ID: 321421
Sample Name: Shipping-Document.com
Cookbook: default.jbs
Time: 22:20:25
Date: 21/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

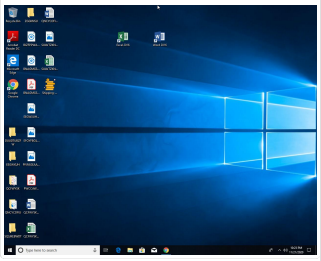
Analysis Report Shipping-Document.com

Overview

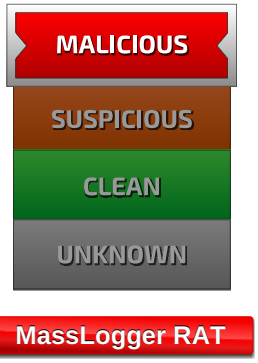
General Information

Sample Name:	Shipping-Document.com (renamed file extension from com to exe)
Analysis ID:	321421
MD5:	47f1684c0075aea.
SHA1:	7198622c341f1f6..
SHA256:	58ba104e01f9650.

Most interesting Screenshot:



Detection

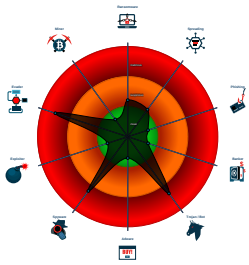


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected MassLogger RAT
- .NET source code references suspic…
- 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 video device inform…
- Tries to detect sandboxes and other…
- Tries to harvest and steal browser in…
- Tries to steal Mail credentials (via fil…

Classification



Startup

- **System is w10x64**
- Shipping-Document.exe (PID: 1364 cmdline: 'C:\Users\user\Desktop\Shipping-Document.exe' MD5: 47F1684C0075AEA74BB225586D55B6E3)
  - Shipping-Document.exe (PID: 3420 cmdline: C:\Users\user\Desktop\Shipping-Document.exe MD5: 47F1684C0075AEA74BB225586D55B6E3)
  - Shipping-Document.exe (PID: 1488 cmdline: C:\Users\user\Desktop\Shipping-Document.exe MD5: 47F1684C0075AEA74BB225586D55B6E3)
- vlc.exe (PID: 1748 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe' MD5: 47F1684C0075AEA74BB225586D55B6E3)
  - vlc.exe (PID: 2792 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: 47F1684C0075AEA74BB225586D55B6E3)
  - vlc.exe (PID: 6052 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: 47F1684C0075AEA74BB225586D55B6E3)
  - vlc.exe (PID: 1872 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: 47F1684C0075AEA74BB225586D55B6E3)
  - vlc.exe (PID: 4472 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: 47F1684C0075AEA74BB225586D55B6E3)
  - vlc.exe (PID: 5352 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: 47F1684C0075AEA74BB225586D55B6E3)
  - vlc.exe (PID: 1256 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: 47F1684C0075AEA74BB225586D55B6E3)
- vlc.exe (PID: 3440 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe' MD5: 47F1684C0075AEA74BB225586D55B6E3)
  - vlc.exe (PID: 1012 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: 47F1684C0075AEA74BB225586D55B6E3)
  - vlc.exe (PID: 4832 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: 47F1684C0075AEA74BB225586D55B6E3)
  - vlc.exe (PID: 484 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe MD5: 47F1684C0075AEA74BB225586D55B6E3)
- **cleanup**

Malware Configuration

Threatname: MassLogger

```
{
  "Config: ": [
    "00000000 -> <|| v2.4.0.0 ||>",
    "User Name: user",
    "IP: 84.17.52.25",
    "Location: United States",
    "Windows OS: Microsoft Windows 10 Pro 64bit",
    "Windows Serial Key: VG7NF-BJ77Y-WRF7X-GJVW7-H3M8T",
    "CPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz",
    "GPU: Microsoft Basic Display Adapter",
    "AV: Windows Defender",
    "Screen Resolution: 1280x1024",
    "Current Time: 11/21/2020 10:23:00 PM",
    "MassLogger Started: 11/21/2020 10:22:56 PM",
    "Interval: 2 hour",
    "MassLogger Process: C:\\Users\\user\\AppData\\Roaming\\Microsoft\\Windows\\Start Menu\\Programs\\VideoLAN\\vlc.exe",
    "MassLogger Melt: false",
    "MassLogger Exit after delivery: false",
    "As Administrator: True",
    "Processes:",
    "Name:nrsfQCpnoELUtpNHbSOcsFhHJG, Title:Chrome",
    "Name:nrsfQCpnoELUtpNHbSOcsFhHJG, Title:Chrome",
    "Name:nrsfQCpnoELUtpNHbSOcsFhHJG, Title:Chrome",
    "Name:nrsfQCpnoELUtpNHbSOcsFhHJG, Title:Chrome",
    "Name:nrsfQCpnoELUtpNHbSOcsFhHJG, Title:Chrome",
    "Name:nrsfQCpnoELUtpNHbSOcsFhHJG, Title:Chrome",
    "Name:nrsfQCpnoELUtpNHbSOcsFhHJG, Title:Chrome",
    "Name:nrsfQCpnoELUtpNHbSOcsFhHJG, Title:Chrome",
    "Name:nrsfQCpnoELUtpNHbSOcsFhHJG, Title:Chrome",
    "Name:nrsfQCpnoELUtpNHbSOcsFhHJG, Title:Chrome",
    "Name:nrsfQCpnoELUtpNHbSOcsFhHJG, Title:Chrome",
    "<|| WD Exclusion ||>",
    "Disabled",
    "<|| Binder ||>",
    "Disabled",
    "<|| Downloader ||>",
    "Disabled",
    "<|| Window Searcher ||>",
    "Disabled",
    "<|| Bot Killer ||>",
    "Disabled",
    "<|| Search And Upload ||>",
    "Disabled",
    "<|| Telegram Desktop ||>",
    "Not Installed",
    "<|| Pidgin ||>",
    "Not Installed",
    "<|| FileZilla ||>",
    "Not Installed",
    "<|| Discord Tokken ||>",
    "Not Installed",
    "<|| NordVPN ||>",
    "Not Installed",
    "<|| Outlook ||>",
    "Not Installed",
    "<|| FoxMail ||>",
    "Not Installed",
    "<|| Thunderbird ||>",
    "Not Installed",
    "<|| FireFox ||>",
    "Not Installed",
    "<|| QQ Browser ||>",
    "Not Installed",
    "<|| Chromium Recovery ||>",
    "Not Installed or Not Found",
    "<|| Keylogger And Clipboard ||>",
    "NA"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000016.00000002.484501673.0000000002B51000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000001A.00000002.484549006.0000000002F71000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.292894367.0000000003997000.00000004.00000001.sdmp	JoeSecurity_MassLogger	Yara detected MassLogger RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000016.00000002.474961619.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_MassLogger	Yara detected MassLogger RAT	Joe Security	
0000000C.00000003.392005702.00000000048A 0000.00000004.00000001.sdmp	JoeSecurity_MassLogger	Yara detected MassLogger RAT	Joe Security	
Click to see the 23 entries				

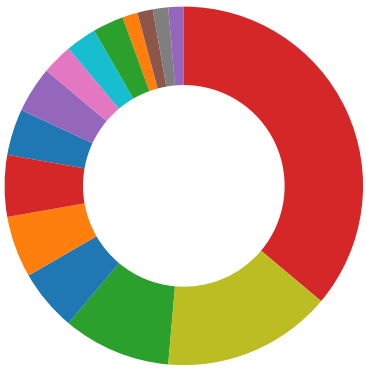
Unpacked PEs

Source	Rule	Description	Author	Strings
26.2.vlc.exe.400000.0.unpack	JoeSecurity_MassLogger	Yara detected MassLogger RAT	Joe Security	
5.2.Shipping-Document.exe.400000.0.unpack	JoeSecurity_MassLogger	Yara detected MassLogger RAT	Joe Security	
22.2.vlc.exe.400000.0.unpack	JoeSecurity_MassLogger	Yara detected MassLogger RAT	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Spreading
- Networking
- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Networking:

May check the online IP address of the machine

System Summary:

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Yara detected Costura Assembly Loader

Malware Analysis System Evasion:

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

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

HIPS / PFW / Operating System Protection Evasion:

.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected MassLogger RAT

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

Tries to steal Mail credentials (via file access)

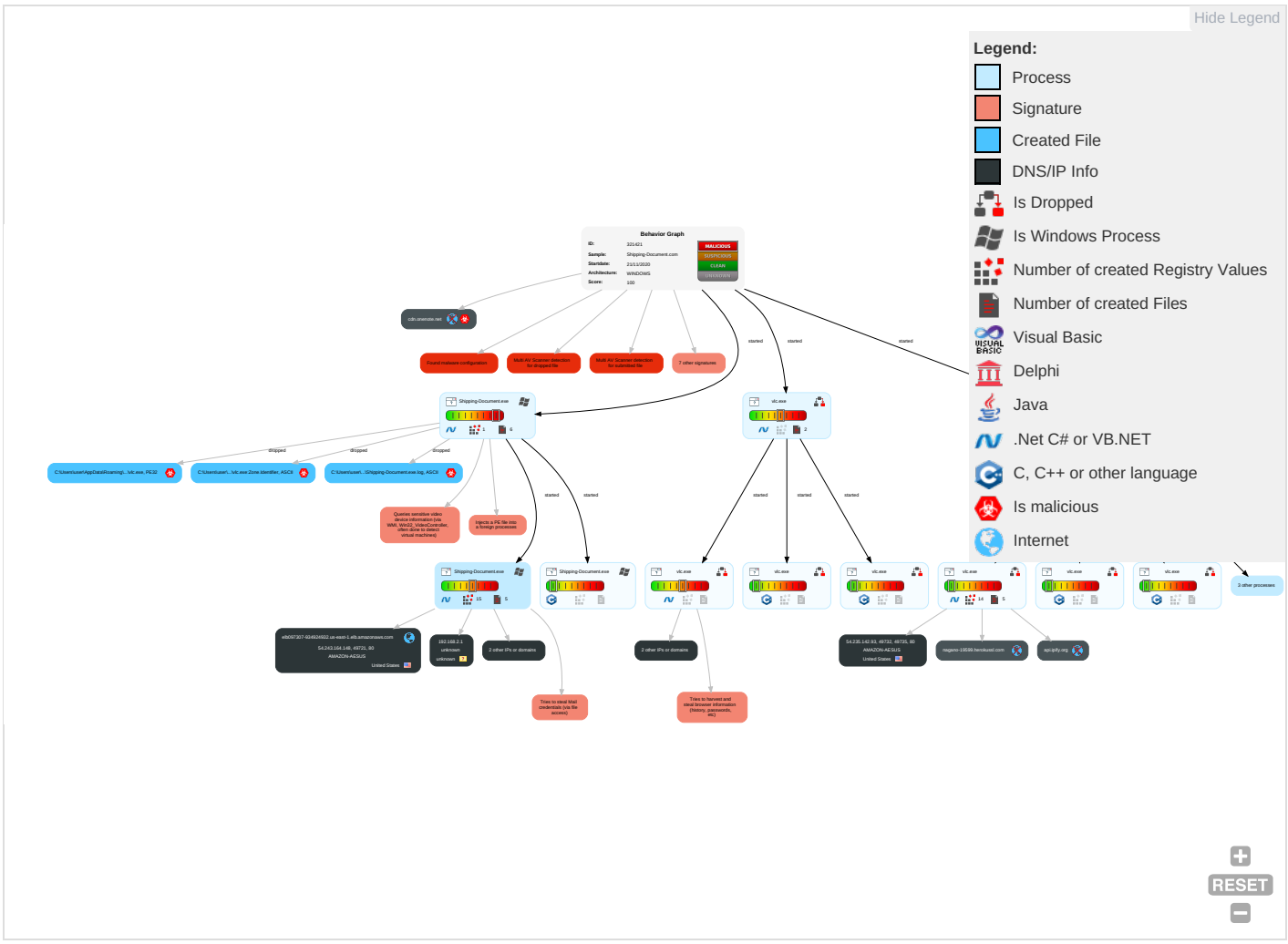
Remote Access Functionality:

Yara detected MassLogger RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 1 2 1	Registry Run Keys / Startup Folder 1 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	Native API 1	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1 1	Obfuscated Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Masquerading 1	Security Account Manager	System Information Discovery 2 5	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 1 3	NTDS	Security Software Discovery 3 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1 2	LSA Secrets	Virtualization/Sandbox Evasion 1 3	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Owner/User 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	Remote System 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	System Network Configuration Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol

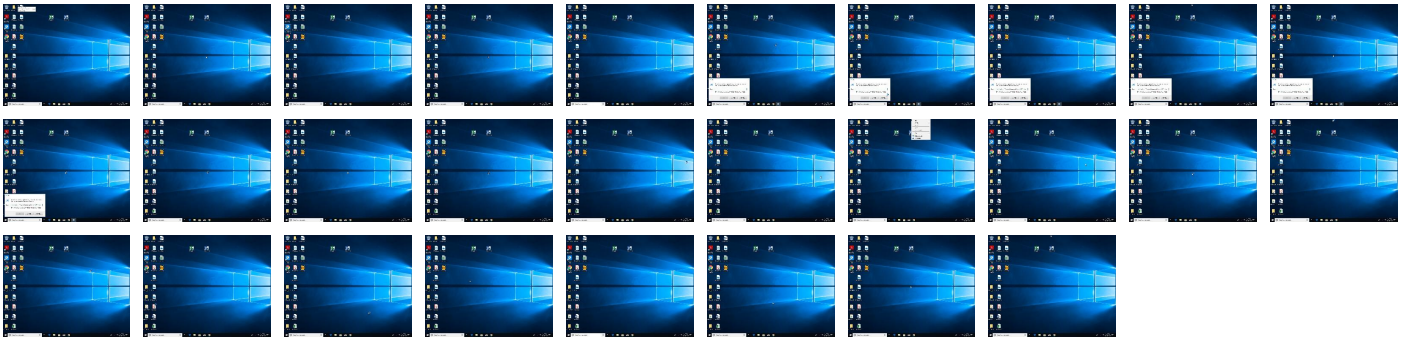
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Shipping-Document.exe	21%	Virustotal		Browse
Shipping-Document.exe	5%	Metadefender		Browse
Shipping-Document.exe	21%	ReversingLabs	Win32.Trojan.Generic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	21%	Virustotal		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	5%	Metadefender		Browse
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	21%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
26.2.vlc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1139343		Download File
5.2.Shipping-Document.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1139343		Download File
