ID: 385435
Sample Name:
VJNPltkyHyI3CCo.exe
Cookbook: default.jbs
Time: 14:20:16
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

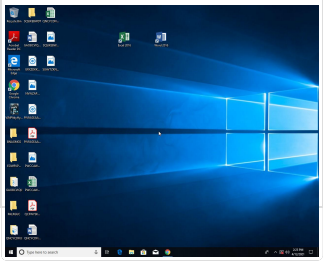
Analysis Report VJNPltkyHyI3CCo.exe

Overview

General Information

Sample Name:	VJNPltkyHyI3CCo.exe
Analysis ID:	385435
MD5:	36a7049a4f3be87.
SHA1:	fbefd649daddd22..
SHA256:	20251c86adaf2dc..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

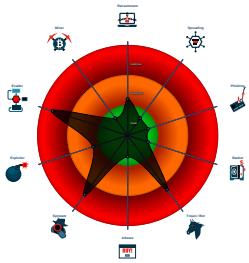
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Injects a PE file into a foreign proce…
- 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 harvest and steal ftp login c…

Classification



Startup

- **System is w10x64**
- VJNPltkyHyI3CCo.exe (PID: 1156 cmdline: 'C:\Users\user\Desktop\VJNPltkyHyI3CCo.exe' MD5: 36A7049A4F3BE8788F0C844319A5364B)
  - VJNPltkyHyI3CCo.exe (PID: 748 cmdline: C:\Users\user\Desktop\VJNPltkyHyI3CCo.exe MD5: 36A7049A4F3BE8788F0C844319A5364B)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "office4@iykmoreentrprise.orgrwkWCM328mail.iykmoreentrprise.org"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.212033159.000000000351 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000002.00000002.464818672.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.212559557.000000000465 E000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.469579413.000000000307 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.469579413.000000000307 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	

Click to see the 4 entries

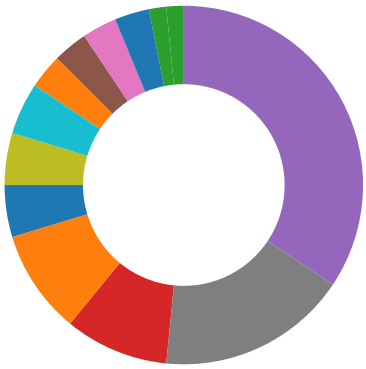
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.VJNPltkyHyl3CCo.exe.47c26f0.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.VJNPltkyHyl3CCo.exe.47c26f0.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.VJNPltkyHyl3CCo.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- 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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

System Summary:

.NET source code contains very large array initializations

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

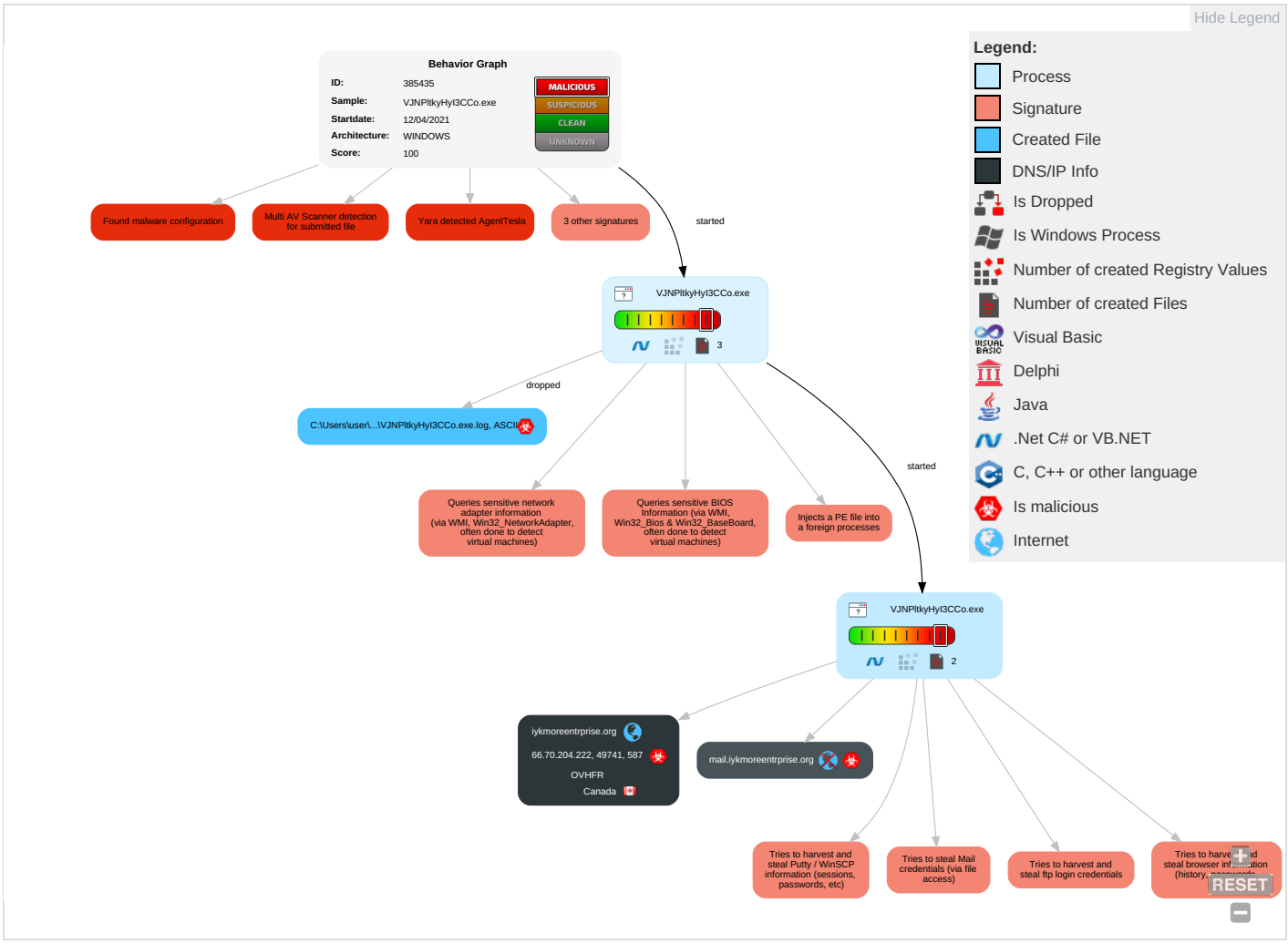
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

