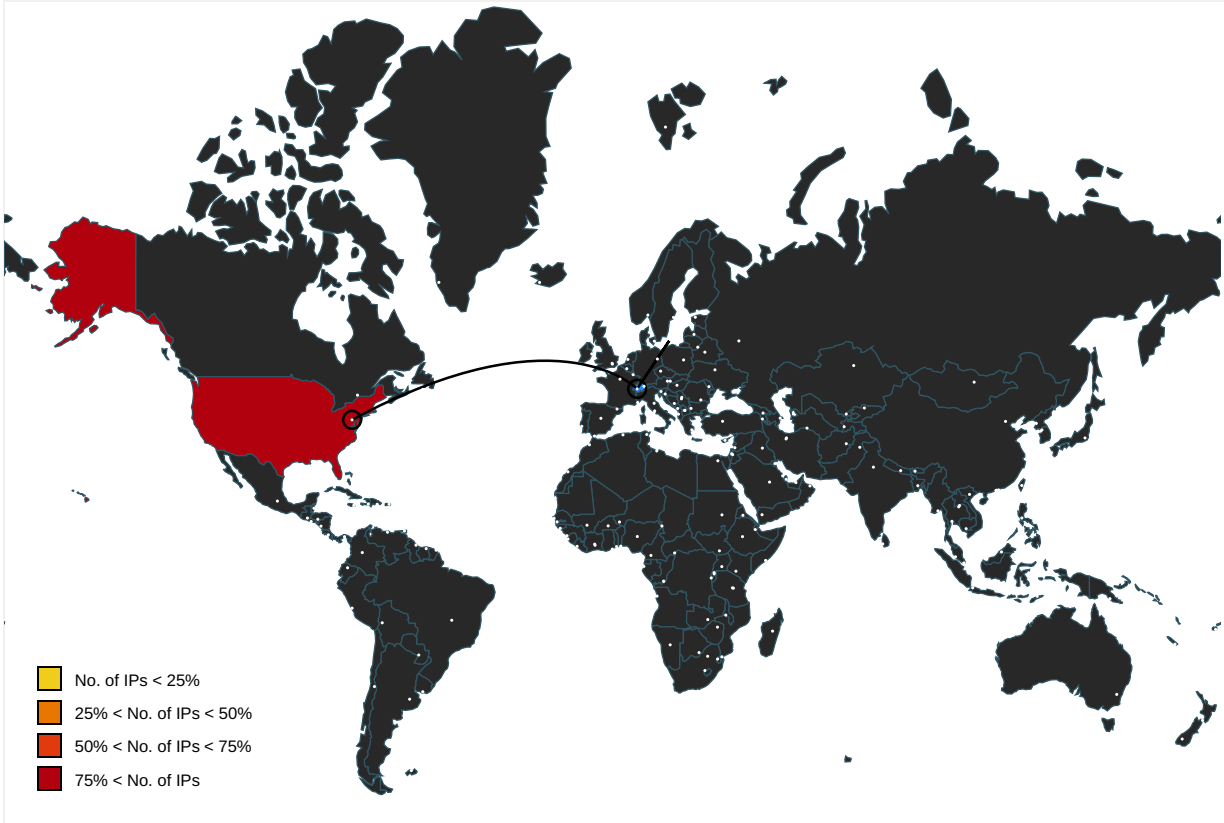
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org/	Sample Order.exe, 00000008.00000002.508711336.00000000031510000.00000004.00000001.sdmp	false		high
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	Sample Order.exe, 00000008.00000002.505914918.00000000015320000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://127.0.0.1:HTTP/1.1	Sample Order.exe, 00000008.00000002.508711336.00000000031510000.00000004.00000001.sdmp, wAyLNJ.exe, 00000018.00000002.507502345.0000000003181000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	Sample Order.exe, 00000000.00000002.281912036.0000000006AB2000.00000004.00000001.sdmp, wAyLNJ.exe, 00000014.00000002.384883678.0000000005A90000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	Sample Order.exe, 00000000.00000002.274019648.0000000000ED7000.00000004.00000040.sdmp, wAyLNJ.exe, 00000014.00000002.384883678.0000000005A90000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	Sample Order.exe, 00000000.00000002.281912036.0000000006AB2000.00000004.00000001.sdmp, wAyLNJ.exe, 00000014.00000002.384883678.0000000005A90000.00000002.00000001.sdmp	false		high
http://DynDns.comDynDNS	wAyLNJ.exe, 00000018.00000002.507502345.0000000003181000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://sectigo.com/CPS0	Sample Order.exe, 00000008.00000002.505914918.00000000015320000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/?	Sample Order.exe, 00000000.00000002.281912036.0000000006AB2000.00000004.00000001.sdmp, wAyLNJ.exe, 00000014.00000002.384883678.0000000005A90000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Sample Order.exe, 00000000.00000002.281912036.0000000006AB2000.00000004.00000001.sdmp, wAyLNJ.exe, 00000014.00000002.384883678.0000000005A90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.sectigo.com0	Sample Order.exe, 00000008.00000002.505914918.0000000001532000.00000004.00000020.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%tordir%%ha	Sample Order.exe, 00000008.00000002.508711336.0000000003151000.00000004.00000001.sdmp, wAyLNJ.exe, 00000018.00000002.507502345.0000000003181000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://DVEXLL.com	wAyLNJ.exe, 00000018.00000002.507502345.0000000003181000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	Sample Order.exe, 00000000.00000002.281912036.0000000006AB2000.00000004.00000001.sdmp, wAyLNJ.exe, 00000014.00000002.384883678.0000000005A90000.00000002.00000001.sdmp	false		high
http://www.tiro.com	wAyLNJ.exe, 00000014.00000002.384883678.0000000005A90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	wAyLNJ.exe, 00000014.00000002.384883678.0000000005A90000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	Sample Order.exe, 00000000.00000002.281912036.0000000006AB2000.00000004.00000001.sdmp, wAyLNJ.exe, 00000014.00000002.384883678.0000000005A90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	Sample Order.exe, 00000000.00000002.281912036.0000000006AB2000.00000004.00000001.sdmp, wAyLNJ.exe, 00000014.00000002.384883678.0000000005A90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	wAyLNJ.exe, 00000018.00000002.507502345.0000000003181000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	Sample Order.exe, 00000000.00000002.281912036.0000000006AB2000.00000004.00000001.sdmp, wAyLNJ.exe, 00000014.00000002.384883678.0000000005A90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Sample Order.exe, 00000000.00000002.281912036.0000000006AB2000.00000004.00000001.sdmp, wAyLNJ.exe, 00000014.00000002.384883678.0000000005A90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Sample Order.exe, 00000000.00000002.281912036.0000000006AB2000.00000004.00000001.sdmp, wAyLNJ.exe, 00000014.00000002.384883678.0000000005A90000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Sample Order.exe, 00000000.00000002.281912036.0000000006AB2000.00000004.00000001.sdmp, wAyLNJ.exe, 00000014.00000002.384883678.0000000005A90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Sample Order.exe, 00000000.00000002.281912036.0000000006AB2000.00000004.00000001.sdmp, wAyLNJ.exe, 00000014.00000002.384883678.0000000005A90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org	Sample Order.exe, 00000008.00000002.508711336.0000000031510000.00000004.00000001.sdmp	false		high