22.2.vlc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1139343		Download File

Domains

Source	Detection	Scanner	Label	Link
cdn.onenote.net	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
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://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://api.ipify8	0%	URL Reputation	safe	
http://api.ipify8	0%	URL Reputation	safe	
http://api.ipify8	0%	URL Reputation	safe	
http://api.ipify8	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://api.ipify8v	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://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	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://api.ipify.orgD	0%	URL Reputation	safe	
http://api.ipify.orgD	0%	URL Reputation	safe	
http://api.ipify.orgD	0%	URL Reputation	safe	
http://api.ipify.orgD	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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.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.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://www.sakkal.com	0%	URL Reputation	safe	
http://api.ipify8R	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
elb097307-934924932.us-east-1.elb.amazonaws.com	54.243.164.148	true	false		high
api.ipify.org	unknown	unknown	false		high
cdn.onenote.net	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://api.ipify.org/	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	Shipping-Document.exe, 00000000.00000002.297409828.000000005850000.00000002.00000001.sdmp, vlc.exe, 0000000C.00000002.405013728.0000000006110000.00000002.00000001.sdmp, vlc.exe, 0000000E.00000002.426931776.00000000055D0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	Shipping-Document.exe, 00000000.00000002.297409828.000000005850000.00000002.00000001.sdmp, vlc.exe, 0000000C.00000002.405013728.0000000006110000.00000002.00000001.sdmp, vlc.exe, 0000000E.00000002.426931776.00000000055D0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	Shipping-Document.exe, 00000000.00000002.297409828.000000005850000.00000002.00000001.sdmp, vlc.exe, 0000000C.00000002.405013728.0000000006110000.00000002.00000001.sdmp, vlc.exe, 0000000E.00000002.426931776.00000000055D0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	Shipping-Document.exe, 00000000.00000002.297409828.000000005850000.00000002.00000001.sdmp, vlc.exe, 0000000C.00000002.405013728.0000000006110000.00000002.00000001.sdmp, vlc.exe, 0000000E.00000002.426931776.00000000055D0000.00000002.00000001.sdmp	false		high

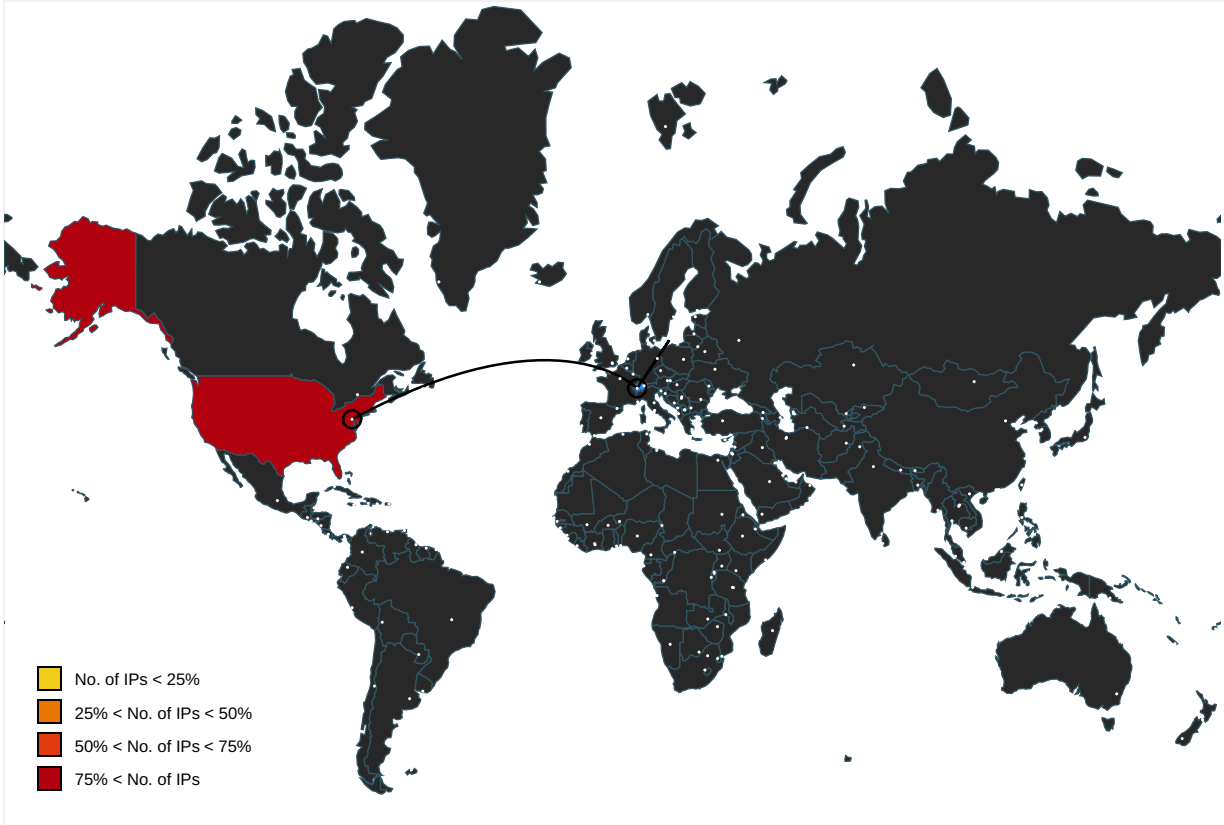
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	Shipping-Document.exe, 00000000.00000002.297409828.000000005850000.00000002.00000001.sdmp, vlc.exe, 0000000C.00000002.405013728.0000000006110000.00000002.00000001.sdmp, vlc.exe, 0000000E.00000002.426931776.00000000055D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Shipping-Document.exe, 00000000.00000002.297409828.000000005850000.00000002.00000001.sdmp, vlc.exe, 0000000C.00000002.405013728.0000000006110000.00000002.00000001.sdmp, vlc.exe, 0000000E.00000002.426931776.00000000055D0000.00000002.00000001.sdmp	false		high
http://api.ipify.org/p	Shipping-Document.exe, 00000005.00000002.484657984.0000000002EDA000.00000004.00000001.sdmp, vlc.exe, 00000016.00000002.485932807.0000000002D0F000.00000004.00000001.sdmp, vlc.exe, 0000001A.00000002.485514489.0000000003130000.00000004.00000001.sdmp	false		high
http://www.tiro.com	vlc.exe, 0000000E.00000002.426931776.00000000055D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://elb097307-934924932.us-east-1.elb.amazonaws.com	Shipping-Document.exe, 00000005.00000002.485116357.0000000002FB4000.00000004.00000001.sdmp, vlc.exe, 00000016.00000002.486045579.0000000002D20000.00000004.00000001.sdmp, vlc.exe, 0000001A.00000002.485599592.0000000003142000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers	vlc.exe, 0000000E.00000002.426931776.00000000055D0000.00000002.00000001.sdmp	false		high
http://api.ipify8	vlc.exe, 0000001A.00000002.485514489.0000000003130000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.goodfont.co.kr	Shipping-Document.exe, 00000000.00000002.297409828.000000005850000.00000002.00000001.sdmp, vlc.exe, 0000000C.00000002.405013728.0000000006110000.00000002.00000001.sdmp, vlc.exe, 0000000E.00000002.426931776.00000000055D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://api.ipify8v	Shipping-Document.exe, 00000005.00000002.485070930.0000000002FAF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	Shipping-Document.exe, 00000000.00000002.297409828.000000005850000.00000002.00000001.sdmp, vlc.exe, 0000000C.00000002.405013728.0000000006110000.00000002.00000001.sdmp, vlc.exe, 0000000E.00000002.426931776.00000000055D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://api.ipify.org	Shipping-Document.exe, 00000005.00000002.485116357.0000000002FB4000.00000004.00000001.sdmp, vlc.exe, 00000016.00000002.484501673.0000000002B51000.00000004.00000001.sdmp, vlc.exe, 0000001A.00000002.484549006.0000000002F71000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	Shipping-Document.exe, 00000000.00000002.297409828.000000005850000.00000002.00000001.sdmp, vlc.exe, 0000000C.00000002.405013728.0000000006110000.00000002.00000001.sdmp, vlc.exe, 0000000E.00000002.426931776.00000000055D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Shipping-Document.exe, 00000000.00000002.297409828.000000005850000.00000002.00000001.sdmp, vlc.exe, 0000000C.00000002.405013728.0000000006110000.00000002.00000001.sdmp, vlc.exe, 0000000E.00000002.426931776.00000000055D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Shipping-Document.exe, 00000000.00000002.297409828.000000005850000.00000002.00000001.sdmp, vlc.exe, 0000000C.00000002.405013728.0000000006110000.00000002.00000001.sdmp, vlc.exe, 0000000E.00000002.426931776.00000000055D0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Shipping-Document.exe, 00000000.00000002.297409828.000000005850000.00000002.00000001.sdmp, vlc.exe, 0000000C.00000002.405013728.0000000006110000.00000002.00000001.sdmp, vlc.exe, 0000000E.00000002.426931776.00000000055D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Shipping-Document.exe, 00000000.00000002.297409828.000000005850000.00000002.00000001.sdmp, vlc.exe, 0000000C.00000002.405013728.0000000006110000.00000002.00000001.sdmp, vlc.exe, 0000000E.00000002.426931776.00000000055D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Shipping-Document.exe, 00000000.00000002.297409828.000000005850000.00000002.00000001.sdmp, vlc.exe, 0000000C.00000002.405013728.0000000006110000.00000002.00000001.sdmp, vlc.exe, 0000000E.00000002.426931776.00000000055D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Shipping-Document.exe, 00000000.00000002.297409828.000000005850000.00000002.00000001.sdmp, vlc.exe, 0000000C.00000002.405013728.0000000006110000.00000002.00000001.sdmp, vlc.exe, 0000000E.00000002.426931776.00000000055D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://api.ipify.orgD	Shipping-Document.exe, 00000005.00000002.483989726.0000000002DE1000.00000004.00000001.sdmp, vlc.exe, 00000016.00000002.484501673.0000000002B51000.00000004.00000001.sdmp, vlc.exe, 000001A.00000002.484549006.00000000002F71000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Shipping-Document.exe, 00000000.00000002.297409828.000000005850000.00000002.00000001.sdmp, vlc.exe, 0000000C.00000002.405013728.0000000006110000.00000002.00000001.sdmp, vlc.exe, 0000000E.00000002.426931776.00000000055D0000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	Shipping-Document.exe, 00000000.00000002.297409828.000000005850000.00000002.00000001.sdmp, vlc.exe, 0000000C.00000002.405013728.0000000006110000.00000002.00000001.sdmp, vlc.exe, 0000000E.00000002.426931776.00000000055D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Shipping-Document.exe, 00000000.00000002.297409828.000000005850000.00000002.00000001.sdmp, vlc.exe, 0000000C.00000002.405013728.0000000006110000.00000002.00000001.sdmp, vlc.exe, 0000000E.00000002.426931776.00000000055D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://api.ipify.org/P	Shipping-Document.exe, 00000005.00000002.484657984.0000000002EDA000.00000004.00000001.sdmp, vlc.exe, 00000016.00000002.485932807.0000000002D0F000.00000004.00000001.sdmp, vlc.exe, 000001A.00000002.485514489.0000000003130000.00000004.00000001.sdmp	false		high