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

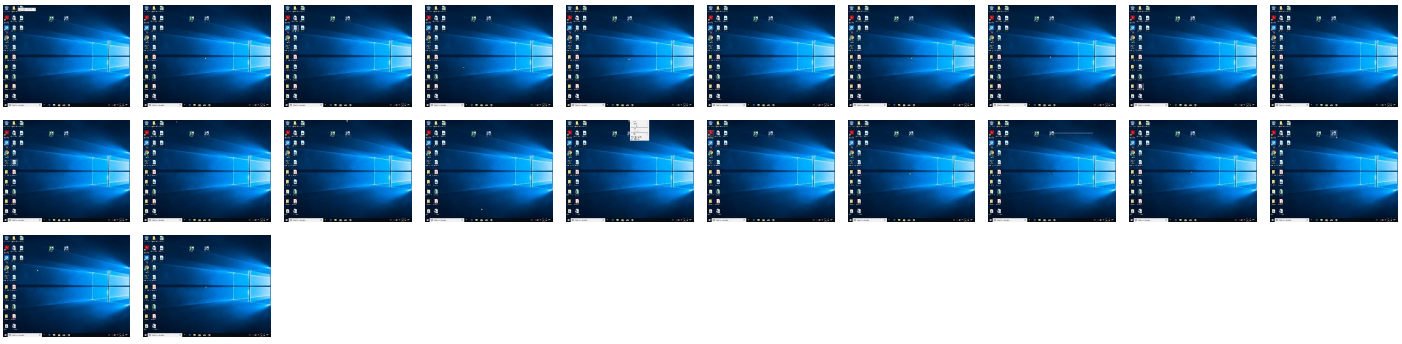
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
VJNPltkyHyI3CCo.exe	17%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.VJNPltkyHyI3CCo.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
mail.iykmoreentrprise.org	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://iykmoreentrprise.org	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	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://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	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://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://api.ipify.org%(	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.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.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comFM	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.i.lencr.org/0	0%	URL Reputation	safe	
http://r3.i.lencr.org/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.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.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.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://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://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	

Source	Detection	Scanner	Label	Link
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	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://GTAZqk.com	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://A84D2ljcLQUVG1tA.net	0%	Avira URL Cloud	safe	
http://www.fontbureau.comttva4	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://mail.iykmoreentrprise.org	0%	Avira URL Cloud	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
iykmoreentrprise.org	66.70.204.222	true	true		unknown
mail.iykmoreentrprise.org	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