http://fontfabrik.com	Sample Order.exe, 00000000.00000002.281912036.0000000006AB2000.00000004.00000001.sdmp, wAyLNJ.exe, 00000014.00000002.384883678.0000000005A90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Sample Order.exe, 00000000.00000002.281912036.0000000006AB2000.00000004.00000001.sdmp, wAyLNJ.exe, 00000014.00000002.384883678.0000000005A90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Sample Order.exe, 00000000.00000002.281912036.0000000006AB2000.00000004.00000001.sdmp, wAyLNJ.exe, 00000014.00000002.384883678.0000000005A90000.00000002.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/	Sample Order.exe, 00000000.00000002.277083861.0000000003BFF000.00000004.00000001.sdmp, Sample Order.exe, 00000008.00000002.500306866.0000000000402000.00000040.00000001.sdmp, wAyLNJ.exe, 00000014.00000002.380533904.0000000003C5F000.00000004.00000001.sdmp, wAyLNJ.exe, 00000018.00000002.500770724.0000000000402000.00000040.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	Sample Order.exe, 00000000.00000002.281912036.0000000006AB2000.00000004.00000001.sdmp, wAyLNJ.exe, 00000014.00000002.384883678.0000000005A90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Sample Order.exe, 00000000.00000002.281912036.0000000006AB2000.00000004.00000001.sdmp, wAyLNJ.exe, 00000014.00000002.384883678.0000000005A90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Sample Order.exe, 00000000.00000002.281912036.0000000006AB2000.00000004.00000001.sdmp, wAyLNJ.exe, 00000014.00000002.384883678.0000000005A90000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comf37x	Sample Order.exe, 00000000.00000002.274019648.0000000000ED7000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	Sample Order.exe, 00000000.00000002.281912036.0000000006AB2000.00000004.00000001.sdmp, wAyLNJ.exe, 00000014.00000002.384883678.0000000005A90000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	Sample Order.exe, 00000000.00000002.281912036.0000000006AB2000.00000004.00000001.sdmp, wAyLNJ.exe, 00000014.00000002.384883678.0000000005A90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Sample Order.exe, 00000000.00000002.281912036.0000000006AB2000.00000004.00000001.sdmp, wAyLNJ.exe, 00000014.00000002.384883678.0000000005A90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Sample Order.exe, 00000000.00000002.281912036.0000000006AB2000.00000004.00000001.sdmp, wAyLNJ.exe, 00000014.00000002.384883678.0000000005A90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Sample Order.exe, 00000000.00000002.274728200.0000000002961000.00000004.00000001.sdmp, Sample Order.exe, 00000008.00000002.508711336.0000000003151000.00000004.00000001.sdmp, wAyLNJ.exe, 00000014.00000002.377708747.00000000029C1000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	Sample Order.exe, 00000000.00000002.281912036.0000000006AB2000.00000004.00000001.sdmp, wAyLNJ.exe, 00000014.00000002.384883678.0000000005A90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	Sample Order.exe, 00000008.00000002.508711336.0000000003151000.00000004.00000001.sdmp, wAyLNJ.exe, 00000018.00000002.507502345.0000000003181000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Sample Order.exe, 00000000.00000002.277083861.0000000003BFF000.00000004.00000001.sdmp, Sample Order.exe, 00000008.00000002.500306866.0000000000402000.00000040.00000001.sdmp, wAyLNJ.exe, 00000014.00000002.380533904.0000000003C5F000.00000004.00000001.sdmp, wAyLNJ.exe, 00000018.00000002.500770724.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
54.225.165.85	elb097307-934924932.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404235
Start date:	04.05.2021
Start time:	20:29:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Sample Order.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:	35
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@12/7@3/2
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 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 104.42.151.234, 23.54.113.53, 52.147.198.201, 104.43.193.48, 52.255.188.83, 23.57.80.111, 20.82.210.154, 92.122.213.194, 92.122.213.247, 93.184.221.240, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, wu.ec.azureedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/404235/sample/Sample Order.exe