http://www.codeplex.com/DotNetZip	vlc.exe, 0000001A.00000002.488438717.0000000004091000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers8	Shipping-Document.exe, 00000000.00000002.297409828.000000005850000.00000002.00000001.sdmp, vlc.exe, 0000000C.00000002.405013728.0000000006110000.00000002.00000001.sdmp, vlc.exe, 0000000E.00000002.426931776.00000000055D0000.00000002.00000001.sdmp	false		high
http://https://www.youtube.com/watch?v=Qxk6cu21JSg	Shipping-Document.exe, 00000005.00000002.483989726.0000000002DE1000.00000004.00000001.sdmp, vlc.exe, 00000016.00000002.484501673.0000000002B51000.00000004.00000001.sdmp, vlc.exe, 000001A.00000002.484549006.0000000002F71000.00000004.00000001.sdmp	false		high
http://www.fonts.com	Shipping-Document.exe, 00000000.00000002.297409828.000000005850000.00000002.00000001.sdmp, vlc.exe, 0000000C.00000002.405013728.0000000006110000.00000002.00000001.sdmp, vlc.exe, 0000000E.00000002.426931776.00000000055D0000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	Shipping-Document.exe, 00000000.00000002.297409828.000000005850000.00000002.00000001.sdmp, vlc.exe, 0000000C.00000002.405013728.0000000006110000.00000002.00000001.sdmp, vlc.exe, 0000000E.00000002.426931776.00000000055D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Shipping-Document.exe, 00000000.00000002.297409828.000000005850000.00000002.00000001.sdmp, vlc.exe, 0000000C.00000002.405013728.0000000006110000.00000002.00000001.sdmp, vlc.exe, 0000000E.00000002.426931776.00000000055D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Shipping-Document.exe, 00000000.00000002.297409828.000000005850000.00000002.00000001.sdmp, vlc.exe, 0000000C.00000002.405013728.0000000006110000.00000002.00000001.sdmp, vlc.exe, 0000000E.00000002.426931776.00000000055D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • 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	Shipping-Document.exe, 00000005.00000002.483989726.000000002DE1000.00000004.00000001.sdmp, vlc.exe, 00000016.00000002.484501673.0000000002B51000.00000004.00000001.sdmp, vlc.exe, 0000001A.00000002.484549006.0000000002F71000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	Shipping-Document.exe, 00000000.00000002.297409828.000000005850000.00000002.00000001.sdmp, vlc.exe, 0000000C.00000002.405013728.0000000006110000.00000002.00000001.sdmp, vlc.exe, 0000000E.00000002.426931776.0000000055D0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://api.ipify8R	vlc.exe, 00000016.00000002.486012293.0000000002D1B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
54.243.164.148	unknown	United States		14618	AMAZON-AESUS	false
54.235.142.93	unknown	United States		14618	AMAZON-AESUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond

Analysis ID:	321421
Start date:	21.11.2020
Start time:	22:20:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Shipping-Document.com (renamed file extension from com to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	34
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@25/10@7/3
EGA Information:	• Successful, ratio: 80%
HDC Information:	• Successful, ratio: 0.4% (good quality ratio 0.4%) • Quality average: 71.6% • Quality standard deviation: 29.9%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 104.43.139.144, 51.11.168.160, 2.20.142.209, 2.20.142.210, 51.104.139.180, 92.122.213.194, 92.122.213.247, 20.54.26.129, 92.122.145.220, 104.108.60.202, 84.53.167.113 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, ris-prod.trafficmanager.net, tile-service.weather.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, a1449.dscg2.akamai.net, e15275.g.akamaiedge.net, arc.msn.com, cdn.onenote.net.edgekey.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, store-images.s-microsoft.com, wildcard.weather.microsoft.com.edgekey.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, e1553.dspg.akamaiedge.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net • Execution Graph export aborted for target Shipping-Document.exe, PID 3420 because there are no executed function • 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 NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
22:21:51	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run vlc "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe"
22:21:59	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run vlc "C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe"
22:22:14	API Interceptor	561x Sleep call for process: Shipping-Document.exe modified
22:22:52	API Interceptor	379x Sleep call for process: vlc.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54.243.164.148	1119_673423.doc	Get hash	malicious	Browse	• api.ipify.org/
	Rewgjqjhqwqn8.exe	Get hash	malicious	Browse	• api.ipify.org/
	i3gRY0HYZn.exe	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	mWKfVsuSZAHcuCc.exe	Get hash	malicious	Browse	• api.ipify.org/
	Catalogue.exe	Get hash	malicious	Browse	• api.ipify.org/
54.235.142.93	RVAgYSH2qh.exe	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	BUILDING ORDER_PROPERTY SPECS.exe	Get hash	malicious	Browse	• api.ipify.org/
	1118_8732615.doc	Get hash	malicious	Browse	• api.ipify.org/
	XN33CLWH.EXE	Get hash	malicious	Browse	• api.ipify.org/
	AI-Hbb_Doc-EUR_Pdf.exe	Get hash	malicious	Browse	• api.ipify.org/
	YV2q4nAPVQ.exe	Get hash	malicious	Browse	• api.ipify.org/
	1105_748543.doc	Get hash	malicious	Browse	• api.ipify.org/
	174028911-035110-sanlccjavap0004-1.exe	Get hash	malicious	Browse	• api.ipify.org/
	RFQ-NOV-2020.exe	Get hash	malicious	Browse	• api.ipify.org/
	OZmn6gKEgi.exe	Get hash	malicious	Browse	• api.ipify.org/
	WFDKJ4wsQ6.exe	Get hash	malicious	Browse	• api.ipify.org/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
elb097307-934924932.us-east-1.elb.amazonaws.com	QRN-CLJC-06112020149.PDF.exe	Get hash	malicious	Browse	• 54.243.161.145
	yQDGREHA9h.exe	Get hash	malicious	Browse	• 54.235.83.248
	mcsrXx9lfD.exe	Get hash	malicious	Browse	• 54.235.83.248
	SecuriteInfo.com.Trojan.PackedNET.461.20928.exe	Get hash	malicious	Browse	• 23.21.42.25
	Defender-update-kit-x86x64.exe	Get hash	malicious	Browse	• 54.225.153.147
	http://https://largemail.r1.rpost.net/files/7xU97qcFgCvB3Uv1wDC4qvS2ZriLfublohKWA5V3/ln/en-us	Get hash	malicious	Browse	• 54.225.66.103
	ORDER.exe	Get hash	malicious	Browse	• 54.235.142.93
	Bill # 2.xlsx	Get hash	malicious	Browse	• 23.21.42.25
	PO1.xlsx	Get hash	malicious	Browse	• 174.129.214.20
	a7UZzCVWKO.exe	Get hash	malicious	Browse	• 54.204.14.42
	QKLQkaCe9M.exe	Get hash	malicious	Browse	• 50.19.252.36
	sAPuJAvs52.exe	Get hash	malicious	Browse	• 54.243.161.145
	JlgyVmPWZr.exe	Get hash	malicious	Browse	• 174.129.214.20
	EIUOzWW2JX.exe	Get hash	malicious	Browse	• 174.129.214.20
	RVAgYSH2qh.exe	Get hash	malicious	Browse	• 54.235.142.93
	yCyc4rN0u8.exe	Get hash	malicious	Browse	• 54.235.83.248
	9cXAnovmQX.exe	Get hash	malicious	Browse	• 54.225.66.103
	T2HDck1Mmy.exe	Get hash	malicious	Browse	• 54.235.142.93
	Purchase Order.exe	Get hash	malicious	Browse	• 54.225.66.103

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Payment Advice Note from 19.11.2020.exe	Get hash	malicious	Browse	• 23.21.126.66

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	QRN-CLJC-06112020149.PDF.exe	Get hash	malicious	Browse	• 54.243.161.145
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 52.71.133.130
	Purchase Order 40,7045.exe	Get hash	malicious	Browse	• 54.208.77.124
	Fennec Pharma .docx	Get hash	malicious	Browse	• 54.84.56.113
	Fennec Pharma .docx	Get hash	malicious	Browse	• 54.84.56.113
	Fennec Pharma.xlsx	Get hash	malicious	Browse	• 54.84.56.113
	Fennec Pharma.xlsx	Get hash	malicious	Browse	• 54.84.56.113
	http://https://albanesebros.sendx.io/lp/shared-doc.html	Get hash	malicious	Browse	• 3.213.165.33
	http://www.openair.com	Get hash	malicious	Browse	• 34.202.206.65
	http://https://faxfax.zizera.com/remittanceadvice	Get hash	malicious	Browse	• 184.73.218.177