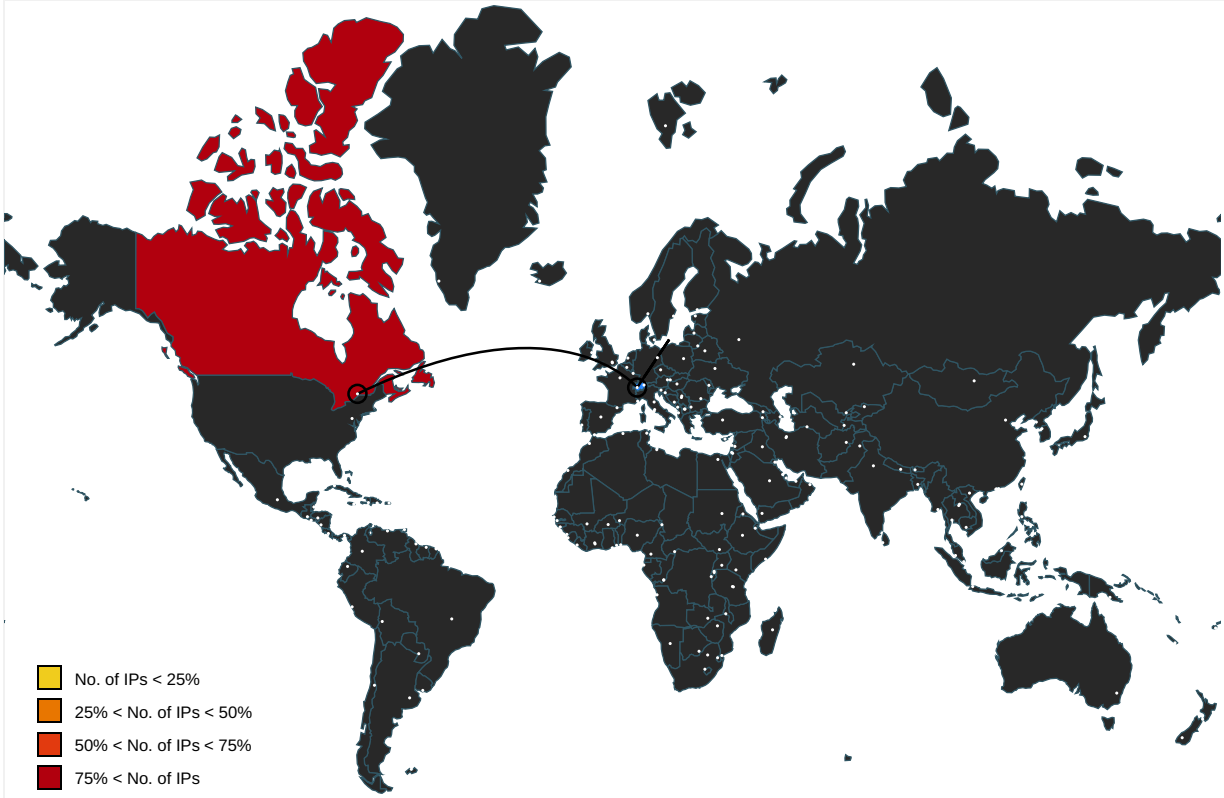
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	VJNPltkyHyI3CCo.exe, 00000002.00000002.469579413.0000000003071000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://iykmoreentrprise.org	VJNPltkyHyI3CCo.exe, 00000002.00000002.472217023.0000000003330000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	VJNPltkyHyI3CCo.exe, 00000001.00000002.216437484.0000000007702000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	VJNPltkyHyI3CCo.exe, 00000001.00000002.216437484.0000000007702000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	VJNPltkyHyI3CCo.exe, 00000001.00000002.216437484.0000000007702000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://DynDns.comDynDNS	VJNPltkyHyI3CCo.exe, 00000002.00000002.469579413.00000000030 71000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comF	VJNPltkyHyI3CCo.exe, 00000001.00000002.211437768.00000000014F7000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	VJNPltkyHyI3CCo.exe, 00000001.00000002.216437484.00000000077 02000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	VJNPltkyHyI3CCo.exe, 00000001.00000002.216437484.00000000077 02000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.letsencrypt.org0	VJNPltkyHyI3CCo.exe, 00000002.00000002.474666607.00000000064 20000.00000004.00000001.sdmp	false	• URL Reputation: safe • 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	VJNPltkyHyI3CCo.exe, 00000002.00000002.469579413.00000000030 71000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	VJNPltkyHyI3CCo.exe, 00000001.00000002.216437484.00000000077 02000.00000004.00000001.sdmp	false		high
http://https://api.ipify.org%(	VJNPltkyHyI3CCo.exe, 00000002.00000002.469579413.00000000030 71000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.tiro.com	VJNPltkyHyI3CCo.exe, 00000001.00000002.216437484.00000000077 02000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	VJNPltkyHyI3CCo.exe, 00000001.00000002.216437484.00000000077 02000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	VJNPltkyHyI3CCo.exe, 00000001.00000002.216437484.00000000077 02000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comFM	VJNPltkyHyI3CCo.exe, 00000001.00000002.211437768.00000000014F7000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	VJNPltkyHyI3CCo.exe, 00000001.00000002.212033159.00000000035 11000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	VJNPltkyHyI3CCo.exe, 00000001.00000002.216437484.00000000077 02000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://r3.i.lencr.org/0	VJNPltkyHyI3CCo.exe, 00000002.00000002.474666607.00000000064 20000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	VJNPltkyHyI3CCo.exe, 00000001.00000002.216437484.00000000077 02000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	VJNPltkyHyI3CCo.exe, 00000001.00000002.216437484.00000000077 02000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	VJNPltkyHyI3CCo.exe, 00000001.00000002.216437484.00000000077 02000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	VJNPltkyHyI3CCo.exe, 00000001.00000002.216437484.00000000077 02000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	VJNPltkyHyI3CCo.exe, 00000001.00000002.216437484.00000000077 02000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	VJNPltkyHyI3CCo.exe, 00000001.00000002.216437484.00000000077 02000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	VJNPltkyHyI3CCo.exe, 00000001.00000003.200177966.000000000645C000.00000004.00000001.sdmp, VJNPltkyHyI3CCo.exe, 