Simulations

Behavior and APIs

Time	Type	Description
20:30:30	API Interceptor	585x Sleep call for process: Sample Order.exe modified
20:31:02	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run wAyLNJ C:\Users\user\AppData\Roaming\wAyLNJ\wAyLNJ.exe
20:31:10	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run wAyLNJ C:\Users\user\AppData\Roaming\wAyLNJ\wAyLNJ.exe
20:31:18	API Interceptor	298x Sleep call for process: wAyLNJ.exe modified

Copyright Joe Security LLC 2021

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54.225.165.85	FxHNFwShW0.exe	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	Quot_466378-09.exe	Get hash	malicious	Browse	• api.ipify.org/
	dzDuodOG0V.exe	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	msals.dll	Get hash	malicious	Browse	• api.ipify.org/?format=xml

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
elb097307-934924932.us-east-1.elb.amazonaws.com	2bb0000.exe	Get hash	malicious	Browse	• 50.16.249.42
	2f50000.exe	Get hash	malicious	Browse	• 23.21.48.44
	SecuriteInfo.com.Heur.31681.xls	Get hash	malicious	Browse	• 54.243.154.178
	3e98fa2d_by_Libranalysis.exe	Get hash	malicious	Browse	• 54.235.83.248
	0429_1556521897736.doc_berd.dll	Get hash	malicious	Browse	• 54.225.169.203
	e3d5e715_by_Libranalysis.exe	Get hash	malicious	Browse	• 54.243.121.36
	8f66.xls.exe	Get hash	malicious	Browse	• 54.225.169.203
	berd.b.dll	Get hash	malicious	Browse	• 23.21.48.44
	0427_5079687843613.doc	Get hash	malicious	Browse	• 107.22.233.72
	SThy2G7fGR.exe	Get hash	malicious	Browse	• 50.19.216.111
	if.ps1	Get hash	malicious	Browse	• 50.19.216.111
	jers.dll	Get hash	malicious	Browse	• 54.235.83.248
	ac8e3612_by_Libranalysis.exe	Get hash	malicious	Browse	• 50.19.252.36
	Onetap.com_Cracked_Auth_Bp_UPDATED_23.04.21.exe	Get hash	malicious	Browse	• 54.225.165.85
	furmt.f.dll	Get hash	malicious	Browse	• 23.21.252.4
	eGXZrIOs3P.exe	Get hash	malicious	Browse	• 54.235.175.90
	ff.exe	Get hash	malicious	Browse	• 54.225.222.160
	8s7bEDfYhT.exe	Get hash	malicious	Browse	• 54.225.155.255
	8c6b2adbcdd8b7f0a0419fd08e5cbd0f7bc52cc702da4.exe	Get hash	malicious	Browse	• 107.22.233.72
smtpauth.earthlink.net	PO19427.exe	Get hash	malicious	Browse	• 207.69.189.204
	RECEIPT DHL.exe	Get hash	malicious	Browse	• 207.69.189.205
	PO16388.exe	Get hash	malicious	Browse	• 207.69.189.206
	PO17440.exe	Get hash	malicious	Browse	• 207.69.189.209
	PO1055.exe	Get hash	malicious	Browse	• 207.69.189.207
	PO10448.exe	Get hash	malicious	Browse	• 207.69.189.208
	PO01044.exe	Get hash	malicious	Browse	• 207.69.189.205
	PO123066.exe	Get hash	malicious	Browse	• 207.69.189.205
	PO1228pdf.exe	Get hash	malicious	Browse	• 207.69.189.205
	PO121856.exe	Get hash	malicious	Browse	• 207.69.189.208
	DHL COPY.exe	Get hash	malicious	Browse	• 207.69.189.210
	C5o57lBFrs.exe	Get hash	malicious	Browse	• 207.69.189.205
	0y9m2LcCmp.exe	Get hash	malicious	Browse	• 207.69.189.206
	uw7Xt03ZwG.exe	Get hash	malicious	Browse	• 207.69.189.203
	Sample Order.exe	Get hash	malicious	Browse	• 207.69.189.202

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	Payment.xlsx	Get hash	malicious	Browse	• 54.156.162.121
	presentation.jar	Get hash	malicious	Browse	• 34.202.206.65
	presentation.jar	Get hash	malicious	Browse	• 34.202.206.65
	heUGqZXAJv.exe	Get hash	malicious	Browse	• 50.17.5.224
	2bb0000.exe	Get hash	malicious	Browse	• 50.16.249.42
	2f50000.exe	Get hash	malicious	Browse	• 23.21.48.44
	SecuriteInfo.com.Heur.31681.xls	Get hash	malicious	Browse	• 54.243.154.178
	MyUY1HeWNL.exe	Get hash	malicious	Browse	• 54.204.119.115
	Documents_111651917_375818984.xls	Get hash	malicious	Browse	• 54.163.9.216

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	detection.exe	Get hash	malicious	Browse	• 3.212.215.225
	4GGwmv0AJm.exe	Get hash	malicious	Browse	• 52.202.22.6
	#U260e#Ufe0fAUDIO-2020-05-26-18-51-m4a_MP4messages_2202-434.htm	Get hash	malicious	Browse	• 23.21.53.13
	OB74.vbs	Get hash	malicious	Browse	• 54.91.196.22
	3e98fa2d_by_Libranalysis.exe	Get hash	malicious	Browse	• 54.235.83.248
	file.exe	Get hash	malicious	Browse	• 3.223.115.185
	Outstanding Payment Plan.xls	Get hash	malicious	Browse	• 3.227.195.104
	0429_1556521897736.doc_berd.dll	Get hash	malicious	Browse	• 54.225.169.203
	KnAY2OIPI3	Get hash	malicious	Browse	• 54.161.176.221
	Bill Of Lading & Packing List.pdf.gz.exe	Get hash	malicious	Browse	• 3.223.115.185
	pVrqrGltiL.exe	Get hash	malicious	Browse	• 3.233.171.147

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	d.exe	Get hash	malicious	Browse	• 54.225.165.85
	d.exe	Get hash	malicious	Browse	• 54.225.165.85
	d.exe	Get hash	malicious	Browse	• 54.225.165.85
	d.exe	Get hash	malicious	Browse	• 54.225.165.85
	2bb0000.exe	Get hash	malicious	Browse	• 54.225.165.85
	2f50000.exe	Get hash	malicious	Browse	• 54.225.165.85
	oiY37pLlj7.exe	Get hash	malicious	Browse	• 54.225.165.85
	3ZtdRsbjxo.exe	Get hash	malicious	Browse	• 54.225.165.85
	Oej1asjUTO.exe	Get hash	malicious	Browse	• 54.225.165.85
	OK0n4zMIIm.exe	Get hash	malicious	Browse	• 54.225.165.85
	BID6200306761.exe	Get hash	malicious	Browse	• 54.225.165.85
	OverdueInvoice-PDF.exe	Get hash	malicious	Browse	• 54.225.165.85
	SLIP.exe	Get hash	malicious	Browse	• 54.225.165.85
	NeworderMay20212021-pdf.exe	Get hash	malicious	Browse	• 54.225.165.85
	1hbYGZf6BQ.exe	Get hash	malicious	Browse	• 54.225.165.85
	c89928a29ebf0c8c2acd7d9a457236e15d1a604d5c892.exe	Get hash	malicious	Browse	• 54.225.165.85
	from-iso_RFQ___PU.EXE1__.exe	Get hash	malicious	Browse	• 54.225.165.85
	80896e11_by_Libranalysis.exe	Get hash	malicious	Browse	• 54.225.165.85
	Xerox Scan_07122020181109.exe	Get hash	malicious	Browse	• 54.225.165.85
	menXxRXr64.exe	Get hash	malicious	Browse	• 54.225.165.85