	http://webnavigator.co	Get hash	malicious	Browse	• 34.235.7.64
	http://https://mcmms.typeform.com/to/Vtnb9OBC	Get hash	malicious	Browse	• 34.200.62.85
	yQDGREHA9h.exe	Get hash	malicious	Browse	• 54.235.83.248
	mcsrXx9lfD.exe	Get hash	malicious	Browse	• 54.235.83.248
	SecuriteInfo.com.Trojan.PackedNET.461.20928.exe	Get hash	malicious	Browse	• 23.21.42.25
	Defender-update-kit-x86x64.exe	Get hash	malicious	Browse	• 54.225.153.147
	http://https://largemail.r1.rpost.net/files/7xU97qcFgCvB3Uv1wDC4qvS2ZriLfublohKWA5V3/ln/en-us	Get hash	malicious	Browse	• 54.225.66.103
	ORDER.exe	Get hash	malicious	Browse	• 54.235.142.93
	http://s1022.t.en25.com/e/er?s=1022&lid=2184&elqTrackId=BEDFF87609C7D9DEAD041308DD8FFFB8&lb_email=bkirwer%40farbestfoods.com&elq=b095bd096fb54161953a2cf8316b5d13&elqaid=3115&elqat=1	Get hash	malicious	Browse	• 52.1.99.77
	Bill # 2.xlsx	Get hash	malicious	Browse	• 23.21.42.25
AMAZON-AESUS	QRN-CLJC-06112020149.PDF.exe	Get hash	malicious	Browse	• 54.243.161.145
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 52.71.133.130
	Purchase Order 40,7045.exe	Get hash	malicious	Browse	• 54.208.77.124
	Fennec Pharma .docx	Get hash	malicious	Browse	• 54.84.56.113
	Fennec Pharma .docx	Get hash	malicious	Browse	• 54.84.56.113
	Fennec Pharma.xlsx	Get hash	malicious	Browse	• 54.84.56.113
	Fennec Pharma.xlsx	Get hash	malicious	Browse	• 54.84.56.113
	http://https://albanesebros.sendx.io/lp/shared-doc.html	Get hash	malicious	Browse	• 3.213.165.33
	http://www.openair.com	Get hash	malicious	Browse	• 34.202.206.65
	http://https://faxfax.zizera.com/remittanceadvice	Get hash	malicious	Browse	• 184.73.218.177
	http://webnavigator.co	Get hash	malicious	Browse	• 34.235.7.64
	http://https://mcmms.typeform.com/to/Vtnb9OBC	Get hash	malicious	Browse	• 34.200.62.85
	yQDGREHA9h.exe	Get hash	malicious	Browse	• 54.235.83.248
	mcsrXx9lfD.exe	Get hash	malicious	Browse	• 54.235.83.248
	SecuriteInfo.com.Trojan.PackedNET.461.20928.exe	Get hash	malicious	Browse	• 23.21.42.25
	Defender-update-kit-x86x64.exe	Get hash	malicious	Browse	• 54.225.153.147
	http://https://largemail.r1.rpost.net/files/7xU97qcFgCvB3Uv1wDC4qvS2ZriLfublohKWA5V3/ln/en-us	Get hash	malicious	Browse	• 54.225.66.103
	ORDER.exe	Get hash	malicious	Browse	• 54.235.142.93
	http://s1022.t.en25.com/e/er?s=1022&lid=2184&elqTrackId=BEDFF87609C7D9DEAD041308DD8FFFB8&lb_email=bkirwer%40farbestfoods.com&elq=b095bd096fb54161953a2cf8316b5d13&elqaid=3115&elqat=1	Get hash	malicious	Browse	• 52.1.99.77
	Bill # 2.xlsx	Get hash	malicious	Browse	• 23.21.42.25

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\AEC365839D\Log.txt	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1800
Entropy (8bit):	5.4448188256893255
Encrypted:	false
SSDEEP:	24:GSZnNMZxaXok+/RV3kdZzM0f2uVM/viyJ1WhnGyJkdEiPv5J80:GSFAg+/RV3OZI0uuu6MchGJj5J80
MD5:	C34F8BF4E27BB68FA0108BC5A5712E24
SHA1:	FC0B4511A39BD5178205D175D4C548ACED69AF23
SHA-256:	D11FCFABCA1A007F95CCB792F723CF6CC6DE29816E16F50330EAC19D4F54127D
SHA-512:	DA6ECBCBC7F93487951101755D70B52404BAB1AA2EC3513B809DE2E9830FF9E153FCC608773BBB6ABA17706462F3DD3243A19A1F5F9449153949207D7AE8B1F
Malicious:	false
Reputation:	low
Preview:	<|| v2.4.0.0 ||>..User Name: user..IP: 84.17.52.25..Location: United States..Windows OS: Microsoft Windows 10 Pro 64bit..Windows Serial Key: VG7NF-BJ77Y-WRF7X-GJVW7-H3M8T..CPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz..GPU: Microsoft Basic Display Adapter..AV: Windows Defender ..Screen Resolution: 1280x1024..Current Time: 11/21/2020 10:23:00 PM..MassLogger Started: 11/21/2020 10:22:56 PM..Interval: 2 hour..MassLogger Process: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe..MassLogger Melt: false..MassLogger Exit after delivery: false..As Administrator: True..Processes:..Name:nrsfQCpnoELUtpNHbSOcsFhHJG, Title:Chrome..Name:nrsfQCpnoELUtpNHbSOcsFhHJG, Title:Chrome..Name:nrsfQCpnoELUtpNHbSOcsFhHJG, Title:Chrome..Name:nrsfQCpnoELUtpNHbSOcsFhHJG, Title:Chrome..Name:nrsfQCpnoELUtpNHbSOcsFhHJG, Title:Chrome..Name:nrsfQCpnoELUtpNHbSOcsFhHJG, Title:Chrome..Name:nrsf

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Shipping-Document.exe.log	
Process:	C:\Users\user\Desktop\Shipping-Document.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1119
Entropy (8bit):	5.356708753875314
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzd
MD5:	3197B1D4714B56F2A6AC9E83761739AE
SHA1:	3B38010F0DF51C1D4D2C020138202DABB686741D
SHA-256:	40586572180B85042FEFED9F367B43831C5D269751D9F3940BBC29B41E18E9F6
SHA-512:	58EC975A53AD9B19B425F6C6843A94CC280F794D436BBF3D29D8B76CA1E8C2D8883B3E754F9D4F2C9E9387FE88825CCD9919369A5446B1AFF73EDBE07FA94D8
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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\vlc.exe.log	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1119
Entropy (8bit):	5.356708753875314
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzd
MD5:	3197B1D4714B56F2A6AC9E83761739AE
SHA1:	3B38010F0DF51C1D4D2C020138202DABB686741D
SHA-256:	40586572180B85042FEFED9F367B43831C5D269751D9F3940BBC29B41E18E9F6
SHA-512:	58EC975A53AD9B19B425F6C6843A94CC280F794D436BBF3D29D8B76CA1E8C2D8883B3E754F9D4F2C9E9387FE88825CCD9919369A5446B1AFF73EDBE07FA94D8
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\vlc.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\Temp\DotNetZip-3hg33bsx.tmp	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	1313
Entropy (8bit):	7.043036922524586
Encrypted:	false
SSDEEP:	24:9wqN/6fFjxKN/Ujj9/ewfbBI6Dt8kme/F0yZhFiR0/xnxN/UjjbZIKN/6fFjGZHb:9xN6NjoNUjj9/PDBHx8kme/7MR8xxNUV
MD5:	DBCE34334D5F6D7582E247A4101BD020
SHA1:	C0D92A5B3A595721D0708901B4EDA33306DAC714
SHA-256:	6CB6784E1A1BB42526FAC9DC4A7EA512EABE2764078BDEE866FC0126A25C4E30
SHA-512:	539FBA7D05E7481FBF47A58DB79CA5B74B706C0646BB23AE62F314DFBAF355395F5A16986D9B969B922FF111066045BFC63672DA79185BA64D72CAF08D4C9FE
Malicious:	false
Reputation:	low
Preview:	PK.....uQ.....2.$.user_United States_AEC365839D_11-21-2020 22.23.4/.. .....v....PK.....uQ.....9.$.user_United States_AEC365839D_11-21-2020 22.23.4/Log.txt.. .....[o.0...#.;..V.,d.*...@[...6..$..0qd;.N|..@..F...<..|.?...l.....`...:#...|...\G.\.../..W~.r.....*f0.....[4.3.q...<..tD..Q3..k...VP*N.}c...../...r.....?r.~..= ..O.....uj....._BMi..v.} ;.J...B..''...~.Q.F.P.&...*.O.j...Q_.g.G....B..C....>...m.._$....[..,K..g.~..(B..a$..q..7...srH....X.].vl..^s....J.....aPcAV.....T...-....D<.....s..q.....+..E..]..k..q... .f\.....g$.".b...U.....c5.J3....0...S.....=.I.5.<...h.7?Q*.DV[h.....g...I..)...{..9t-.Tbt .bw.O...s,..p}..4V....AUe.AH...~7T..FIv.il...[E..,J.T.....r.....\.g.....$.3...*..P-.x.Y..q.{.xL.TjyN..t..g. ."..4.::..F.u.xz...yu..Ih.E"].P.U6.N...."CC...FzY.~.e.I.L.?*....7PK.....uQ.....9.$.user_United States_AEC365839D_11-21-2020 22.23.4/Log.txt.. .....

C:\Users\user\AppData\Local\Temp\DotNetZip-4b2ut3ef.tmp	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	1317
Entropy (8bit):	7.031494974591168
Encrypted:	false
SSDEEP:	24:93NzHNzdj6ETBEVZ/EVKkC71ETR6PaSAEjw1kaOIrENzSZXNzlZJpNzTil:93pHplrlGZ/XHXiPEjw11apSZXplZvpK
MD5:	8132E6EA831C1B6BE4BD2291AADB6039
SHA1:	D976FFAA6CD0E120B8776CFAFB09D7B716ADEEC6
SHA-256:	F530344314CBD18FAD28D37A886B9597EC8DA7497B13EFD859A0D1048CC68F0C
SHA-512:	E61875E84C19AD02AFAB345922335F8CF709F15CD19074A3688122617160ACE1E0E785A346F334B335A8B703FC88DB3360BDABE869CD4E326E9272B10FFCFD1
Malicious:	false
Reputation:	low
Preview:	PK.....uQ.....3.$.user_United States_AEC365839D_11-21-2020 22.22.58/.. .....}....PK.....uQ.....:.$.user_United States_AEC365839D_11-21-2020 22.22.58/Log.txt.. .....[o.0...#.;..V.,d. ...e@[Bi.mS^Lr...G.C.....J..0M.....s...v.k.X.zE....32...W.`.u..un....b.R.....tU.P..Q",.0..q..Hb.l.a. ..VF.,..%..Z.uy*..;@-..{|a0 nWz.B..R.Y.<.*?...R.|..C.i.G.n.....J..0...p}.y..(....R...7.unD.MaR._....v....5q.IL.. ..<.Q2.Z....e.i.....T*}...|."d..J..\'..t.|N.)?..t.-Wwl..^s.....a.`a^.....-..._.d...._#.w.B.I.....+..E..[.k..q...PZ.3..{.....g$.b.b.....c5.J3....0...S...&.{wd.^g:x.Lk.k..TZ....j.....7.&.S$3C.j?s.Z...@.....\k..D*.....i.p.->.....n.%1.....%.F.YZ...9.M..././.H..-!..I.g.:?R:..Z...Q.~...Y... ....g. ."..4.:>..F.u.x|...yu..Ih.E"[.P.T>.N...."CK...FzY.~...IH.N.?*.....PK.....uQ.BW.....:.$.user_United States_AEC365839D_11-21-2020 22.22.58/Log.txt.. .....