00000001.00000003.199446008.000000000646 1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	VJNPltkyHyI3CCo.exe, 00000001.00000002.216437484.000000000770 2000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	VJNPltkyHyI3CCo.exe, 00000001.00000002.216437484.000000000770 2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://r3.o.lencr.org0	VJNPltkyHyI3CCo.exe, 00000002.00000002.474666607.000000000642 0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	VJNPltkyHyI3CCo.exe, 00000001.00000002.216437484.000000000770 2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	VJNPltkyHyI3CCo.exe, 00000001.00000002.216437484.000000000770 2000.00000004.00000001.sdmp	false		high
http://https://api.ipify.org%GETMozilla/5.0	VJNPltkyHyI3CCo.exe, 00000002.00000002.469579413.000000000307 1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://GTAZqk.com	VJNPltkyHyI3CCo.exe, 00000002.00000002.469579413.000000000307 1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	VJNPltkyHyI3CCo.exe, 00000001.00000003.198143597.000000000646B000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	VJNPltkyHyI3CCo.exe, 00000001.00000002.216437484.000000000770 2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	VJNPltkyHyI3CCo.exe, 00000001.00000002.216437484.000000000770 2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	VJNPltkyHyI3CCo.exe, 00000001.00000002.216437484.000000000770 2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://A84D2ljcLQUVG1tA.net	VJNPltkyHyI3CCo.exe, 00000002.00000002.469579413.000000000307 1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	VJNPltkyHyI3CCo.exe, 00000001.00000002.211954442.000000000034C1000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comttva4	VJNPltkyHyI3CCo.exe, 00000001.00000002.211437768.000000000014F7000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	VJNPltkyHyI3CCo.exe, 00000001.00000002.216437484.000000000770 2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	VJNPltkyHyI3CCo.exe, 00000001.00000002.212559557.000000000465E000.00000004.00000001.sdmp, VJNPltkyHyI3CCo.exe, 00000002.00000002.464818672.000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mail.iykmoreentrprise.org	VJNPltkyHyI3CCo.exe, 00000002.00000002.472217023.000000000333 0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://cps.root-x1.letsencrypt.org0	VJNPltkyHyI3CCo.exe, 00000002.00000002.472254348.000000000333 8000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
66.70.204.222	iykmoreentrprise.org	Canada		16276	OVHFR	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385435
Start date:	12.04.2021
Start time:	14:20:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	VJNPltkyHyI3CCo.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:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/1@2/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0%) • Quality average: 43.3% • Quality standard deviation: 30.7%
HCA Information:	• Successful, ratio: 98% • 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, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 93.184.220.29, 168.61.161.212, 104.43.139.144, 104.42.151.234, 13.107.42.23, 13.107.5.88, 20.82.209.183, 184.30.24.56, 40.88.32.150, 92.122.213.194, 92.122.213.247, 20.54.26.129, 13.88.21.125, 13.64.90.137, 2.17.179.193, 84.53.167.113 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, client-office365-tas.msedge.net, ocos-office365-s2s.msedge.net, arc.msn.com.nsatc.net, config.edge.skype.com.trafficmanager.net, e-0009.e-msedge.net, config-edge-skype.l-0014.l-msedge.net, l-0014.config.skype.