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Sample Order.exe.log	
Process:	C:\Users\user\Desktop\Sample Order.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:	false
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Sample Order.exe.log	
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\Local\Microsoft\CLR_v4.0_32\UsageLogs\wAyLNJ.exe.log	
Process:	C:\Users\user\AppData\Roaming\wAyLNJ\wAyLNJ.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:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp3F4E.tmp	
Process:	C:\Users\user\AppData\Roaming\wAyLNJ\wAyLNJ.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1657
Entropy (8bit):	5.168510869426027
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBRtn:cbhH7MlNQ8/rydbz9I3YODOLNdq3p
MD5:	58480DD89319E839621E894EF3259821
SHA1:	E21BAA8814F20FD74F53A3DC0C3AC05C1C0E3FA5
SHA-256:	DC33DF52253490D45B2131EACCCA2EC4B426833DC0BCA2FC98F9034A7EDB33C3
SHA-512:	3F55934FDA0EE64696727DE286841D70436A6369938855698DCE5D033D75410691219355D6CD9BD7619A82233F2395A480F1F5B331F0CF50AD5A58E428EE3754
Malicious:	false
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>.. <StartWhenAv

C:\Users\user\AppData\Local\Temp\tmp8100.tmp	
Process:	C:\Users\user\Desktop\Sample Order.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1657
Entropy (8bit):	5.168510869426027
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBRtn:cbhH7MlNQ8/rydbz9I3YODOLNdq3p
MD5:	58480DD89319E839621E894EF3259821
SHA1:	E21BAA8814F20FD74F53A3DC0C3AC05C1C0E3FA5
SHA-256:	DC33DF52253490D45B2131EACCCA2EC4B426833DC0BCA2FC98F9034A7EDB33C3
SHA-512:	3F55934FDA0EE64696727DE286841D70436A6369938855698DCE5D033D75410691219355D6CD9BD7619A82233F2395A480F1F5B331F0CF50AD5A58E428EE3754
Malicious:	**true**
Reputation:	low

C:\Users\user\AppData\Local\Temp\tmp8100.tmp	
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>.. <StartWhenAv

C:\Users\user\AppData\Roaming\OnUeAYnP.exe	
Process:	C:\Users\user\Desktop\Sample Order.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1027584
Entropy (8bit):	7.140958849064524
Encrypted:	false
SSDEEP:	12288:aPbB4fWXY3Ot6InK1sLuNp+dM0kKg0D75wAPG+zETi/Pih2CV5R2DMajN2vZOmFb:afN2vsQ1oLAL+rdgUSzcr9Pr3fYM99U
MD5:	72D643819882BAF6C48246024D4755D1
SHA1:	EDC461E732F56CAA64C1CE4B02094FDD3D9AF99F
SHA-256:	C590C197137574E792A991B5C56791B8F7CCCD4985D46B9F459FC6C39FDEB4AB
SHA-512:	D54692E43D07CD232DF9B206C23DB1A8FB05FC1D7BA8C60C30CF68F46ABBC13CF18617867C5FDEDE8D89B5110F41D4E0F72A3C2ED4F2792301F0FAFECC294AE
Malicious:	false
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...}.....0.....J.... .....@.. ....@.....O..... ....H.....text...P.... ....`.rsrc.....@..@.reloc..... .....@..B.....,.....H.....i....r..XN.....0.....r...p.+..*..0.....r!..p.+..*"(.....*.0..p.....r1..p..{....s.....o.....s.....o....r...p.o... .o....&.o....&r...pr...p..@(....&.o.....o ...(!...&...*.....]^.....0..c.....r...p..{....s.....o.....s.....o....r8..p.o....o....&.o....rF..p.o....o....&.o....rV..p.o....o....&.o....rf..p..o....o....&.o. ...rv..p..o"...o#...o....&.o....r...p..o....o....&.o....r...p..o$....

C:\Users\user\AppData\Roaming\wAyLNJ\wAyLNJ.exe	
Process:	C:\Users\user\Desktop\Sample Order.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1027584
Entropy (8bit):	7.140958849064524
Encrypted:	false
SSDEEP:	12288:aPbB4fWXY3Ot6InK1sLuNp+dM0kKg0D75wAPG+zETi/Pih2CV5R2DMajN2vZOmFb:afN2vsQ1oLAL+rdgUSzcr9Pr3fYM99U
MD5:	72D643819882BAF6C48246024D4755D1
SHA1:	EDC461E732F56CAA64C1CE4B02094FDD3D9AF99F
SHA-256:	C590C197137574E792A991B5C56791B8F7CCCD4985D46B9F459FC6C39FDEB4AB
SHA-512:	D54692E43D07CD232DF9B206C23DB1A8FB05FC1D7BA8C60C30CF68F46ABBC13CF18617867C5FDEDE8D89B5110F41D4E0F72A3C2ED4F2792301F0FAFECC294AE
Malicious:	**true**
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...}.....0.....J.... .....@.. ....@.....O..... ....H.....text...P.... ....`.rsrc.....@..@.reloc..... .....@..B.....,.....H.....i....r..XN.....0.....r...p.+..*..0.....r!..p.+..*"(.....*.0..p.....r1..p..{....s.....o.....s.....o....r...p.o... .o....&.o....&r...pr...p..@(....&.o.....o ...(!...&...*.....]^.....0..c.....r...p..{....s.....o.....s.....o....r8..p.o....o....&.o....rF..p.o....o....&.o....rV..p.o....o....&.o....rf..p..o....o....&.o. ...rv..p..o"...o#...o....&.o....r...p..o....o....&.o....r...p..o$....

C:\Users\user\AppData\Roaming\wAyLNJ\wAyLNJ.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Sample Order.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.140958849064524
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:	Sample Order.exe
File size:	1027584
MD5:	72d643819882baf6c48246024d4755d1
SHA1:	edc461e732f56caa64c1ce4b02094fdd3d9af99f
SHA256:	c590c197137574e792a991b5c56791b8f7cccd4985d46b9f459fc6c39fdeb4ab
SHA512:	d54692e43d07cd232df9b206c23db1a8fb05fc1d7ba8c60c30cf68f46abbc13cf18617867c5fdede8d89b5110f41d4e0f72a3c2ed4f2792301f0fafecc2942ae
SSDEEP:	12288:aPbB4fWXY3Ot6InK1sLuNp+dM0kKg0D75wAPG+zETi/Pih2CV5R2DMajN2vZOmFb:afN2vsQ1oLAL+rdgUSzcr9Pr3fYM99U
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...}.....0.....J.... .....@.. .... @.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4fc14a
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:	0xDA92057D [Fri Mar 15 03:52:29 2086 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

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

Copyright Joe Security LLC 2021

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xfc0f8	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xfe000	0x604	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x100000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xfc0dc	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xfa150	0xfa200	False	0.619275323276	data	7.14748707063	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xfe000	0x604	0x800	False	0.33056640625	data	3.442123386	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x100000	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	0xfe090	0x374	data		
RT_MANIFEST	0xfe414	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

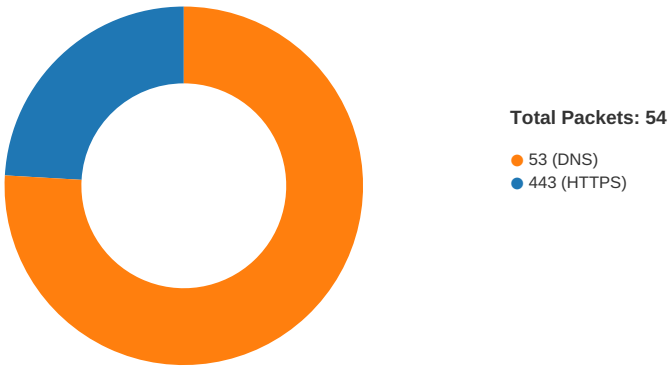
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2019
Assembly Version	1.0.0.0
InternalName	R0QTaaU57lgwlvp.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	HospitalManagementSystem
ProductVersion	1.0.0.0
FileDescription	HospitalManagementSystem
OriginalFilename	R0QTaaU57lgwlvp.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:32:14.657835007 CEST	49745	443	192.168.2.7	54.225.165.85
May 4, 2021 20:32:14.794311047 CEST	443	49745	54.225.165.85	192.168.2.7
May 4, 2021 20:32:14.794464111 CEST	49745	443	192.168.2.7	54.225.165.85
May 4, 2021 20:32:14.944673061 CEST	49745	443	192.168.2.7	54.225.165.85
May 4, 2021 20:32:15.080727100 CEST	443	49745	54.225.165.85	192.168.2.7
May 4, 2021 20:32:15.081146955 CEST	443	49745	54.225.165.85	192.168.2.7
May 4, 2021 20:32:15.081177950 CEST	443	49745	54.225.165.85	192.168.2.7
May 4, 2021 20:32:15.081199884 CEST	443	49745	54.225.165.85	192.168.2.7
May 4, 2021 20:32:15.081214905 CEST	443	49745	54.225.165.85	192.168.2.7
May 4, 2021 20:32:15.081254005 CEST	49745	443	192.168.2.7	54.225.165.85
May 4, 2021 20:32:15.081312895 CEST	49745	443	192.168.2.7	54.225.165.85
May 4, 2021 20:32:15.082535028 CEST	443	49745	54.225.165.85	192.168.2.7
May 4, 2021 20:32:15.082566023 CEST	443	49745	54.225.165.85	192.168.2.7
May 4, 2021 20:32:15.082684040 CEST	49745	443	192.168.2.7	54.225.165.85
May 4, 2021 20:32:15.106251955 CEST	49745	443	192.168.2.7	54.225.165.85
May 4, 2021 20:32:15.242754936 CEST	443	49745	54.225.165.85	192.168.2.7
May 4, 2021 20:32:15.389569044 CEST	49745	443	192.168.2.7	54.225.165.85

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:32:15.728473902 CEST	49745	443	192.168.2.7	54.225.165.85
May 4, 2021 20:32:15.878981113 CEST	443	49745	54.225.165.85	192.168.2.7
May 4, 2021 20:32:15.926398039 CEST	49745	443	192.168.2.7	54.225.165.85
May 4, 2021 20:32:33.874614954 CEST	49745	443	192.168.2.7	54.225.165.85
May 4, 2021 20:32:34.010678053 CEST	443	49745	54.225.165.85	192.168.2.7
May 4, 2021 20:32:34.010718107 CEST	443	49745	54.225.165.85	192.168.2.7
May 4, 2021 20:32:34.010852098 CEST	49745	443	192.168.2.7	54.225.165.85
May 4, 2021 20:32:34.010889053 CEST	49745	443	192.168.2.7	54.225.165.85

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:30:08.858066082 CEST	58562	53	192.168.2.7	8.8.8.8
May 4, 2021 20:30:08.860856056 CEST	53	61242	8.8.8.8	192.168.2.7
May 4, 2021 20:30:08.908843040 CEST	53	58562	8.8.8.8	192.168.2.7
May 4, 2021 20:30:10.097419977 CEST	56590	53	192.168.2.7	8.8.8.8
May 4, 2021 20:30:10.148925066 CEST	53	56590	8.8.8.8	192.168.2.7
May 4, 2021 20:30:10.873898029 CEST	60501	53	192.168.2.7	8.8.8.8
May 4, 2021 20:30:10.933217049 CEST	53	60501	8.8.8.8	192.168.2.7
May 4, 2021 20:30:11.218646049 CEST	53775	53	192.168.2.7	8.8.8.8
May 4, 2021 20:30:11.269264936 CEST	53	53775	8.8.8.8	192.168.2.7
May 4, 2021 20:30:12.459719896 CEST	51837	53	192.168.2.7	8.8.8.8
May 4, 2021 20:30:12.511441946 CEST	53	51837	8.8.8.8	192.168.2.7
May 4, 2021 20:30:14.032279015 CEST	55411	53	192.168.2.7	8.8.8.8
May 4, 2021 20:30:14.089430094 CEST	53	55411	8.8.8.8	192.168.2.7
May 4, 2021 20:30:15.235475063 CEST	63668	53	192.168.2.7	8.8.8.8
May 4, 2021 20:30:15.297601938 CEST	53	63668	8.8.8.8	192.168.2.7
May 4, 2021 20:30:16.129601955 CEST	54640	53	192.168.2.7	8.8.8.8
May 4, 2021 20:30:16.180043936 CEST	53	54640	8.8.8.8	192.168.2.7
May 4, 2021 20:30:16.953202009 CEST	58739	53	192.168.2.7	8.8.8.8
May 4, 2021 20:30:17.002230883 CEST	53	58739	8.8.8.8	192.168.2.7
May 4, 2021 20:30:18.285514116 CEST	60338	53	192.168.2.7	8.8.8.8
May 4, 2021 20:30:18.336981058 CEST	53	60338	8.8.8.8	192.168.2.7
May 4, 2021 20:30:20.190808058 CEST	58717	53	192.168.2.7	8.8.8.8
May 4, 2021 20:30:20.242209911 CEST	53	58717	8.8.8.8	192.168.2.7
May 4, 2021 20:30:21.235343933 CEST	59762	53	192.168.2.7	8.8.8.8
May 4, 2021 20:30:21.285810947 CEST	53	59762	8.8.8.8	192.168.2.7
May 4, 2021 20:30:22.165676117 CEST	54329	53	192.168.2.7	8.8.8.8
May 4, 2021 20:30:22.214337111 CEST	53	54329	8.8.8.8	192.168.2.7
May 4, 2021 20:30:23.331059933 CEST	58052	53	192.168.2.7	8.8.8.8
May 4, 2021 20:30:23.379683971 CEST	53	58052	8.8.8.8	192.168.2.7
May 4, 2021 20:30:24.278430939 CEST	54008	53	192.168.2.7	8.8.8.8
May 4, 2021 20:30:24.340960026 CEST	53	54008	8.8.8.8	192.168.2.7
May 4, 2021 20:30:25.797188997 CEST	59451	53	192.168.2.7	8.8.8.8
May 4, 2021 20:30:25.845814943 CEST	53	59451	8.8.8.8	192.168.2.7
May 4, 2021 20:30:26.936392069 CEST	52914	53	192.168.2.7	8.8.8.8
May 4, 2021 20:30:26.989067078 CEST	53	52914	8.8.8.8	192.168.2.7
May 4, 2021 20:30:27.815330029 CEST	64569	53	192.168.2.7	8.8.8.8
May 4, 2021 20:30:27.866847992 CEST	53	64569	8.8.8.8	192.168.2.7
May 4, 2021 20:30:28.927364111 CEST	52816	53	192.168.2.7	8.8.8.8
May 4, 2021 20:30:28.976022005 CEST	53	52816	8.8.8.8	192.168.2.7
May 4, 2021 20:30:30.022737980 CEST	50781	53	192.168.2.7	8.8.8.8
May 4, 2021 20:30:30.071572065 CEST	53	50781	8.8.8.8	192.168.2.7
May 4, 2021 20:30:31.006349087 CEST	54230	53	192.168.2.7	8.8.8.8
May 4, 2021 20:30:31.055059910 CEST	53	54230	8.8.8.8	192.168.2.7
May 4, 2021 20:30:33.959883928 CEST	54911	53	192.168.2.7	8.8.8.8
May 4, 2021 20:30:34.023421049 CEST	53	54911	8.8.8.8	192.168.2.7
May 4, 2021 20:30:47.864540100 CEST	49958	53	192.168.2.7	8.8.8.8
May 4, 2021 20:30:47.915407896 CEST	53	49958	8.8.8.8	192.168.2.7
May 4, 2021 20:31:00.323000908 CEST	50860	53	192.168.2.7	8.8.8.8
May 4, 2021 20:31:00.391858101 CEST	53	50860	8.8.8.8	192.168.2.7
May 4, 2021 20:31:04.054985046 CEST	50452	53	192.168.2.7	8.8.8.8
May 4, 2021 20:31:04.109242916 CEST	53	50452	8.8.8.8	192.168.2.7
May 4, 2021 20:31:33.836658001 CEST	59730	53	192.168.2.7	8.8.8.8

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:31:33.885449886 CEST	53	59730	8.8.8.8	192.168.2.7
May 4, 2021 20:31:40.126043081 CEST	59310	53	192.168.2.7	8.8.8.8
May 4, 2021 20:31:40.178687096 CEST	53	59310	8.8.8.8	192.168.2.7
May 4, 2021 20:32:00.569900990 CEST	51919	53	192.168.2.7	8.8.8.8
May 4, 2021 20:32:00.631804943 CEST	53	51919	8.8.8.8	192.168.2.7
May 4, 2021 20:32:01.364115953 CEST	64296	53	192.168.2.7	8.8.8.8
May 4, 2021 20:32:01.421082973 CEST	53	64296	8.8.8.8	192.168.2.7
May 4, 2021 20:32:02.005837917 CEST	56680	53	192.168.2.7	8.8.8.8
May 4, 2021 20:32:02.055875063 CEST	58820	53	192.168.2.7	8.8.8.8
May 4, 2021 20:32:02.066869974 CEST	53	56680	8.8.8.8	192.168.2.7
May 4, 2021 20:32:02.114784002 CEST	53	58820	8.8.8.8	192.168.2.7
May 4, 2021 20:32:02.530379057 CEST	60983	53	192.168.2.7	8.8.8.8
May 4, 2021 20:32:02.590306044 CEST	53	60983	8.8.8.8	192.168.2.7
May 4, 2021 20:32:03.279875040 CEST	49247	53	192.168.2.7	8.8.8.8
May 4, 2021 20:32:03.328921080 CEST	53	49247	8.8.8.8	192.168.2.7
May 4, 2021 20:32:03.916090012 CEST	52286	53	192.168.2.7	8.8.8.8
May 4, 2021 20:32:03.973351955 CEST	53	52286	8.8.8.8	192.168.2.7
May 4, 2021 20:32:04.578849077 CEST	56064	53	192.168.2.7	8.8.8.8
May 4, 2021 20:32:04.715496063 CEST	53	56064	8.8.8.8	192.168.2.7
May 4, 2021 20:32:05.982620001 CEST	63744	53	192.168.2.7	8.8.8.8
May 4, 2021 20:32:06.094033957 CEST	53	63744	8.8.8.8	192.168.2.7
May 4, 2021 20:32:08.383146048 CEST	61457	53	192.168.2.7	8.8.8.8
May 4, 2021 20:32:08.467329979 CEST	53	61457	8.8.8.8	192.168.2.7
May 4, 2021 20:32:08.930804014 CEST	58367	53	192.168.2.7	8.8.8.8
May 4, 2021 20:32:09.063206911 CEST	53	58367	8.8.8.8	192.168.2.7
May 4, 2021 20:32:14.348215103 CEST	60599	53	192.168.2.7	8.8.8.8
May 4, 2021 20:32:14.402070045 CEST	53	60599	8.8.8.8	192.168.2.7
May 4, 2021 20:32:14.419312954 CEST	59571	53	192.168.2.7	8.8.8.8
May 4, 2021 20:32:14.468091965 CEST	53	59571	8.8.8.8	192.168.2.7
May 4, 2021 20:32:33.872912884 CEST	52689	53	192.168.2.7	8.8.8.8
May 4, 2021 20:32:33.922251940 CEST	53	52689	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 20:32:14.348215103 CEST	192.168.2.7	8.8.8.8	0x6aa9	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
May 4, 2021 20:32:14.419312954 CEST	192.168.2.7	8.8.8.8	0x38d6	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
May 4, 2021 20:32:33.872912884 CEST	192.168.2.7	8.8.8.8	0xe9af	Standard query (0)	smtpauth.earthlink.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 20:32:14.402070045 CEST	8.8.8.8	192.168.2.7	0x6aa9	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 20:32:14.402070045 CEST	8.8.8.8	192.168.2.7	0x6aa9	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 20:32:14.402070045 CEST	8.8.8.8	192.168.2.7	0x6aa9	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.165.85	A (IP address)	IN (0x0001)
May 4, 2021 20:32:14.402070045 CEST	8.8.8.8	192.168.2.7	0x6aa9	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.83.248	A (IP address)	IN (0x0001)
May 4, 2021 20:32:14.402070045 CEST	8.8.8.8	192.168.2.7	0x6aa9	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.144.221	A (IP address)	IN (0x0001)
May 4, 2021 20:32:14.402070045 CEST	8.8.8.8	192.168.2.7	0x6aa9	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.216.111	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 20:32:14.402070045 CEST	8.8.8.8	192.168.2.7	0x6aa9	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.242.215	A (IP address)	IN (0x0001)
May 4, 2021 20:32:14.402070045 CEST	8.8.8.8	192.168.2.7	0x6aa9	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.252.4	A (IP address)	IN (0x0001)
May 4, 2021 20:32:14.402070045 CEST	8.8.8.8	192.168.2.7	0x6aa9	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)
May 4, 2021 20:32:14.402070045 CEST	8.8.8.8	192.168.2.7	0x6aa9	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.96.218	A (IP address)	IN (0x0001)
May 4, 2021 20:32:14.468091965 CEST	8.8.8.8	192.168.2.7	0x38d6	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 20:32:14.468091965 CEST	8.8.8.8	192.168.2.7	0x38d6	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 20:32:14.468091965 CEST	8.8.8.8	192.168.2.7	0x38d6	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.165.85	A (IP address)	IN (0x0001)
May 4, 2021 20:32:14.468091965 CEST	8.8.8.8	192.168.2.7	0x38d6	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.83.248	A (IP address)	IN (0x0001)
May 4, 2021 20:32:14.468091965 CEST	8.8.8.8	192.168.2.7	0x38d6	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.144.221	A (IP address)	IN (0x0001)
May 4, 2021 20:32:14.468091965 CEST	8.8.8.8	192.168.2.7	0x38d6	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.216.111	A (IP address)	IN (0x0001)
May 4, 2021 20:32:14.468091965 CEST	8.8.8.8	192.168.2.7	0x38d6	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.242.215	A (IP address)	IN (0x0001)
May 4, 2021 20:32:14.468091965 CEST	8.8.8.8	192.168.2.7	0x38d6	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.252.4	A (IP address)	IN (0x0001)
May 4, 2021 20:32:14.468091965 CEST	8.8.8.8	192.168.2.7	0x38d6	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)
May 4, 2021 20:32:14.468091965 CEST	8.8.8.8	192.168.2.7	0x38d6	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.96.218	A (IP address)	IN (0x0001)
May 4, 2021 20:32:33.922251940 CEST	8.8.8.8	192.168.2.7	0xe9af	No error (0)	smtpauth.earthlink.net		207.69.189.209	A (IP address)	IN (0x0001)
May 4, 2021 20:32:33.922251940 CEST	8.8.8.8	192.168.2.7	0xe9af	No error (0)	smtpauth.earthlink.net		207.69.189.210	A (IP address)	IN (0x0001)
May 4, 2021 20:32:33.922251940 CEST	8.8.8.8	192.168.2.7	0xe9af	No error (0)	smtpauth.earthlink.net		207.69.189.201	A (IP address)	IN (0x0001)
May 4, 2021 20:32:33.922251940 CEST	8.8.8.8	192.168.2.7	0xe9af	No error (0)	smtpauth.earthlink.net		207.69.189.202	A (IP address)	IN (0x0001)
May 4, 2021 20:32:33.922251940 CEST	8.8.8.8	192.168.2.7	0xe9af	No error (0)	smtpauth.earthlink.net		207.69.189.203	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 20:32:33.922251940 CEST	8.8.8.8	192.168.2.7	0xe9af	No error (0)	smtpauth.earthlink.net		207.69.189.204	A (IP address)	IN (0x0001)
May 4, 2021 20:32:33.922251940 CEST	8.8.8.8	192.168.2.7	0xe9af	No error (0)	smtpauth.earthlink.net		207.69.189.205	A (IP address)	IN (0x0001)
May 4, 2021 20:32:33.922251940 CEST	8.8.8.8	192.168.2.7	0xe9af	No error (0)	smtpauth.earthlink.net		207.69.189.206	A (IP address)	IN (0x0001)
May 4, 2021 20:32:33.922251940 CEST	8.8.8.8	192.168.2.7	0xe9af	No error (0)	smtpauth.earthlink.net		207.69.189.207	A (IP address)	IN (0x0001)
May 4, 2021 20:32:33.922251940 CEST	8.8.8.8	192.168.2.7	0xe9af	No error (0)	smtpauth.earthlink.net		207.69.189.208	A (IP address)	IN (0x0001)

HTTPS Packets

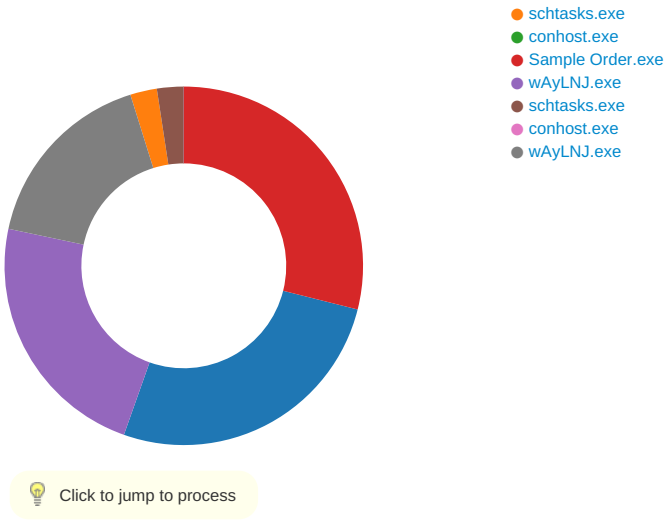
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
May 4, 2021 20:32:15.082566023 CEST	54.225.165.85	443	192.168.2.7	49745	CN=*.ipify.org CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Jan 19 01:00:00 CET 2021 Fri Nov 02 01:00:00 CET 2018 Tue Mar 12 01:00:00 CET 2019 Thu Jan 01 01:00:00 CET 2004	Sun Feb 20 00:59:59 CET 2022 Wed Jan 01 00:59:59 CET 2031 Mon Jan 01 00:59:59 CET 2029 Mon Jan 01 00:59:59 CET 2029	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford, ST=Greater Manchester, C=GB	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	Fri Nov 02 01:00:00 CET 2018	Wed Jan 01 00:59:59 CET 2031		
					CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, L=Jersey City, ST=New Jersey, C=US	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Mar 12 01:00:00 CET 2019	Mon Jan 01 00:59:59 CET 2029		
					CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB	Thu Jan 01 01:00:00 CET 2004	Mon Jan 01 00:59:59 CET 2029		

Code Manipulations

Statistics

Behavior

● Sample Order.exe



System Behavior

Analysis Process: Sample Order.exe PID: 5488 Parent PID: 5700

General

Start time:	20:30:16
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\Sample Order.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Sample Order.exe'
Imagebase:	0x520000
File size:	1027584 bytes
MD5 hash:	72D643819882BAF6C48246024D4755D1
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: 00000000.00000002.277083861.0000000003BFF000.00000004.00000001.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	6D3CCF06	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	6D3CCF06	unknown
C:\Users\user\AppData\Roaming\OnUeAYnP.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C211E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp8100.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C217038	GetTempFileNameW

Copyright Joe Security LLC 2021

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Sample Order.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6DC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8100.tmp	success or wait	1	6C216A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\OnUeAYnP.exe	unknown	1027584	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 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 7d 05 92 da 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 a2 0f 00 00 0a 00 00 00 00 00 00 4a c1 0f 00 00 20 00 00 00 e0 0f 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 20 10 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...}............ ....0.............J.... ....@.. ....@................	success or wait	1	6C211B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8100.tmp	unknown	1657	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 66 72 6f 6e 74 64 65 73 6b 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	<?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>.. </Registrati	success or wait	1	6C211B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Sample Order.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	6D6DC907	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	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3ACA54	ReadFile

Copyright Joe Security LLC 2021

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C211B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C211B4F	ReadFile
C:\Users\user\Desktop\Sample Order.exe	unknown	1027584	success or wait	1	6C211B4F	ReadFile

Analysis Process: schtasks.exe PID: 5828 Parent PID: 5488

General

Start time:	20:30:33
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\OnUeAYnP' /XML 'C:\Users \user\AppData\Local\Temp\tmp8100.tmp'
Imagebase:	0xd60000
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\tmp8100.tmp	unknown	2	success or wait	1	D6AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp8100.tmp	unknown	1658	success or wait	1	D6ABD9	ReadFile

Analysis Process: conhost.exe PID: 5784 Parent PID: 5828

General

Start time:	20:30:35
Start date:	04/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Copyright Joe Security LLC 2021

Analysis Process: Sample Order.exe PID: 4452 Parent PID: 5488

General

Start time:	20:30:35
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\Sample Order.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xc60000
File size:	1027584 bytes
MD5 hash:	72D643819882BAF6C48246024D4755D1
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: 00000008.00000002.508711336.0000000003151000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000008.00000002.508711336.0000000003151000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.500306866.0000000000402000.00000040.00000001.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	6D3CCF06	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	6D3CCF06	unknown
C:\Users\user\AppData\Roaming\wAyLNJ	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C21BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\wAyLNJ\wAyLNJ.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	6C21DD66	CopyFileW
C:\Users\user\AppData\Roaming\wAyLNJ\wAyLNJ.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C21DD66	CopyFileW

File Path	Completion	Count	Source Address	Symbol

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\wAyLNJ\wAyLNJ.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 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 50 45 00 00 4c 01 03 00 7d 05 92 da 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 a2 0f 00 00 0a 00 00 00 00 00 00 4a c1 0f 00 00 20 00 00 00 e0 0f 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 20 10 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...}............ ....0.............J.... ....@.. ....@................	success or wait	4	6C21DD66	CopyFileW
C:\Users\user\AppData\Roaming\wAyLNJ\wAyLNJ.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	6C21DD66	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	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C211B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C211B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6C211B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\84e8604f-8521-4e0b-88d1-6427068cb6a8	unknown	4096	success or wait	1	6C211B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6C211B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	wAyLNJ	unicode	C:\Users\user\AppData\Roaming\wAyLNJ\wAyLNJ.exe	success or wait	1	6C21646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	wAyLNJ	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C21DE2E	RegSetValueExW

Analysis Process: wAyLNJ.exe PID: 6420 Parent PID: 3292

General

Start time:	20:31:11
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Roaming\wAyLNJ\wAyLNJ.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\wAyLNJ\wAyLNJ.exe'
Imagebase:	0x5f0000
File size:	1027584 bytes
MD5 hash:	72D643819882BAF6C48246024D4755D1
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: 00000014.00000002.380533904.0000000003C5F000.00000004.00000001.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	6D3CCF06	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	6D3CCF06	unknown
C:\Users\user\AppData\Local\Temp\tmp3F4E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C217038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\wAyLNJ.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6DC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp3F4E.tmp	success or wait	1	6C216A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Copyright Joe Security LLC 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp3F4E.tmp	unknown	1657	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 66 72 6f 6e 74 64 65 73 6b 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	<?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>.. </Registrati	success or wait	1	6C211B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\wAyLNJ.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	6D6DC907	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	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3ACA54	ReadFile

Copyright Joe Security LLC 2021

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C211B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C211B4F	ReadFile

Analysis Process: schtasks.exe PID: 6616 Parent PID: 6420

General

Start time:	20:31:21
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\OnUeAYnP' /XML 'C:\Users \user\AppData\Local\Temp\tmp3F4E.tmp'
Imagebase:	0xa30000
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\tmp3F4E.tmp	unknown	2	success or wait	1	A3AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp3F4E.tmp	unknown	1658	success or wait	1	A3ABD9	ReadFile

Analysis Process: conhost.exe PID: 6632 Parent PID: 6616

General

Start time:	20:31:22
Start date:	04/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Copyright Joe Security LLC 2021

Analysis Process: wAyLNJ.exe PID: 6668 Parent PID: 6420

General

Start time:	20:31:23
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Roaming\wAyLNJ\wAyLNJ.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xc90000
File size:	1027584 bytes
MD5 hash:	72D643819882BAF6C48246024D4755D1
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: 00000018.00000002.500770724.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000018.00000002.507502345.0000000003181000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000018.00000002.507502345.0000000003181000.00000004.00000001.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	6D3CCF06	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	6D3CCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C211B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C211B4F	ReadFile

Disassembly

Copyright Joe Security LLC 2021

Code Analysis