C:\Users\user\AppData\Local\Temp\DotNetZip-fu3v0fes.tmp	
Process:	C:\Users\user\Desktop\Shipping-Document.exe
File Type:	Zip archive data, at least v2.0 to extract
Category:	dropped
Size (bytes):	1297
Entropy (8bit):	7.030906938500873
Encrypted:	false
SSDEEP:	24:9rNmNTbeBs5whYIPS9u3ShMBoyoINsn/CbuuKmmNTUZLNUZfzNTs:9rIN76OIPS9uiioyTNsn/CadmmNUZL6g
MD5:	018370A0F32AFAE7CD5FA0B7CA08BF33
SHA1:	F4A3ABD2679619E0476A65D01D090B6F97064F27
SHA-256:	C48C00649DE76CF63D8ED975D6C6926F5E12E46559EFD3F329AF19576AAFF383
SHA-512:	226DCA9CBBF1B4EF9B207D3316B256791FB9D60E954F4655FE6339E1FD64BCFED526B12988DC0AB85A05FB69F4D23F038BA492C49DCBBEAFA432F773AE1647 9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\DotNetZip-fu3v0fes.tmp	
Preview:	PK.....uQ.....3.$.user_United States_AEC365839D_11-21-2020 22.22.19/.. .....PK.....uQ.....:.$.user_United States_AEC365839D_11-21-2020 22.22.19/Log.txt.. .....h.....h.....mo.0...G.w...4X...j.....%.6..$.X.8...N|.]...F...)yu....;..b...\){e....32.....`.u..u...j..._-.....unU.P..Q",.0..q..Hb.d.n.'"...[8X}..Z.ye&..;D-...\|f0.T..R.Z.Q.<...K...Z.~..B.i.F.....J.I.;...p~.y..(...:]R...7..nD.-aR.....v.....k.....w.a...x@.d....j.....B(.,...~/.(B.....1.j. ...My....Ym..A.G....T.~.....1..l.W.Lw.....J..HS.,J-.ek.V.....Ci..4...a...l.Q.G..X.P..".jn.f.../j.0..].D..}3M.....lx....{..D...Ys.....&...4F&-.O.....~.P....@4.....S".p}.4-....A.e.FH...~7..Fi~.q,D.....a{.O..c.....x!...-$.$I....#.c..j.E..D.....R.U. ..q!..p..u.....\|.....4X..8..n...4k#...#,(z...V$.....by9.R.3._.....7PK.....uQ.A.S}.....:.$.user_United States_AEC365839D_11-21-2020 22.22.19/Log.txt.. .....h.....h.....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe	
Process:	C:\Users\user\Desktop\Shipping-Document.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1631688
Entropy (8bit):	4.471355537934198
Encrypted:	false
SSDEEP:	24576:rZpGi0JaVRMk7p5aYo6KdumheNUSlt2TZ+rSY6GJX1Vgsms38jZcPuUdlZTkLmuD:W
MD5:	47F1684C0075AEA74BB225586D55B6E3
SHA1:	7198622C341F1F6982EB20AC7A431508289DF924
SHA-256:	58BA104E01F9650518E256C03102A8105428E761988CE5905DE77CD45A53AD90
SHA-512:	863AF48BCE8E913D01E43EF0DD6BE8CA683D2B37EFA36AF9F517F76AEC6D99D6975F9797A8069996C591E06737AB3E978FFEAAD6612DE27C285202FD2B0D028A
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 21%, Browse • Antivirus: Metadefender, Detection: 5%, Browse • Antivirus: ReversingLabs, Detection: 21%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._..... ... .@.. .....@.....`...K.... ..p.....9..... ..... ..H.....text..... ..... ..`.rsrc...p.... .....@..@.reloc.....@..B.....H.....>..03.....q.....0..?.....(....8...8.....E.....8....*.(.... ....:....& ....8.....0..d..... .....8.....E.....0...{...I...[.....8.....{....o....(....(....& ....(....:....&8..... ....(....:....&8.....(....& ....8.....Y.. ....(....9k...& ....8`.....(....(....&8 ....{....o....(..... .....8*...*(#... ....(....9....& ....8....8?... ....(....9....&8.... T...(....8.....{....(....(....o..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Shipping-Document.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	4.471355537934198
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Shipping-Document.exe
File size:	1631688
MD5:	47f1684c0075aea74bb225586d55b6e3
SHA1:	7198622c341f1f6982eb20ac7a431508289df924

General

SHA256:	58ba104e01f9650518e256c03102a8105428e761988ce5905de77cd45a53ad90
SHA512:	863af48bce8e913d01e43ef0dd6be8ca683d2b37efa36af9f517f76aec6d99d6975f9797a8069996c591e06737ab3e978ffeaad6612de27c285202fd2b0d028a
SSDEEP:	24576:rZpGi0JaVRMk7p5aYo6KdumheNUSIt2TZ+rSY6GJX1Vgsms38jZcPuUdIZTkLmuD:W
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..... ....@.. ..... @.....

File Icon

Icon Hash:	3dfce089e4c4d4e4

Static PE Info

General

Entrypoint:	0x570bae
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FB8C219 [Sat Nov 21 07:30:33 2020 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

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=DigiCert Assured ID Code Signing CA-1, OU=www.digicert.com, O=DigiCert Inc, C=US
Signature Validation Error:	**The digital signature of the object did not verify**
Error Number:	-2146869232
Not Before, Not After	• 11/7/2019 4:00:00 PM 11/16/2022 4:00:00 AM
Subject Chain	• CN=Google LLC, O=Google LLC, L=Mountain View, S=California, C=US
Version:	3
Thumbprint MD5:	463BFA4FA69A9E6C4D8813CCFAAF16EE
Thumbprint SHA-1:	A3958AE522F3C54B878B20D7B0F63711E08666B2
Thumbprint SHA-256:	5F2F2840C6E51D17F09334ADA05D9DCDD9AEEB11AF0AE163816757D539ABE3EE
Serial:	06AEA76BAC46A9E8CFE6D29E45AAF033

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x170b60	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x172000	0x1ba70	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x18ac00	0x39c8	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x18e000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x16ebb4	0x16ec00	False	0.47218960357	data	4.03017385847	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x172000	0x1ba70	0x1bc00	False	0.202509149775	data	5.19563928652	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x18e000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x172220	0x2320	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x174540	0x10828	dBase III DBT, version number 0, next free block index 40		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x184d68	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x188f90	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x18b538	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 4473920		
RT_ICON	0x18c5e0	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x18ca48	0x5a	data		
RT_VERSION	0x18caa4	0x374	data		
RT_MANIFEST	0x18ce18	0xc55	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

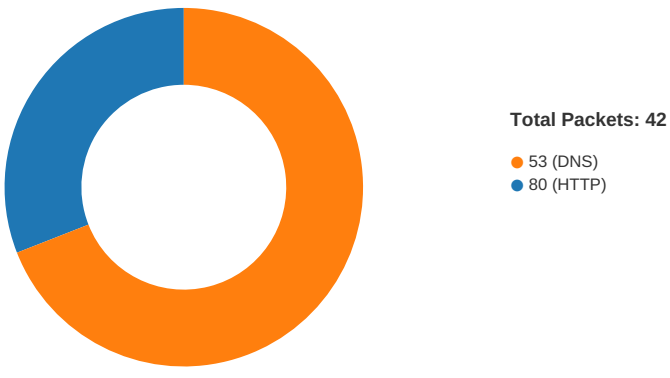
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018 Google LLC
Assembly Version	1.3.35.451
InternalName	Ulzzwremyvkd6.exe
FileVersion	1.3.35.451
CompanyName	Google LLC
Comments	Google Installer
ProductName	Google Update
ProductVersion	1.3.35.451
FileDescription	Google Installer
OriginalFilename	Ulzzwremyvkd6.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 22:22:00.762152910 CET	49721	80	192.168.2.3	54.243.164.148
Nov 21, 2020 22:22:00.864978075 CET	80	49721	54.243.164.148	192.168.2.3
Nov 21, 2020 22:22:00.865180016 CET	49721	80	192.168.2.3	54.243.164.148
Nov 21, 2020 22:22:00.866674900 CET	49721	80	192.168.2.3	54.243.164.148
Nov 21, 2020 22:22:00.969307899 CET	80	49721	54.243.164.148	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 22:22:00.976836920 CET	80	49721	54.243.164.148	192.168.2.3
Nov 21, 2020 22:22:01.021373034 CET	49721	80	192.168.2.3	54.243.164.148
Nov 21, 2020 22:22:49.953600883 CET	49732	80	192.168.2.3	54.235.142.93
Nov 21, 2020 22:22:50.056014061 CET	80	49732	54.235.142.93	192.168.2.3
Nov 21, 2020 22:22:50.056130886 CET	49732	80	192.168.2.3	54.235.142.93
Nov 21, 2020 22:22:50.056575060 CET	49732	80	192.168.2.3	54.235.142.93
Nov 21, 2020 22:22:50.158710003 CET	80	49732	54.235.142.93	192.168.2.3
Nov 21, 2020 22:22:50.164937019 CET	80	49732	54.235.142.93	192.168.2.3
Nov 21, 2020 22:22:50.212912083 CET	49732	80	192.168.2.3	54.235.142.93
Nov 21, 2020 22:22:58.560981989 CET	49735	80	192.168.2.3	54.235.142.93
Nov 21, 2020 22:22:58.664211988 CET	80	49735	54.235.142.93	192.168.2.3
Nov 21, 2020 22:22:58.664439917 CET	49735	80	192.168.2.3	54.235.142.93
Nov 21, 2020 22:22:58.665633917 CET	49735	80	192.168.2.3	54.235.142.93
Nov 21, 2020 22:22:58.768011093 CET	80	49735	54.235.142.93	192.168.2.3
Nov 21, 2020 22:22:58.773164034 CET	80	49735	54.235.142.93	192.168.2.3
Nov 21, 2020 22:22:58.921525002 CET	49735	80	192.168.2.3	54.235.142.93
Nov 21, 2020 22:23:00.887444973 CET	80	49721	54.243.164.148	192.168.2.3
Nov 21, 2020 22:23:00.888092041 CET	49721	80	192.168.2.3	54.243.164.148

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 22:21:09.186827898 CET	64185	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:21:09.222868919 CET	53	64185	8.8.8.8	192.168.2.3
Nov 21, 2020 22:21:09.993848085 CET	65110	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:21:10.031853914 CET	53	65110	8.8.8.8	192.168.2.3
Nov 21, 2020 22:21:10.809195995 CET	58361	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:21:10.836564064 CET	53	58361	8.8.8.8	192.168.2.3
Nov 21, 2020 22:21:13.862592936 CET	63492	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:21:13.889771938 CET	53	63492	8.8.8.8	192.168.2.3
Nov 21, 2020 22:21:14.660721064 CET	60831	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:21:14.687913895 CET	53	60831	8.8.8.8	192.168.2.3
Nov 21, 2020 22:21:15.488516092 CET	60100	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:21:15.515783072 CET	53	60100	8.8.8.8	192.168.2.3
Nov 21, 2020 22:21:16.470161915 CET	53195	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:21:16.497458935 CET	53	53195	8.8.8.8	192.168.2.3
Nov 21, 2020 22:21:17.383024931 CET	50141	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:21:17.410284996 CET	53	50141	8.8.8.8	192.168.2.3
Nov 21, 2020 22:21:18.664967060 CET	53023	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:21:18.700856924 CET	53	53023	8.8.8.8	192.168.2.3
Nov 21, 2020 22:21:19.479413033 CET	49563	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:21:19.507297039 CET	53	49563	8.8.8.8	192.168.2.3
Nov 21, 2020 22:21:20.338855028 CET	51352	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:21:20.366700888 CET	53	51352	8.8.8.8	192.168.2.3
Nov 21, 2020 22:21:21.156471014 CET	59349	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:21:21.183614016 CET	53	59349	8.8.8.8	192.168.2.3
Nov 21, 2020 22:21:21.959223986 CET	57084	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:21:21.994941950 CET	53	57084	8.8.8.8	192.168.2.3
Nov 21, 2020 22:21:22.774533033 CET	58823	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:21:22.801701069 CET	53	58823	8.8.8.8	192.168.2.3
Nov 21, 2020 22:21:33.957308054 CET	57568	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:21:33.984694958 CET	53	57568	8.8.8.8	192.168.2.3
Nov 21, 2020 22:21:59.075335026 CET	50540	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:21:59.112881899 CET	53	50540	8.8.8.8	192.168.2.3
Nov 21, 2020 22:22:00.357954979 CET	54366	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:22:00.385130882 CET	53	54366	8.8.8.8	192.168.2.3
Nov 21, 2020 22:22:00.455102921 CET	53034	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:22:00.482178926 CET	53	53034	8.8.8.8	192.168.2.3
Nov 21, 2020 22:22:07.953336954 CET	57762	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:22:07.980539083 CET	53	57762	8.8.8.8	192.168.2.3
Nov 21, 2020 22:22:11.918097973 CET	55435	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:22:11.955988884 CET	53	55435	8.8.8.8	192.168.2.3
Nov 21, 2020 22:22:43.168602943 CET	50713	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:22:43.196012974 CET	53	50713	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2020 22:22:49.819142103 CET	56132	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:22:49.846364975 CET	53	56132	8.8.8.8	192.168.2.3
Nov 21, 2020 22:22:49.866417885 CET	58987	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:22:49.893604994 CET	53	58987	8.8.8.8	192.168.2.3
Nov 21, 2020 22:22:52.974126101 CET	56579	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:22:53.017977953 CET	53	56579	8.8.8.8	192.168.2.3
Nov 21, 2020 22:22:57.601746082 CET	60633	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:22:57.639264107 CET	53	60633	8.8.8.8	192.168.2.3