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, e15275.g.akamaiedge.net, arc.msn.com, cdn.onenote.net.edgekey.net, skypedataprdcoleus15.cloudapp.net, ocsp.digicert.com, wildcard.weather.microsoft.com.edgekey.net, www-bing-com.dual-a-0001.a-msedge.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, cdn.onenote.net, config.edge.skype.com, www.bing.com, skypedataprdcolwus17.cloudapp.net, afdo-tas-offload.trafficmanager.net, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, tile-service.weather.microsoft.com, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, ocos-office365-s2s-msedge-net.e-0009.e-msedge.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, blobcollector.events.data.trafficmanager.net, e1553.dspg.akamaiedge.net, l-0014.l-msedge.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:21:06	API Interceptor	793x Sleep call for process: VJNPltkyHyI3CCo.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
66.70.204.222	0L2qr7kJMh40sxq.exe	Get hash	malicious	Browse	
	ApuE9QrdQxe7Um6.exe	Get hash	malicious	Browse	
	77iET1jNLJyV8ez.exe	Get hash	malicious	Browse	
	bOkrXdoYekZPyWI.exe	Get hash	malicious	Browse	
	ayZYB5SkqMPA06M.exe	Get hash	malicious	Browse	
	fyZ6iHys7CIIHFR.exe	Get hash	malicious	Browse	
	uMLNLd9kgPez84h.exe	Get hash	malicious	Browse	
	YQfInBo2DDpDfIX.exe	Get hash	malicious	Browse	
	ORDER 700198.exe	Get hash	malicious	Browse	
	sZJd8ClputxKLHL.exe	Get hash	malicious	Browse	
	MZE1fH3FADpILLo.exe	Get hash	malicious	Browse	
	I5aSXk7QgcVm507.exe	Get hash	malicious	Browse	
	H6KJ04yw37dsJsX.exe	Get hash	malicious	Browse	
	hyUBmXyIgoC5I09.exe	Get hash	malicious	Browse	
	3i8aJ4R0PXl4wT3.exe	Get hash	malicious	Browse	
	AKBEsuPu9JfDXz3.exe	Get hash	malicious	Browse	
	9W5K7OGmYCsPbcT.exe	Get hash	malicious	Browse	
	c3oWuf8mb3ix7MY.exe	Get hash	malicious	Browse	
	QAhqxmnssOm5ho4.exe	Get hash	malicious	Browse	
	Z2YtRnoxRhFt3lk.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	SecuriteInfo.com.Trojan.MinerNET.8.21400.exe	Get hash	malicious	Browse	• 51.255.34.118
	Anmodning om tilbud 12-04-2021#U00b7pdf.exe	Get hash	malicious	Browse	• 51.195.53.221
	PAYMENT COPY.exe	Get hash	malicious	Browse	• 167.114.6.31
	Swift copy.pdf.exe	Get hash	malicious	Browse	• 51.222.80.112
	PO-4147074_pdf.exe	Get hash	malicious	Browse	• 51.195.53.221
	kQVi54bTM0.exe	Get hash	malicious	Browse	• 5.196.102.93
	cym4u.exe	Get hash	malicious	Browse	• 188.165.17.91
	Statement-ID-(400603).vbs	Get hash	malicious	Browse	• 51.89.204.5
	$108,459.00.html	Get hash	malicious	Browse	• 146.59.152.166
	LtfVNumoON.exe	Get hash	malicious	Browse	• 144.217.30.204
	giATspz5dw.exe	Get hash	malicious	Browse	• 142.4.204.181
	SecuriteInfo.com.__vbaHresultCheckObj.21994.exe	Get hash	malicious	Browse	• 149.202.83.171
	SecuriteInfo.com.Variant.Johnnie.321295.17359.exe	Get hash	malicious	Browse	• 91.121.140.167
	fileshare.doc	Get hash	malicious	Browse	• 188.165.24 5.148
	SecuriteInfo.com.Variant.Bulz.421173.18141.exe	Get hash	malicious	Browse	• 51.89.77.2
	R1210322PIR-2FQUOTATION(P21C00285).exe	Get hash	malicious	Browse	• 51.38.214.75
	Notice of change schedule for CID_ CMA CGM AMBER 0 QA8FS1NC 0QA8GN1NC - 1st Rev.pdf.exe	Get hash	malicious	Browse	• 51.195.53.221
	Notice of change schedule for CID_ CMA CGM AMBER 0 QA8FS1NC 0QA8GN1NC - 1st Rev.pdf_1.exe	Get hash	malicious	Browse	• 51.195.53.221
	Purchase Order No.10056.exe	Get hash	malicious	Browse	• 51.195.53.221
	Quotation_pdf.exe	Get hash	malicious	Browse	• 51.195.53.221

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\VJNPltkyHyI3CCo.exe.log	
Process:	C:\Users\user\Desktop\VJNPltkyHyI3CCo.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.803865308867252
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	VJNPltkyHyI3CCo.exe
File size:	836608
MD5:	36a7049a4f3be8788f0c844319a5364b
SHA1:	fbefd649daddd22154920dcae7dc79f8d6a036ff
SHA256:	20251c86adaf2dc2cf0513e3dc83e78a768d1b016e0dcd738a0e55d3ba7227c4
SHA512:	aaf5d36c7322e2f050debb26289f208dbd1388b1a980c7e0616ba4b7df42e95f60b382c3f5b88e9b1b4794c169d90332a19327230f0b011f13b7f595c4a40020
SSDEEP:	12288:z63pA3f95jKm8HAKA1bBSxvVa6VsOMG6e46bXxec0N4iAhAMLsguzxWYTlK:qpa4m8HAKA3SNqG6jgvCyyhdxWYTs
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....t`.....P.....^.... .....@.. .... @.....

File Icon

Icon Hash:	9c9ee4f0f2d2d2da

Static PE Info

General

Entrypoint:	0x4bc35e

General

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:	0x6074018F [Mon Apr 12 08:15:11 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
or dword ptr [edx], ecx
or eax, 00000020h
add byte ptr [ecx+49h], cl
sub al, byte ptr [eax]
add byte ptr [eax], al
add byte ptr [eax], al
dec ebp
dec ebp
add byte ptr [edx], ch
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbc30c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbe000	0x11a3c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd0000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0xba37c	0xba400	False	0.920096214346	data	7.9009190253	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xbe000	0x11a3c	0x11c00	False	0.507840008803	data	5.85054037808	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd0000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xbe100	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0xce938	0x14	data		
RT_VERSION	0xce95c	0x3a4	data		
RT_MANIFEST	0xced10	0xd25	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

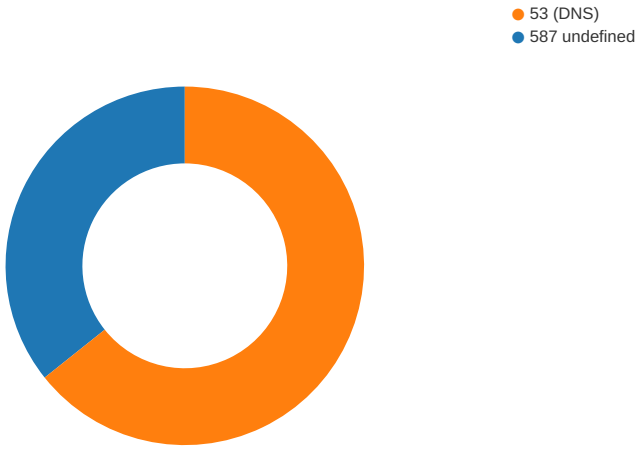
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Adobe Inc, Sel 2011 - 2021
Assembly Version	1.0.0.0
InternalName	SpecialNameAttribute.exe
FileVersion	1.0.0.0
CompanyName	Adobe Inc, Sel
LegalTrademarks	
Comments	
ProductName	Image Studio
ProductVersion	1.0.0.0
FileDescription	Image Studio
OriginalFilename	SpecialNameAttribute.exe

Network Behavior

Network Port Distribution

Total Packets: 56



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:22:50.436736107 CEST	49741	587	192.168.2.3	66.70.204.222
Apr 12, 2021 14:22:50.570462942 CEST	587	49741	66.70.204.222	192.168.2.3
Apr 12, 2021 14:22:50.570601940 CEST	49741	587	192.168.2.3	66.70.204.222
Apr 12, 2021 14:22:50.833848953 CEST	587	49741	66.70.204.222	192.168.2.3
Apr 12, 2021 14:22:50.834433079 CEST	49741	587	192.168.2.3	66.70.204.222
Apr 12, 2021 14:22:50.970660925 CEST	587	49741	66.70.204.222	192.168.2.3
Apr 12, 2021 14:22:50.971146107 CEST	49741	587	192.168.2.3	66.70.204.222
Apr 12, 2021 14:22:51.106420994 CEST	587	49741	66.70.204.222	192.168.2.3
Apr 12, 2021 14:22:51.156291962 CEST	49741	587	192.168.2.3	66.70.204.222
Apr 12, 2021 14:22:51.221162081 CEST	49741	587	192.168.2.3	66.70.204.222
Apr 12, 2021 14:22:51.361119032 CEST	587	49741	66.70.204.222	192.168.2.3
Apr 12, 2021 14:22:51.361181974 CEST	587	49741	66.70.204.222	192.168.2.3
Apr 12, 2021 14:22:51.361213923 CEST	587	49741	66.70.204.222	192.168.2.3
Apr 12, 2021 14:22:51.361365080 CEST	49741	587	192.168.2.3	66.70.204.222
Apr 12, 2021 14:22:51.373605967 CEST	49741	587	192.168.2.3	66.70.204.222
Apr 12, 2021 14:22:51.507543087 CEST	587	49741	66.70.204.222	192.168.2.3
Apr 12, 2021 14:22:51.562681913 CEST	49741	587	192.168.2.3	66.70.204.222
Apr 12, 2021 14:22:51.779840946 CEST	49741	587	192.168.2.3	66.70.204.222
Apr 12, 2021 14:22:51.913562059 CEST	587	49741	66.70.204.222	192.168.2.3
Apr 12, 2021 14:22:51.916742086 CEST	49741	587	192.168.2.3	66.70.204.222
Apr 12, 2021 14:22:52.050908089 CEST	587	49741	66.70.204.222	192.168.2.3
Apr 12, 2021 14:22:52.052015066 CEST	49741	587	192.168.2.3	66.70.204.222
Apr 12, 2021 14:22:52.197036028 CEST	587	49741	66.70.204.222	192.168.2.3
Apr 12, 2021 14:22:52.197877884 CEST	49741	587	192.168.2.3	66.70.204.222
Apr 12, 2021 14:22:52.334011078 CEST	587	49741	66.70.204.222	192.168.2.3
Apr 12, 2021 14:22:52.334661961 CEST	49741	587	192.168.2.3	66.70.204.222
Apr 12, 2021 14:22:52.491643906 CEST	587	49741	66.70.204.222	192.168.2.3
Apr 12, 2021 14:22:52.492017984 CEST	49741	587	192.168.2.3	66.70.204.222
Apr 12, 2021 14:22:52.625983000 CEST	587	49741	66.70.204.222	192.168.2.3
Apr 12, 2021 14:22:52.632345915 CEST	49741	587	192.168.2.3	66.70.204.222
Apr 12, 2021 14:22:52.632644892 CEST	49741	587	192.168.2.3	66.70.204.222
Apr 12, 2021 14:22:52.632867098 CEST	49741	587	192.168.2.3	66.70.204.222
Apr 12, 2021 14:22:52.633090019 CEST	49741	587	192.168.2.3	66.70.204.222
Apr 12, 2021 14:22:52.768244028 CEST	587	49741	66.70.204.222	192.168.2.3
Apr 12, 2021 14:22:52.768296003 CEST	587	49741	66.70.204.222	192.168.2.3
Apr 12, 2021 14:22:52.768328905 CEST	587	49741	66.70.204.222	192.168.2.3
Apr 12, 2021 14:22:52.768359900 CEST	587	49741	66.70.204.222	192.168.2.3
Apr 12, 2021 14:22:52.770149946 CEST	587	49741	66.70.204.222	192.168.2.3
Apr 12, 2021 14:22:52.812777996 CEST	49741	587	192.168.2.3	66.70.204.222

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:20:54.282417059 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:20:54.360526085 CEST	53	64938	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:20:54.747649908 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:20:54.796515942 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 12, 2021 14:20:55.078618050 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:20:55.128582001 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 12, 2021 14:21:02.091650963 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:21:02.150515079 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 12, 2021 14:21:03.015203953 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:21:03.077584982 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 12, 2021 14:21:05.027339935 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:21:05.076035023 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 12, 2021 14:21:05.965487957 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:21:06.014250994 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 12, 2021 14:21:07.100564957 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:21:07.149406910 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 12, 2021 14:21:08.059403896 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:21:08.116575956 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 12, 2021 14:21:25.293231010 CEST	58722	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:21:25.299341917 CEST	56596	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:21:25.300570965 CEST	64101	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:21:25.344033003 CEST	53	58722	8.8.8.8	192.168.2.3
Apr 12, 2021 14:21:25.348047972 CEST	53	56596	8.8.8.8	192.168.2.3
Apr 12, 2021 14:21:25.349284887 CEST	53	64101	8.8.8.8	192.168.2.3
Apr 12, 2021 14:21:28.104584932 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:21:28.157736063 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 12, 2021 14:21:34.428991079 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:21:34.487699986 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 12, 2021 14:21:39.763340950 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:21:39.816123009 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 12, 2021 14:21:40.961142063 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:21:41.018534899 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 12, 2021 14:21:41.914843082 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:21:41.967256069 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 12, 2021 14:21:42.952872038 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:21:43.019298077 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 12, 2021 14:21:44.368967056 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:21:44.432106972 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 12, 2021 14:21:47.789033890 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:21:47.837738037 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 12, 2021 14:21:54.222506046 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:21:54.293562889 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 12, 2021 14:22:04.008586884 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:22:04.057455063 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 12, 2021 14:22:07.453449965 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:22:07.522109985 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 12, 2021 14:22:18.253395081 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:22:18.302119970 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 12, 2021 14:22:39.251099110 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:22:39.303725958 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 12, 2021 14:22:41.328479052 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:22:41.396962881 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 12, 2021 14:22:47.999886036 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:22:48.048607111 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 12, 2021 14:22:49.165318012 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:22:49.216259956 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 12, 2021 14:22:50.113877058 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:22:50.220279932 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 12, 2021 14:22:50.244390011 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:22:50.301708937 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 12, 2021 14:22:56.786207914 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:22:56.834899902 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 12, 2021 14:23:01.025154114 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:23:01.075602055 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 12, 2021 14:23:02.307183027 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:23:02.367217064 CEST	53	61292	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 14:23:04.606638908 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:23:04.656563997 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 12, 2021 14:23:12.221443892 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:23:12.222440004 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 12, 2021 14:23:12.281131983 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 12, 2021 14:23:12.282808065 CEST	53	64938	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 14:22:50.113877058 CEST	192.168.2.3	8.8.8.8	0x7377	Standard query (0)	mail.iykmoreentrprise.org	A (IP address)	IN (0x0001)
Apr 12, 2021 14:22:50.244390011 CEST	192.168.2.3	8.8.8.8	0x5d52	Standard query (0)	mail.iykmoreentrprise.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 14:22:50.220279932 CEST	8.8.8.8	192.168.2.3	0x7377	No error (0)	mail.iykmoreentrprise.org	iykmoreentrprise.org		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:22:50.220279932 CEST	8.8.8.8	192.168.2.3	0x7377	No error (0)	iykmoreentrprise.org		66.70.204.222	A (IP address)	IN (0x0001)
Apr 12, 2021 14:22:50.301708937 CEST	8.8.8.8	192.168.2.3	0x5d52	No error (0)	mail.iykmoreentrprise.org	iykmoreentrprise.org		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 14:22:50.301708937 CEST	8.8.8.8	192.168.2.3	0x5d52	No error (0)	iykmoreentrprise.org		66.70.204.222	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 12, 2021 14:22:50.833848953 CEST	587	49741	66.70.204.222	192.168.2.3	220-server.wlcserver.com ESMTP Exim 4.94 #2 Mon, 12 Apr 2021 16:22:50 +0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Apr 12, 2021 14:22:50.834433079 CEST	49741	587	192.168.2.3	66.70.204.222	EHLO 134349
Apr 12, 2021 14:22:50.970660925 CEST	587	49741	66.70.204.222	192.168.2.3	250-server.wlcserver.com Hello 134349 [84.17.52.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-X_PIPE_CONNECT 250-STARTTLS 250 HELP
Apr 12, 2021 14:22:50.971146107 CEST	49741	587	192.168.2.3	66.70.204.222	STARTTLS
Apr 12, 2021 14:22:51.106420994 CEST	587	49741	66.70.204.222	192.168.2.3	220 TLS go ahead

Code Manipulations

Statistics

Behavior

● VJNPltkyHyI3CCo.exe
● VJNPltkyHyI3CCo.exe

Click to jump to process

System Behavior

Analysis Process: VJNPltkyHyI3CCo.exe PID: 1156 Parent PID: 5624

General

Start time:	14:21:01
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\VJNPltkyHyI3CCo.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\VJNPltkyHyI3CCo.exe'
Imagebase:	0xf20000
File size:	836608 bytes
MD5 hash:	36A7049A4F3BE8788F0C844319A5364B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.212033159.0000000003511000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.212559557.000000000465E000.00000004.00000001.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	6E11CF06	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	6E11CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\VJNPltkyHyI3CCo.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E42C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\VJNPltkyHyI3CCo.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6E42C907	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	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF61B4F	ReadFile

Analysis Process: VJNPltkyHyI3CCo.exe PID: 748 Parent PID: 1156

General

Start time:	14:21:07
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\VJNPltkyHyI3CCo.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\VJNPltkyHyI3CCo.exe
Imagebase:	0xb20000
File size:	836608 bytes
MD5 hash:	36A7049A4F3BE8788F0C844319A5364B

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: 00000002.00000002.464818672.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.469579413.0000000003071000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.469579413.0000000003071000.00000004.00000001.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	6E11CF06	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	6E11CF06	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	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF61B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CF61B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11168	success or wait	1	6CF61B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\0607d547-57a0-41db-8ed4-1c4eb4b0c0ed	unknown	4096	success or wait	1	6CF61B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11168	success or wait	1	6CF61B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CF61B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CF61B4F	ReadFile

Disassembly

Code Analysis