Nov 21, 2020 22:22:57.786498070 CET	61292	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:22:57.813941956 CET	53	61292	8.8.8.8	192.168.2.3
Nov 21, 2020 22:22:58.480577946 CET	63619	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:22:58.507960081 CET	53	63619	8.8.8.8	192.168.2.3
Nov 21, 2020 22:23:16.125009060 CET	64938	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:23:16.126764059 CET	61946	53	192.168.2.3	8.8.8.8
Nov 21, 2020 22:23:16.162115097 CET	53	64938	8.8.8.8	192.168.2.3
Nov 21, 2020 22:23:16.163928032 CET	53	61946	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 21, 2020 22:22:00.357954979 CET	192.168.2.3	8.8.8.8	0x2079	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:00.455102921 CET	192.168.2.3	8.8.8.8	0x1600	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:49.819142103 CET	192.168.2.3	8.8.8.8	0xf7e8	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:49.866417885 CET	192.168.2.3	8.8.8.8	0xe1e4	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:57.786498070 CET	192.168.2.3	8.8.8.8	0x59b2	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:58.480577946 CET	192.168.2.3	8.8.8.8	0xc345	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 21, 2020 22:23:16.125009060 CET	192.168.2.3	8.8.8.8	0xfcb0	Standard query (0)	cdn.onenote.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 21, 2020 22:22:00.385130882 CET	8.8.8.8	192.168.2.3	0x2079	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 22:22:00.385130882 CET	8.8.8.8	192.168.2.3	0x2079	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 22:22:00.385130882 CET	8.8.8.8	192.168.2.3	0x2079	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.164.148	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:00.385130882 CET	8.8.8.8	192.168.2.3	0x2079	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.66.103	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:00.385130882 CET	8.8.8.8	192.168.2.3	0x2079	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.252.4	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:00.385130882 CET	8.8.8.8	192.168.2.3	0x2079	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.169.28	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:00.385130882 CET	8.8.8.8	192.168.2.3	0x2079	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.182.194	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:00.385130882 CET	8.8.8.8	192.168.2.3	0x2079	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		174.129.214.20	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 21, 2020 22:22:00.385130882 CET	8.8.8.8	192.168.2.3	0x2079	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:00.385130882 CET	8.8.8.8	192.168.2.3	0x2079	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		184.73.247.141	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:00.482178926 CET	8.8.8.8	192.168.2.3	0x1600	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 22:22:00.482178926 CET	8.8.8.8	192.168.2.3	0x1600	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 22:22:00.482178926 CET	8.8.8.8	192.168.2.3	0x1600	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.164.148	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:00.482178926 CET	8.8.8.8	192.168.2.3	0x1600	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.66.103	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:00.482178926 CET	8.8.8.8	192.168.2.3	0x1600	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.252.4	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:00.482178926 CET	8.8.8.8	192.168.2.3	0x1600	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.169.28	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:00.482178926 CET	8.8.8.8	192.168.2.3	0x1600	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.182.194	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:00.482178926 CET	8.8.8.8	192.168.2.3	0x1600	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		174.129.214.20	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:00.482178926 CET	8.8.8.8	192.168.2.3	0x1600	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:00.482178926 CET	8.8.8.8	192.168.2.3	0x1600	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		184.73.247.141	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:49.846364975 CET	8.8.8.8	192.168.2.3	0xf7e8	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 22:22:49.846364975 CET	8.8.8.8	192.168.2.3	0xf7e8	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 22:22:49.846364975 CET	8.8.8.8	192.168.2.3	0xf7e8	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.142.93	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:49.846364975 CET	8.8.8.8	192.168.2.3	0xf7e8	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.66.103	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:49.846364975 CET	8.8.8.8	192.168.2.3	0xf7e8	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:49.846364975 CET	8.8.8.8	192.168.2.3	0xf7e8	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.126.66	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 21, 2020 22:22:49.846364975 CET	8.8.8.8	192.168.2.3	0xf7e8	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.83.248	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:49.846364975 CET	8.8.8.8	192.168.2.3	0xf7e8	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.252.4	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:49.846364975 CET	8.8.8.8	192.168.2.3	0xf7e8	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.161.145	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:49.846364975 CET	8.8.8.8	192.168.2.3	0xf7e8	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		184.73.247.141	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:49.893604994 CET	8.8.8.8	192.168.2.3	0xe1e4	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 22:22:49.893604994 CET	8.8.8.8	192.168.2.3	0xe1e4	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 22:22:49.893604994 CET	8.8.8.8	192.168.2.3	0xe1e4	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.66.103	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:49.893604994 CET	8.8.8.8	192.168.2.3	0xe1e4	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.142.93	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:49.893604994 CET	8.8.8.8	192.168.2.3	0xe1e4	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.252.4	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:49.893604994 CET	8.8.8.8	192.168.2.3	0xe1e4	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.153.147	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:49.893604994 CET	8.8.8.8	192.168.2.3	0xe1e4	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.169.28	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:49.893604994 CET	8.8.8.8	192.168.2.3	0xe1e4	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.164.148	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:49.893604994 CET	8.8.8.8	192.168.2.3	0xe1e4	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.42.25	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:49.893604994 CET	8.8.8.8	192.168.2.3	0xe1e4	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.83.248	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:57.813941956 CET	8.8.8.8	192.168.2.3	0x59b2	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 22:22:57.813941956 CET	8.8.8.8	192.168.2.3	0x59b2	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 22:22:57.813941956 CET	8.8.8.8	192.168.2.3	0x59b2	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.142.93	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:57.813941956 CET	8.8.8.8	192.168.2.3	0x59b2	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.66.103	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 21, 2020 22:22:57.813941956 CET	8.8.8.8	192.168.2.3	0x59b2	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:57.813941956 CET	8.8.8.8	192.168.2.3	0x59b2	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.126.66	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:57.813941956 CET	8.8.8.8	192.168.2.3	0x59b2	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.83.248	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:57.813941956 CET	8.8.8.8	192.168.2.3	0x59b2	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.252.4	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:57.813941956 CET	8.8.8.8	192.168.2.3	0x59b2	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.161.145	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:57.813941956 CET	8.8.8.8	192.168.2.3	0x59b2	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		184.73.247.141	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:58.507960081 CET	8.8.8.8	192.168.2.3	0xc345	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 22:22:58.507960081 CET	8.8.8.8	192.168.2.3	0xc345	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 21, 2020 22:22:58.507960081 CET	8.8.8.8	192.168.2.3	0xc345	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		174.129.214.20	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:58.507960081 CET	8.8.8.8	192.168.2.3	0xc345	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.142.93	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:58.507960081 CET	8.8.8.8	192.168.2.3	0xc345	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.153.147	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:58.507960081 CET	8.8.8.8	192.168.2.3	0xc345	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		184.73.247.141	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:58.507960081 CET	8.8.8.8	192.168.2.3	0xc345	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:58.507960081 CET	8.8.8.8	192.168.2.3	0xc345	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.164.148	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:58.507960081 CET	8.8.8.8	192.168.2.3	0xc345	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.169.28	A (IP address)	IN (0x0001)
Nov 21, 2020 22:22:58.507960081 CET	8.8.8.8	192.168.2.3	0xc345	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.42.25	A (IP address)	IN (0x0001)
Nov 21, 2020 22:23:16.162115097 CET	8.8.8.8	192.168.2.3	0xfcb0	No error (0)	cdn.onenote.net	cdn.onenote.net.edgekey.net		CNAME (Canonical name)	IN (0x0001)

HTTP Request Dependency Graph

- api.ipify.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49721	54.243.164.148	80	C:\Users\user\Desktop\Shipping-Document.exe

Timestamp	kBytes transferred	Direction	Data
Nov 21, 2020 22:22:00.866674900 CET	348	OUT	GET / HTTP/1.1 Host: api.ipify.org Connection: Keep-Alive
Nov 21, 2020 22:22:00.976836920 CET	349	IN	HTTP/1.1 200 OK Server: Cowboy Connection: keep-alive Content-Type: text/plain Vary: Origin Date: Sat, 21 Nov 2020 21:22:00 GMT Content-Length: 11 Via: 1.1 vegur Data Raw: 38 34 2e 31 37 2e 35 32 2e 32 35 Data Ascii: 84.17.52.25

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49732	54.235.142.93	80	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe

Timestamp	kBytes transferred	Direction	Data
Nov 21, 2020 22:22:50.056575060 CET	3658	OUT	GET / HTTP/1.1 Host: api.ipify.org Connection: Keep-Alive
Nov 21, 2020 22:22:50.164937019 CET	3658	IN	HTTP/1.1 200 OK Server: Cowboy Connection: keep-alive Content-Type: text/plain Vary: Origin Date: Sat, 21 Nov 2020 21:22:50 GMT Content-Length: 11 Via: 1.1 vegur Data Raw: 38 34 2e 31 37 2e 35 32 2e 32 35 Data Ascii: 84.17.52.25

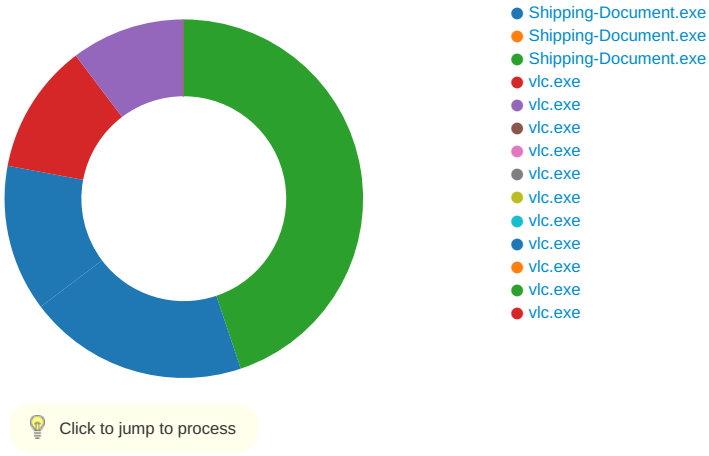
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49735	54.235.142.93	80	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe

Timestamp	kBytes transferred	Direction	Data
Nov 21, 2020 22:22:58.665633917 CET	3669	OUT	GET / HTTP/1.1 Host: api.ipify.org Connection: Keep-Alive
Nov 21, 2020 22:22:58.773164034 CET	3675	IN	HTTP/1.1 200 OK Server: Cowboy Connection: keep-alive Content-Type: text/plain Vary: Origin Date: Sat, 21 Nov 2020 21:22:58 GMT Content-Length: 11 Via: 1.1 vegur Data Raw: 38 34 2e 31 37 2e 35 32 2e 32 35 Data Ascii: 84.17.52.25

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Shipping-Document.exe PID: 1364 Parent PID: 5600

General

Start time:	22:21:14
Start date:	21/11/2020
Path:	C:\Users\user\Desktop\Shipping-Document.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Shipping-Document.exe'
Imagebase:	0x450000
File size:	1631688 bytes
MD5 hash:	47F1684C0075AEA74BB225586D55B6E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_MassLogger, Description: Yara detected MassLogger RAT, Source: 00000000.00000002.292894367.0000000003997000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MassLogger, Description: Yara detected MassLogger RAT, Source: 00000000.00000003.285012492.0000000003F10000.00000004.00000001.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	6DFACF06	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	6DFACF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CDFBEFF	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Shipping-Document.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E2BC78D	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\Shipping-Document.exe.log	unknown	1119	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	6E2BC907	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	6DF85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DF85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DEE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF8CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DEE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DEE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DEE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DEE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DF85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CDF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CDF1B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	vlc	unicode	"C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe"	success or wait	1	6CDF646A	RegSetValueExW

Analysis Process: Shipping-Document.exe PID: 3420 Parent PID: 1364

General

Start time:	22:21:49
Start date:	21/11/2020
Path:	C:\Users\user\Desktop\Shipping-Document.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Shipping-Document.exe
Imagebase:	0x3f0000
File size:	1631688 bytes
MD5 hash:	47F1684C0075AEA74BB225586D55B6E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Shipping-Document.exe PID: 1488 Parent PID: 1364

General

Start time:	22:21:50
Start date:	21/11/2020
Path:	C:\Users\user\Desktop\Shipping-Document.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Shipping-Document.exe
Imagebase:	0x990000
File size:	1631688 bytes
MD5 hash:	47F1684C0075AEA74BB225586D55B6E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.483989726.0000000002DE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MassLogger, Description: Yara detected MassLogger RAT, Source: 00000005.00000002.474947911.0000000000402000.00000040.00000001.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	6DFACF06	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	6DFACF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\AEC365839D	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CDFBEFF	CreateDirectoryW
C:\Users\user\AppData\Local\AEC365839D\Log.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CDF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\DotNetZip-fu3v0fes.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CDF1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\AEC365839D\Log.txt	success or wait	1	6CDF6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\user_United States_AEC365839D_11-21-2020 22.22.19.zip	success or wait	1	6CDF6A95	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DotNetZip-fu3v0fes.tmp	C:\Users\user\AppData\Local\Temp\user_United States_AEC365839D_11-21-2020 22.22.19.zip	success or wait	1	6CDF930D	MoveFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\AEC365839D\Log.txt	unknown	1759	3c 7c 7c 20 76 32 2e 34 2e 30 2e 30 20 7c 7c 3e 0d 0a 55 73 65 72 20 4e 61 6d 65 3a 20 68 61 72 64 7a 0d 0a 49 50 3a 20 38 34 2e 31 37 2e 35 32 2e 32 35 0d 0a 4c 6f 63 61 74 69 6f 6e 3a 20 55 6e 69 74 65 64 20 53 74 61 74 65 73 0d 0a 57 69 6e 64 6f 77 73 20 4f 53 3a 20 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 31 30 20 50 72 6f 20 36 34 62 69 74 0d 0a 57 69 6e 64 6f 77 73 20 53 65 72 69 61 6c 20 4b 65 79 3a 20 56 47 37 4e 46 2d 42 4a 37 37 59 2d 57 52 46 37 58 2d 47 4a 56 57 37 2d 48 33 4d 38 54 0d 0a 43 50 55 3a 20 49 6e 74 65 6c 28 52 29 20 43 6f 72 65 28 54 4d 29 32 20 43 50 55 20 36 36 30 30 20 40 20 32 2e 34 30 20 47 48 7a 0d 0a 47 50 55 3a 20 4d 69 63 72 6f 73 6f 66 74 20 42 61 73 69 63 20 44 69 73 70 6c 61 79 20 41 64 61 70 74 65 72 0d	<|| v2.4.0.0 ||>..User Name: user..IP: 84.17.52.25..Location: United States..Windows OS: Microsoft Windows 10 Pro 64bit..Windows Serial Key: VG7NF-BJ77Y-WRF7X-GJVW7-H3M8T..CPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz..GPU: Microsoft Basic Display Adapter.	success or wait	1	6CDF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DotNetZip-fu3v0fes.tmp	unknown	878	50 4b 03 04 14 00 00 00 00 00 c9 b2 75 51 00 00 00 00 00 00 00 00 00 00 00 00 33 00 24 00 68 61 72 64 7a 5f 55 6e 69 74 65 64 20 53 74 61 74 65 73 5f 41 45 43 33 36 35 38 33 39 44 5f 31 31 2d 32 31 2d 32 30 32 30 20 32 32 2e 32 32 2e 31 39 2f 0a 00 20 00 00 00 00 00 01 00 18 00 f1 8a d4 d4 97 c0 d6 01 f1 8a d4 d4 97 c0 d6 01 de 9d 9b d1 97 c0 d6 01 50 4b 03 04 14 00 00 00 08 00 c9 b2 75 51 00 00 00 00 00 00 00 00 00 00 00 00 3a 00 24 00 68 61 72 64 7a 5f 55 6e 69 74 65 64 20 53 74 61 74 65 73 5f 41 45 43 33 36 35 38 33 39 44 5f 31 31 2d 32 31 2d 32 30 32 30 20 32 32 2e 32 32 2e 31 39 2f 4c 6f 67 2e 74 78 74 0a 00 20 00 00 00 00 00 01 00 18 00 68 ed d6 d4 97 c0 d6 01 68 ed d6 d4 97 c0 d6 01 f1 8a d4 d4 97 c0 d6 01 ed 95 6d 6f da 30 10 c7 df 47 ca 77 b8 97	PK.....uQ.....3.$. user_United States_AEC365839D_11-21-2020 22.22.19/.. ....PK.. .....uQ.....:.$.user _United States_AEC365839D_11-21-2020 22.22.19/Log.txt.. .....h.....h..... .mo.0...G.w..	success or wait	1	6CDF1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\DotNetZip-fu3v0fes.tmp	unknown	124	50 4b 03 04 14 00 00 00 08 00 c9 b2 75 51 95 41 e1 53 7d 02 00 00 df 06 00 00 3a 00 24 00 68 61 72 64 7a 5f 55 6e 69 74 65 64 20 53 74 61 74 65 73 5f 41 45 43 33 36 35 38 33 39 44 5f 31 31 2d 32 31 2d 32 30 32 30 20 32 32 2e 32 32 2e 31 39 2f 4c 6f 67 2e 74 78 74 0a 00 20 00 00 00 00 00 01 00 18 00 68 ed d6 d4 97 c0 d6 01 68 ed d6 d4 97 c0 d6 01 f1 8a d4 d4 97 c0 d6 01	PK.....uQ.A.S}.....:.$. user_United States_AEC365839D_11-21-2020 22.22.19/Log.txt.. .....h.....h.....	success or wait	1	6CDF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DotNetZip-fu3v0fes.tmp	unknown	295	50 4b 01 02 2d 00 14 00 00 00 00 00 c9 b2 75 51 00 00 00 00 00 00 00 00 00 00 00 00 33 00 24 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 68 61 72 64 7a 5f 55 6e 69 74 65 64 20 53 74 61 74 65 73 5f 41 45 43 33 36 35 38 33 39 44 5f 31 31 2d 32 31 2d 32 30 32 30 20 32 32 2e 32 32 2e 31 39 2f 0a 00 20 00 00 00 00 00 01 00 18 00 f1 8a d4 d4 97 c0 d6 01 f1 8a d4 d4 97 c0 d6 01 de 9d 9b d1 97 c0 d6 01 50 4b 01 02 2d 00 14 00 00 00 08 00 c9 b2 75 51 95 41 e1 53 7d 02 00 00 df 06 00 00 3a 00 24 00 00 00 00 00 00 00 00 20 00 00 00 75 00 00 00 68 61 72 64 7a 5f 55 6e 69 74 65 64 20 53 74 61 74 65 73 5f 41 45 43 33 36 35 38 33 39 44 5f 31 31 2d 32 31 2d 32 30 32 30 20 32 32 2e 32 32 2e 31 39 2f 4c 6f 67 2e 74 78 74 0a 00 20 00 00 00 00 00 01 00 18 00 68 ed d6 d4 97 c0	PK..-.....uQ.....3. $.....user_United States_AEC365839D_11-21-2020 22.22.19/.. .....PK..-.....uQ.A.S}.....:.$..... ...u...user_United States_AEC365839D_11-21-2020 22.22.19/Log.txt.. .....h.....	success or wait	1	6CDF1B4F	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	6DF85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DF85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DEE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF8CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DEE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DEE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DF85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DEE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DEE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CDF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CDF1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CDF1B4F	ReadFile
C:\Users\user\AppData\Local\AEC365839D\Log.txt	unknown	32768	success or wait	1	6CDF1B4F	ReadFile
C:\Users\user\AppData\Local\AEC365839D\Log.txt	unknown	32768	end of file	1	6CDF1B4F	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles	success or wait	1	6CDF5F3C	RegCreateKeyExW

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\17.0\Outlook	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\17.0\Outlook\Profiles	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\17.0\Outlook\Profiles\Outlook	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\17.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\18.0	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\18.0\Outlook	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\18.0\Outlook\Profiles	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\18.0\Outlook\Profiles\Outlook	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\18.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\19.0	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\19.0\Outlook	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\19.0\Outlook\Profiles	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\19.0\Outlook\Profiles\Outlook	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\19.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\20.0	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\20.0\Outlook	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\20.0\Outlook\Profiles	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\20.0\Outlook\Profiles\Outlook	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\20.0\Outlook\Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem \Profiles\Outlook\9375CFF0413111d3B88A00104B2A6676	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging Subsystem	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging Subsystem\Profiles	success or wait	1	6CDF5F3C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows Messaging Subsystem\Profiles\9375CFF0413111d3 B88A00104B2A6676	success or wait	1	6CDF5F3C	RegCreateKeyExW

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: vlc.exe PID: 1748 Parent PID: 3388

General

Start time:	22:22:00
Start date:	21/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe'
Imagebase:	0xbe0000
File size:	1631688 bytes
MD5 hash:	47F1684C0075AEA74BB225586D55B6E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_MassLogger, Description: Yara detected MassLogger RAT, Source: 0000000C.00000003.392005702.00000000048A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MassLogger, Description: Yara detected MassLogger RAT, Source: 0000000C.00000002.399837462.0000000004325000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MassLogger, Description: Yara detected MassLogger RAT, Source: 0000000C.00000003.380082858.00000000048A0000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 21%, Virustotal, Browse • Detection: 5%, Metadefender, Browse • Detection: 21%, ReversingLabs
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	6DFACF06	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	6DFACF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\vlc.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E2BC78D	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\vlc.exe.log	unknown	1119	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	6E2BC907	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	6DF85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DF85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DEE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF8CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DEE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DEE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DEE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DEE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DF85705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CDF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CDF1B4F	ReadFile

Analysis Process: vlc.exe PID: 3440 Parent PID: 3388

General

Start time:	22:22:08
Start date:	21/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe'
Imagebase:	0xb0000
File size:	1631688 bytes
MD5 hash:	47F1684C0075AEA74BB225586D55B6E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_MassLogger, Description: Yara detected MassLogger RAT, Source: 0000000E.00000003.401816626.00000000040ED000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MassLogger, Description: Yara detected MassLogger RAT, Source: 0000000E.00000002.411380915.0000000003515000.00000004.00000001.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	6DFACF06	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	6DFACF06	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	6DF85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DF85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DEE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF8CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DEE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DEE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DEE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DEE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DF85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CDF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CDF1B4F	ReadFile

Analysis Process: vlc.exe PID: 2792 Parent PID: 1748

General

Start time:	22:22:34
Start date:	21/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Imagebase:	0x4b0000
File size:	1631688 bytes
MD5 hash:	47F1684C0075AEA74BB225586D55B6E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vlc.exe PID: 6052 Parent PID: 1748

General

Start time:	22:22:34
Start date:	21/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Imagebase:	0x230000
File size:	1631688 bytes
MD5 hash:	47F1684C0075AEA74BB225586D55B6E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vlc.exe PID: 1872 Parent PID: 1748

General

Start time:	22:22:36
Start date:	21/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Imagebase:	0x90000
File size:	1631688 bytes
MD5 hash:	47F1684C0075AEA74BB225586D55B6E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vlc.exe PID: 4472 Parent PID: 1748

General

Start time:	22:22:37

Start date:	21/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Imagebase:	0x190000
File size:	1631688 bytes
MD5 hash:	47F1684C0075AEA74BB225586D55B6E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vlc.exe PID: 5352 Parent PID: 1748

General

Start time:	22:22:37
Start date:	21/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Imagebase:	0x10000
File size:	1631688 bytes
MD5 hash:	47F1684C0075AEA74BB225586D55B6E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vlc.exe PID: 1256 Parent PID: 1748

General

Start time:	22:22:40
Start date:	21/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Imagebase:	0x7ff7488e0000
File size:	1631688 bytes
MD5 hash:	47F1684C0075AEA74BB225586D55B6E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000016.00000002.484501673.0000000002B51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MassLogger, Description: Yara detected MassLogger RAT, Source: 00000016.00000002.474961619.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DFACF06	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	6DFACF06	unknown
C:\Users\user\AppData\Local\AEC365839D	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CDFBEFF	CreateDirectoryW
C:\Users\user\AppData\Local\AEC365839D\Log.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CDF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\DotNetZip-4b2ut3ef.tmp	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CDF1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\AEC365839D\Log.txt	success or wait	1	6CDF6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\user_United States_AEC365839D_11-21-2020 22.22.58.zip	success or wait	1	6CDF6A95	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DotNetZip-4b2ut3ef.tmp	C:\Users\user\AppData\Local\Temp\user_United States_AEC365839D_11-21-2020 22.22.58.zip	success or wait	1	6CDF930D	MoveFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\AEC365839D\Log.txt	unknown	1800	3c 7c 7c 20 76 32 2e 34 2e 30 2e 30 20 7c 7c 3e 0d 0a 55 73 65 72 20 4e 61 6d 65 3a 20 68 61 72 64 7a 0d 0a 49 50 3a 20 38 34 2e 31 37 2e 35 32 2e 32 35 0d 0a 4c 6f 63 61 74 69 6f 6e 3a 20 55 6e 69 74 65 64 20 53 74 61 74 65 73 0d 0a 57 69 6e 64 6f 77 73 20 4f 53 3a 20 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 31 30 20 50 72 6f 20 36 34 62 69 74 0d 0a 57 69 6e 64 6f 77 73 20 53 65 72 69 61 6c 20 4b 65 79 3a 20 56 47 37 4e 46 2d 42 4a 37 37 59 2d 57 52 46 37 58 2d 47 4a 56 57 37 2d 48 33 4d 38 54 0d 0a 43 50 55 3a 20 49 6e 74 65 6c 28 52 29 20 43 6f 72 65 28 54 4d 29 32 20 43 50 55 20 36 36 30 30 20 40 20 32 2e 34 30 20 47 48 7a 0d 0a 47 50 55 3a 20 4d 69 63 72 6f 73 6f 66 74 20 42 61 73 69 63 20 44 69 73 70 6c 61 79 20 41 64 61 70 74 65 72 0d	<|| v2.4.0.0 ||>..User Name: user..IP: 84.17.52.25..Location: United States..Windows OS: Microsoft Windows 10 Pro 64bit..Windows Serial Key: VG7NF-BJ77Y-WRF7X-GJVW7-H3M8T..CPU: Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz..GPU: Microsoft Basic Display Adapter.	success or wait	1	6CDF1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\DotNetZip-4b2ut3ef.tmp	unknown	898	50 4b 03 04 14 00 00 00 00 00 dd b2 75 51 00 00 00 00 00 00 00 00 00 00 00 00 33 00 24 00 68 61 72 64 7a 5f 55 6e 69 74 65 64 20 53 74 61 74 65 73 5f 41 45 43 33 36 35 38 33 39 44 5f 31 31 2d 32 31 2d 32 30 32 30 20 32 32 2e 32 32 2e 35 38 2f 0a 00 20 00 00 00 00 00 01 00 18 00 01 14 f2 eb 97 c0 d6 01 01 14 f2 eb 97 c0 d6 01 18 8c 7d e8 97 c0 d6 01 50 4b 03 04 14 00 00 00 08 00 dd b2 75 51 00 00 00 00 00 00 00 00 00 00 00 00 3a 00 24 00 68 61 72 64 7a 5f 55 6e 69 74 65 64 20 53 74 61 74 65 73 5f 41 45 43 33 36 35 38 33 39 44 5f 31 31 2d 32 31 2d 32 30 32 30 20 32 32 2e 32 32 2e 35 38 2f 4c 6f 67 2e 74 78 74 0a 00 20 00 00 00 00 00 01 00 18 00 01 14 f2 eb 97 c0 d6 01 01 14 f2 eb 97 c0 d6 01 01 14 f2 eb 97 c0 d6 01 ed 95 5b 6f da 30 14 c7 df 23 e5 3b 9c c7	PK.....uQ.....3.$. user_United States_AEC365839D_11-21-2020 22.22.58/.. ....}.....PK.. .....uQ.....:.$.user _United States_AEC365839D_11-21-2020 22.22.58/Log.txt.. ..... [o.0...#.;..	success or wait	1	6CDF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DotNetZip-4b2ut3ef.tmp	unknown	124	50 4b 03 04 14 00 00 00 08 00 dd b2 75 51 0c 42 57 f1 91 02 00 00 08 07 00 00 3a 00 24 00 68 61 72 64 7a 5f 55 6e 69 74 65 64 20 53 74 61 74 65 73 5f 41 45 43 33 36 35 38 33 39 44 5f 31 31 2d 32 31 2d 32 30 32 30 20 32 32 2e 32 32 2e 35 38 2f 4c 6f 67 2e 74 78 74 0a 00 20 00 00 00 00 00 01 00 18 00 01 14 f2 eb 97 c0 d6 01 01 14 f2 eb 97 c0 d6 01 01 14 f2 eb 97 c0 d6 01	PK.....uQ.BW.....:.$. user_United States_AEC365839D_11-21-2020 22.22.58/Log.txt..	success or wait	1	6CDF1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\DotNetZip-4b2ut3ef.tmp	unknown	295	50 4b 01 02 2d 00 14 00 00 00 00 00 dd b2 75 51 00 00 00 00 00 00 00 00 00 00 00 33 00 24 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 68 61 72 64 7a 5f 55 6e 69 74 65 64 20 53 74 61 74 65 73 5f 41 45 43 33 36 35 38 33 39 44 5f 31 31 2d 32 31 2d 32 30 32 30 20 32 32 2e 32 32 2e 35 38 2f 0a 00 20 00 00 00 00 00 01 00 18 00 01 14 f2 eb 97 c0 d6 01 01 14 f2 eb 97 c0 d6 01 18 8c 7d e8 97 c0 d6 01 50 4b 01 02 2d 00 14 00 00 00 08 00 dd b2 75 51 0c 42 57 f1 91 02 00 00 08 07 00 00 3a 00 24 00 00 00 00 00 00 00 00 20 00 00 00 00 75 00 00 00 68 61 72 64 7a 5f 55 6e 69 74 65 64 20 53 74 61 74 65 73 5f 41 45 43 33 36 35 38 33 39 44 5f 31 31 2d 32 31 2d 32 30 32 30 20 32 32 2e 32 32 2e 35 38 2f 4c 6f 67 2e 74 78 74 0a 00 20 00 00 00 00 00 01 00 18 00 01 14 f2 eb 97 c0	PK..-.....uQ.....3. $.....user_United States_AEC365839D_11-21-2020 22.22.58/.. .....}.....PK..-.....uQ.BW.....:.$..... ...u...user_United States_AEC365839D_11-21-2020 22.22.58/Log.txt..	success or wait	1	6CDF1B4F	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	6DF85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DF85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DEE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF8CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DEE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DEE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DF85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DEE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DEE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CDF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CDF1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CDF1B4F	ReadFile
C:\Users\user\AppData\Local\AEC365839D\Log.txt	unknown	32768	success or wait	1	6CDF1B4F	ReadFile
C:\Users\user\AppData\Local\AEC365839D\Log.txt	unknown	32768	end of file	1	6CDF1B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: vlc.exe PID: 1012 Parent PID: 3440

General

Start time:	22:22:43
Start date:	21/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Imagebase:	0x7ff7488e0000
File size:	1631688 bytes
MD5 hash:	47F1684C0075AEA74BB225586D55B6E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vlc.exe PID: 4832 Parent PID: 3440

General

Start time:	22:22:45
Start date:	21/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Imagebase:	0x350000
File size:	1631688 bytes
MD5 hash:	47F1684C0075AEA74BB225586D55B6E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vlc.exe PID: 484 Parent PID: 3440

General

Start time:	22:22:45
Start date:	21/11/2020
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\VideoLAN\vlc.exe
Imagebase:	0xb10000
File size:	1631688 bytes
MD5 hash:	47F1684C0075AEA74BB225586D55B6E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001A.00000002.484549006.0000000002F71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MassLogger, Description: Yara detected MassLogger RAT, Source: 0000001A.00000002.475038821.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis