ID: 756232
Sample Name: shipping docs.exe
Cookbook: default.jbs
Time: 21:18:08
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

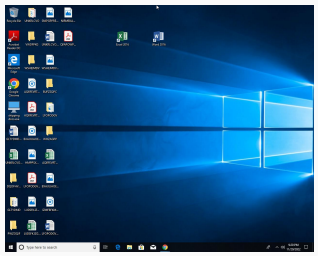
Windows Analysis Report

shipping docs.exe

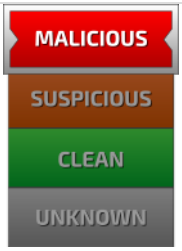
Overview

General Information

Sample Name:	shipping docs.exe
Analysis ID:	756232
MD5:	6308ae755a893c..
SHA1:	00ada70aa14a5c..
SHA256:	9dfdb5048599b1..
Tags:	agenttesla exe
Infos:	



Detection



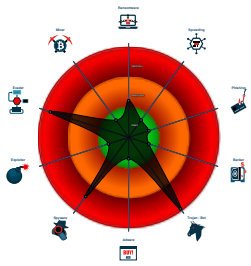
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Telegram RAT
- Yara detected AgentTesla
- Yara detected AntiVM3
- Sigma detected: Scheduled temp fil…
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- shipping docs.exe (PID: 2400 cmdline: C:\Users\user\Desktop\shipping docs.exe MD5: 6308AE755A893C15A989B1CCF2C56393)
  - schtasks.exe (PID: 5248 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\yVGAJfiVEvtg" /XML "C:\Users\user\AppData\Local\Temp\tmp7934.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5220 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - shipping docs.exe (PID: 3776 cmdline: {path} MD5: 6308AE755A893C15A989B1CCF2C56393)
- yVGAJfiVEvtg.exe (PID: 4552 cmdline: C:\Users\user\AppData\Roaming\yVGAJfiVEvtg.exe MD5: 6308AE755A893C15A989B1CCF2C56393)
  - schtasks.exe (PID: 4792 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\yVGAJfiVEvtg" /XML "C:\Users\user\AppData\Local\Temp\tmpF5B7.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4536 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - yVGAJfiVEvtg.exe (PID: 3680 cmdline: {path} MD5: 6308AE755A893C15A989B1CCF2C56393)
- VMqTMMD.exe (PID: 1280 cmdline: "C:\Users\user\AppData\Roaming\VMqTMMD\VMqTMMD.exe" MD5: 6308AE755A893C15A989B1CCF2C56393)
- VMqTMMD.exe (PID: 3124 cmdline: "C:\Users\user\AppData\Roaming\VMqTMMD\VMqTMMD.exe" MD5: 6308AE755A893C15A989B1CCF2C56393)
  - schtasks.exe (PID: 4184 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\yVGAJfiVEvtg" /XML "C:\Users\user\AppData\Local\Temp\tmp3418.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4404 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - VMqTMMD.exe (PID: 5228 cmdline: {path} MD5: 6308AE755A893C15A989B1CCF2C56393)
- **cleanup**

Malware Configuration

Threatname: Telegram RAT

```
{
  "C2 url": "https://api.telegram.org/bot5676971476:AAFdGsXW8kwzXNIluAGV-a4sJ2XBy6809WI/sendMessage"
}
```

Threatname: Agenttesla

```
{
  "Exfil Mode": "Telegram",
  "Telegram Url": "https://api.telegram.org/bot5676971476:AAFdGsXW8kwzXNIluAGV-o4sJ2XBy68O9WI/sendMessage?chat_id=1644584536"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.343723068.0000000002D38000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.270616747.00000000034A9000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.270616747.00000000034A9000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.270616747.00000000034A9000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x15b63d:$a13: get_DnsResolver • 0x191c5d:$a13: get_DnsResolver • 0x159d4a:$a20: get_LastAccessed • 0x19036a:$a20: get_LastAccessed • 0x15c06b:$a27: set_InternalServerPort • 0x19268b:$a27: set_InternalServerPort • 0x15c3a0:$a30: set_GuidMasterKey • 0x1929c0:$a30: set_GuidMasterKey • 0x159e5c:$a33: get_Clipboard • 0x19047c:$a33: get_Clipboard • 0x159e6a:$a34: get_Keyboard • 0x19048a:$a34: get_Keyboard • 0x15b237:$a35: get_ShiftKeyDown • 0x191857:$a35: get_ShiftKeyDown • 0x15b248:$a36: get_AltKeyDown • 0x191868:$a36: get_AltKeyDown • 0x159e77:$a37: get_Password • 0x190497:$a37: get_Password • 0x15a992:$a38: get_PasswordHash • 0x190fb2:$a38: get_PasswordHash • 0x15ba9f:$a39: get_DefaultCredentials
00000012.00000002.520653491.00000000030C1000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 28 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.shipping docs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.0.shipping docs.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
3.0.shipping docs.exe.400000.0.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x34a4b:$s10: logins • 0x344c5:$s11: credential • 0x3072c:$g1: get_Clipboard • 0x3073a:$g2: get_Keyboard • 0x30747:$g3: get_Password • 0x31af7:$g4: get_CtrlKeyDown • 0x31b07:$g5: get_ShiftKeyDown • 0x31b18:$g6: get_AltKeyDown
3.0.shipping docs.exe.400000.0.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x31f0d:$a13: get_DnsResolver • 0x3061a:$a20: get_LastAccessed • 0x3293b:$a27: set_InternalServerPort • 0x32c70:$a30: set_GuidMasterKey • 0x3072c:$a33: get_Clipboard • 0x3073a:$a34: get_Keyboard • 0x31b07:$a35: get_ShiftKeyDown • 0x31b18:$a36: get_AltKeyDown • 0x30747:$a37: get_Password • 0x31262:$a38: get_PasswordHash • 0x3236f:$a39: get_DefaultCredentials
0.2.shipping docs.exe.35d2730.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 7 entries				

Sigma Signatures

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Snort Signatures

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.3 - Destination IP: 149.154.167.220

Timestamp:	192.168.2.3149.154.167.220496994432851779 11/29/22-21:19:34.793087
SID:	2851779
Source Port:	49699
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.3 - Destination IP: 149.154.167.220

Timestamp:	192.168.2.3149.154.167.220497004432851779 11/29/22-21:20:32.964256
SID:	2851779
Source Port:	49700
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Agent Tesla Telegram Exfil - Source IP: 192.168.2.3 - Destination IP: 149.154.167.220

Timestamp:	192.168.2.3149.154.167.220497014432851779 11/29/22-21:20:48.592868
SID:	2851779
Source Port:	49701
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

Uses the Telegram API (likely for C&C communication)

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Boot Survival

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Telegram RAT

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

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

Tries to harvest and steal ftp login credentials

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

Remote Access Functionality

Yara detected Telegram RAT

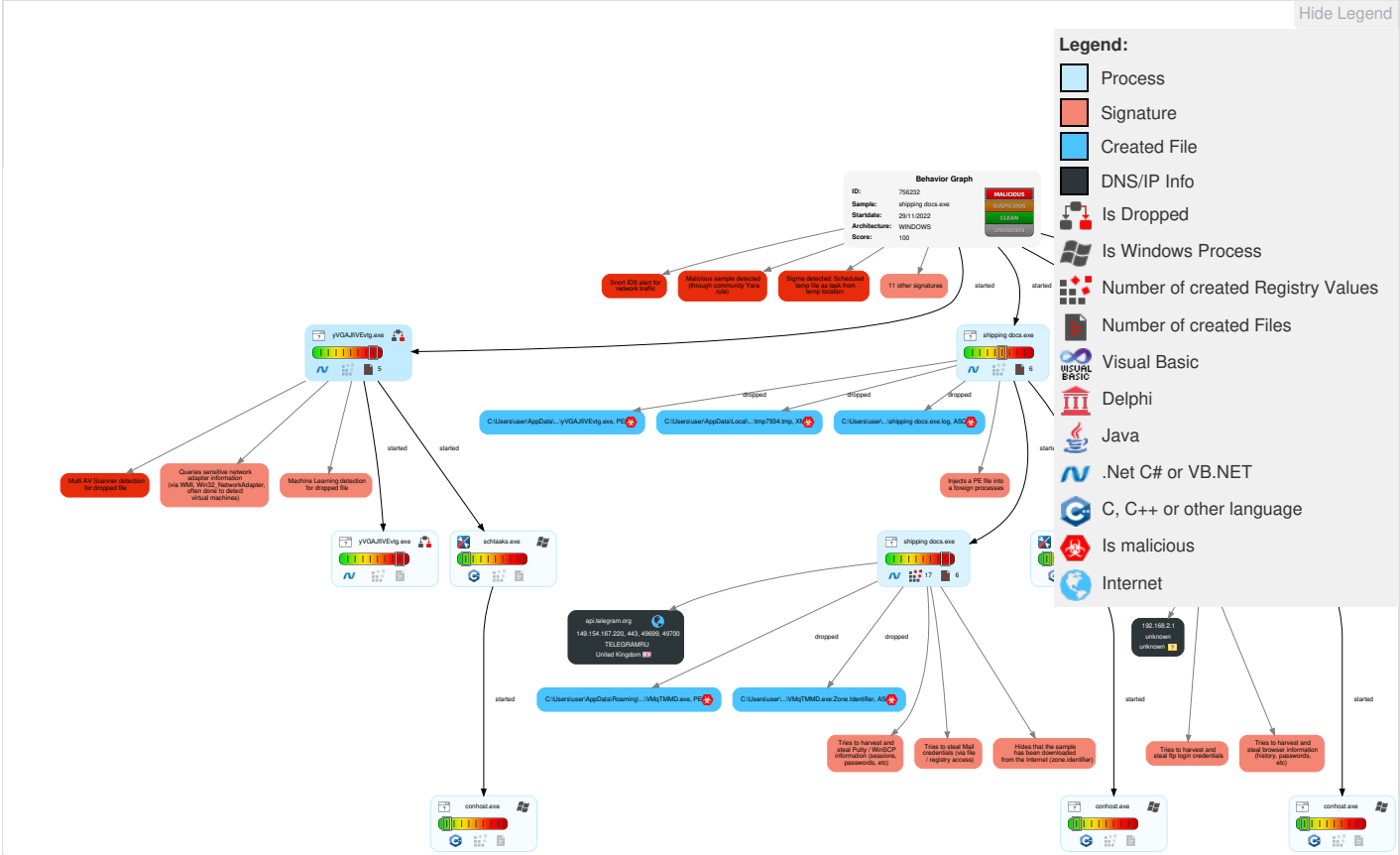
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 Scheduled Task/Job	1 1 1 Process Injection	1 Disable or Modify Tools	2 OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Web Service	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	1 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	1 Deobfuscate/Decode Files or Information	1 Input Capture	1 1 4 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	2 Obfuscated Files or Information	1 Credentials in Registry	1 Query Registry	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 Software Packing	NTDS	3 1 1 Security Software Discovery	Distributed Component Object Model	1 Input Capture	Scheduled Transfer	3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	1 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 1 1 Process Injection	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Hidden Files and Directories	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

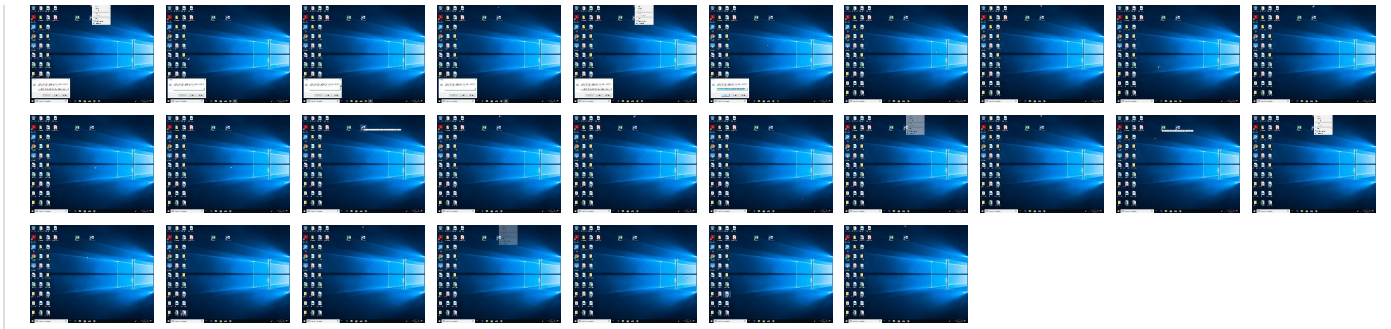
Behavior Graph



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 docs.exe	73%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
shipping docs.exe	47%	Virustotal		Browse
shipping docs.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\yVGAJfiVEvtg.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\VMqTMMD\VMqTMMD.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\VMqTMMD\VMqTMMD.exe	73%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\yVGAJfiVEvtg.exe	73%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.shipping docs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
c-0001.c-msedge.net	0%	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.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.s.$	0%	Avira URL Cloud	safe	
http://https://api.telegram.org4	0%	URL Reputation	safe	
http://https://api.telegram.org4	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.sajatypeworks.comteP$	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/O	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/$	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://https://JIQ1JKgQReGyOBe.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/=	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.founder.com.cn/cnu-h	0%	URL Reputation	safe	
http://www.fonts.com8	0%	URL Reputation	safe	
http://www.founder.com.cn/cn%	0%	URL Reputation	safe	
http://www.sandoll.co.krT	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.sandoll.co.krigh	0%	Avira URL Cloud	safe	
http://Unbjpy.com	0%	Avira URL Cloud	safe	
http://www.fonts.comtteJ	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnlJ	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/ko	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
c-0001.c-msedge.net	13.107.4.50	true	false	• 0%, Virustotal, Browse	unknown
api.telegram.org	149.154.167.220	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot5676971476:AAFdGsXW8kwzXNIluAGV-a4sJ2XBy68O9WI/sendDocument	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	shipping docs.exe, 00000003.00000002.518422910.0000000002FA1000.00000004.00000800.00020000.00000000.sdmp, yVGAJfiVEvtg.exe, 00000012.00000002.520653491.00000000030C1000.00000004.00000800.00020000.00000000.sdmp, VMqTMMD.exe, 00000015.00000002.518773451.0000000002E61000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	shipping docs.exe, 00000000.00000002.279908957.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	shipping docs.exe, 00000000.00000002.279908957.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	shipping docs.exe, 00000000.00000002.279908957.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.telegram.org	shipping docs.exe, 00000003.00000002.534292549.0000000003336000.00000004.00000800.00020000.00000000.sdmp, yVGAJfiVEvtg.exe, 00000012.00000002.537543749.00000000349A000.00000004.00000800.00020000.00000000.sdmp, VMqTMMD.exe, 00000015.00000002.534577687.00000000031EE000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers?	shipping docs.exe, 00000000.00000002.279908957.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.s.$	shipping docs.exe, 00000000.00000003.239908062.0000000005493000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.240179699.0000000005493000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.240220486.0000000005493000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.239881609.0000000005491000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.240113755.0000000005493000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.tiro.com	shipping docs.exe, 00000000.00000002.279908957.0000000006732000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.240459510.000000000548B000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.240423951.000000000548B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

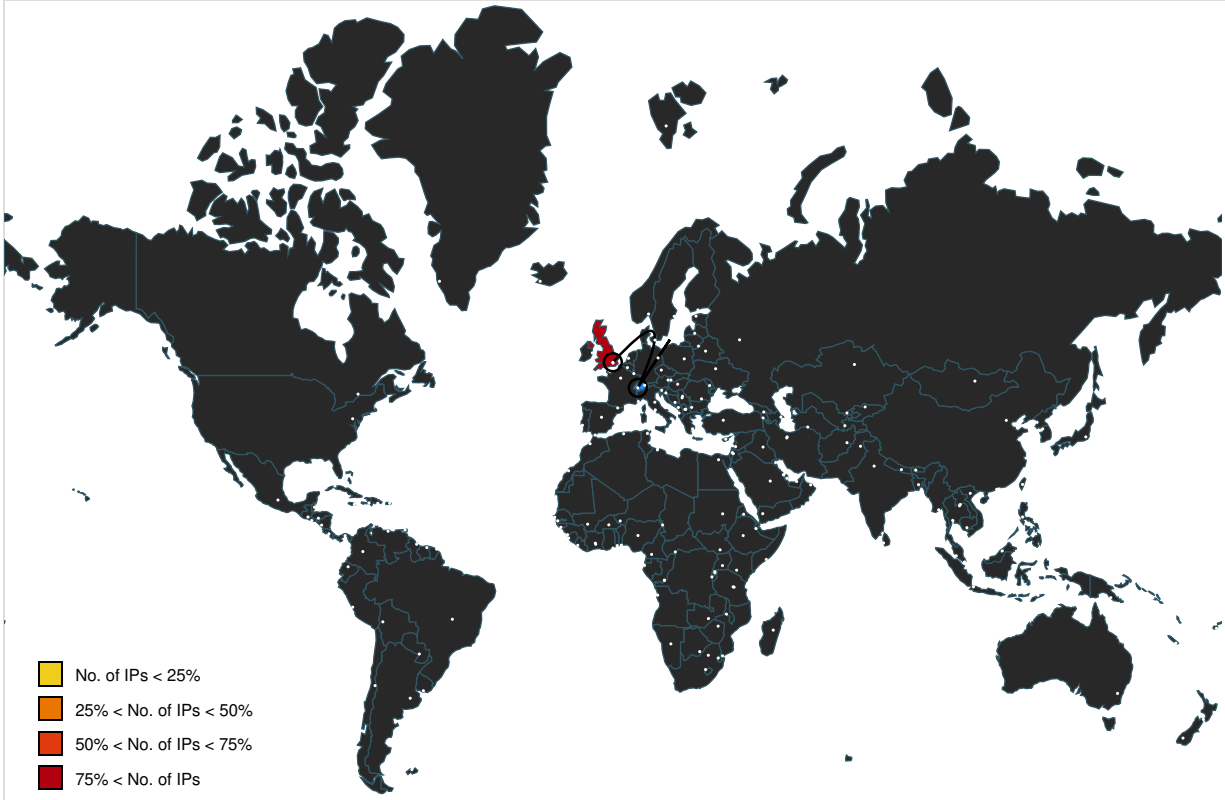
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers	shipping docs.exe, 00000000.00000002.279908957.0000000006732000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.245303030.0000000005479000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.245545950.000000000547D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	shipping docs.exe, 00000000.00000002.279908957.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.com	shipping docs.exe, 00000000.00000003.242487064.0000000005480000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org/bot5676971476:AAFdGsXW8kwzXNIluAGV-a4sJ2XBy68O9WI/1644584536%discordapi%yyy	VMqTMMD.exe, 00000015.00000002.518773451.0000000002E61000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.comteP$	shipping docs.exe, 00000000.00000003.239908062.0000000005493000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.240179699.0000000005493000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.240220486.0000000005493000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.239881609.0000000005491000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.240113755.0000000005493000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.sajatypeworks.com	shipping docs.exe, 00000000.00000002.279908957.0000000006732000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.240049534.0000000005494000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.239908062.0000000005493000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.240150934.0000000005494000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.240179699.0000000005493000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.240220486.0000000005493000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.239973997.0000000005494000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.240136652.0000000005494000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.239881609.0000000005491000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.239942097.0000000005494000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.240113755.0000000005493000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.240076834.0000000005494000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	shipping docs.exe, 00000000.00000002.279908957.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://JIQ1JKgQReGyOBe.com	VMqTMMD.exe, 00000015.00000002.533512375.00000000031B2000.00000004.00000800.00020000.00000000.sdmp, VMqTMMD.exe, 00000015.00000002.518773451.0000000002E61000.00000004.00000800.00020000.00000000.sdmp, VMqTMMD.exe, 00000015.00000002.534481256.00000000031E8000.00000004.00000800.00020000.00000000.sdmp, VMqTMMD.exe, 00000015.00000002.534906198.0000000003201000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/cThe	shipping docs.exe, 00000000.00000002.279908957.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krigh	shipping docs.exe, 00000000.00000003.241289310.0000000005479000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot5676971476:AAFdGsXW8kwzXNIluAGV-a4sJ2XBy68O9WI/	shipping docs.exe, 00000003.00000002.518422910.0000000002FA1000.00000004.00000800.00020000.00000000.sdmp, yVGAJfiVEvtg.exe, 00000012.00000002.520653491.00000000030C1000.00000004.00000800.00020000.00000000.sdmp, VMqTMMD.exe, 00000015.00000002.518773451.0000000002E61000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/staff/dennis.htm	shipping docs.exe, 00000000.00000002.279908957.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	shipping docs.exe, 00000000.00000002.279908957.0000000006732000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.240423951.000000000548B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comgrita	shipping docs.exe, 00000000.00000003.264268952.0000000005470000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org4	shipping docs.exe, 00000003.00000002.534292549.0000000003336000.00000004.00000800.00020000.00000000.sdmp, yVGAJfiVEvtg.exe, 00000012.00000002.537543749.000000000349A000.00000004.00000800.00020000.00000000.sdmp, VMqTMMD.exe, 00000015.00000002.534577687.00000000031EE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://Unbjpy.com	VMqTMMD.exe, 00000015.00000002.518773451.0000000002E61000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.krT	shipping docs.exe, 00000000.00000003.241289310.0000000005479000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	VMqTMMD.exe, 00000015.00000002.518773451.0000000002E61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.comtteJ	shipping docs.exe, 00000000.00000003.240136652.0000000005494000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	shipping docs.exe, 00000000.00000002.279908957.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/O	shipping docs.exe, 00000000.00000003.243601775.0000000005474000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	shipping docs.exe, 00000000.00000002.279908957.0000000006732000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.240126460.000000000548B000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.240159233.000000000548B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	shipping docs.exe, 00000000.00000002.279908957.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	shipping docs.exe, 00000000.00000002.279908957.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/$	shipping docs.exe, 00000000.00000003.243601775.0000000005474000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	shipping docs.exe, 00000000.00000002.279908957.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	shipping docs.exe, 00000000.00000002.265489624.0000000002481000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000003.00000002.534292549.0000000003336000.00000004.00000800.00020000.00000000.sdmp, yVGAJfiVEvtg.exe, 00000004.00000002.364468167.0000000002C61000.00000004.00000800.00020000.00000000.sdmp, VMqTMMD.exe, 0000000F.00000002.373989607.0000000002D06000.00000004.00000800.00020000.00000000.sdmp, yVGAJfiVEvtg.exe, 00000012.00000002.537543749.000000000349A000.00000004.00000800.00020000.00000000.sdmp, VMqTMMD.exe, 00000015.00000002.534577687.00000000031EE000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	shipping docs.exe, 00000000.00000002.279908957.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y	shipping docs.exe, 00000000.00000003.243601775.0000000005474000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	shipping docs.exe, 00000000.00000002.279908957.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	shipping docs.exe, 00000000.00000002.279908957.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	shipping docs.exe, 00000003.00000002.518422910.0000000002FA1000.00000004.00000800.00020000.00000000.sdmp, yVGAJfiVEvtg.exe, 00000012.00000002.520653491.00000000030C1000.00000004.00000800.00020000.00000000.sdmp, VMqTMMD.exe, 00000015.00000002.518773451.0000000002E61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	shipping docs.exe, 00000000.00000003.243601775.0000000005474000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.w	shipping docs.exe, 00000000.00000003.239628147.0000000000BDD000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/=	shipping docs.exe, 00000000.00000003.243601775.0000000005474000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/ko	shipping docs.exe, 00000000.00000003.243601775.0000000005474000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	shipping docs.exe, 00000000.00000002.279908957.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	shipping docs.exe, 00000000.00000003.242044098.0000000005474000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	shipping docs.exe, 00000000.00000002.279908957.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	shipping docs.exe, 00000000.00000002.279908957.0000000006732000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.241799498.00000000054AD000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.241823423.0000000005474000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.242049495.0000000005479000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers-	shipping docs.exe, 00000000.00000003.245303030.0000000005479000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/frere-jones.html	shipping docs.exe, 00000000.00000002.279908957.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comm	shipping docs.exe, 00000000.00000003.264268952.0000000005470000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	shipping docs.exe, 00000000.00000002.279908957.0000000006732000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.243601775.0000000005474000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	shipping docs.exe, 00000000.00000002.279908957.0000000006732000.00000004.00000800.00020000.00000000.sdmp	false		high
http://api.telegram.org	shipping docs.exe, 00000003.00000002.534617829.000000000334B000.00000004.00000800.00020000.00000000.sdmp, yVGAJfiVEvtg.exe, 00000012.00000002.537871887.00000000034AF000.00000004.00000800.00020000.00000000.sdmp, VMqTMMD.exe, 00000015.00000002.534906198.0000000003201000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cnu-h	shipping docs.exe, 00000000.00000003.241799498.00000000054AD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com8	shipping docs.exe, 00000000.00000003.240136652.0000000005494000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.240113755.0000000005493000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn%	shipping docs.exe, 00000000.00000003.241799498.00000000054AD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnlJ	shipping docs.exe, 00000000.00000003.241823423.0000000005474000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.242158018.000000000547B000.00000004.00000800.00020000.00000000.sdmp, shipping docs.exe, 00000000.00000003.242049495.0000000005479000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
149.154.167.220	api.telegram.org	United Kingdom		62041	TELEGRAMRU	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756232
Start date and time:	2022-11-29 21:18:08 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 43s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	shipping docs.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
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@19/9@3/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 209.197.3.8
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, wu-bg-shim.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:19:06	API Interceptor	602x Sleep call for process: shipping docs.exe modified
21:19:09	Task Scheduler	Run new task: yVGAJfiVEvtg path: C:\Users\user\AppData\Roaming\yVGAJfiVEvtg.exe
21:19:18	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run VMqTMMD C:\Users\user\AppData\Roaming\VMqTMMD\VMqTMMD.exe
21:19:26	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run VMqTMMD C:\Users\user\AppData\Roaming\VMqTMMD\VMqTMMD.exe
21:19:28	API Interceptor	113x Sleep call for process: yVGAJfiVEvtg.exe modified
21:19:41	API Interceptor	193x Sleep call for process: VMqTMMD.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\AppData\Roaming\VMqTMMD\VMqTMMD.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	false
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..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

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

Process:	C:\Users\user\Desktop\shipping docs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	**true**
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..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

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

Process:	C:\Users\user\AppData\Roaming\yVGAJfiVEvtg.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216

Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	false
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, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Cultur e=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.Con figuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp3418.tmp

Process:	C:\Users\user\AppData\Roaming\VMqTMMD\VMqTMMD.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.196605565254392
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBx3tn:cbh47TlNQ//rydbz9I3YODOLNdq3jd
MD5:	FD5E93C3EBB783A2036F64992EA982BD
SHA1:	3D41B17EFE57C343E7C40FAD2F14EFEA143CB502
SHA-256:	9BD161BA3D8CD57B581AF3CB7879BCC2FE34A62E2C3BCF3B8CEA9E3FAD9DDCE2
SHA-512:	0707F1A58755FD8E38E22E5352C84FFE372C7F621A3EE48EE389AD5AC35F6AAE64696F59F032148D5B31913100A093777DA331B59FDE3ACA82B3E1549145E70C
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Pri ncipal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatte ries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmp7934.tmp

Process:	C:\Users\user\Desktop\shipping docs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.196605565254392
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBx3tn:cbh47TlNQ//rydbz9I3YODOLNdq3jd
MD5:	FD5E93C3EBB783A2036F64992EA982BD
SHA1:	3D41B17EFE57C343E7C40FAD2F14EFEA143CB502
SHA-256:	9BD161BA3D8CD57B581AF3CB7879BCC2FE34A62E2C3BCF3B8CEA9E3FAD9DDCE2
SHA-512:	0707F1A58755FD8E38E22E5352C84FFE372C7F621A3EE48EE389AD5AC35F6AAE64696F59F032148D5B31913100A093777DA331B59FDE3ACA82B3E1549145E70C
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Pri ncipal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatte ries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmpF5B7.tmp

Process:	C:\Users\user\AppData\Roaming\yVGAJfiVEvtg.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.196605565254392
Encrypted:	false

SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBx3tn:cbh47TINQ//rydbz9I3YODOLNdq3jd
MD5:	FD5E93C3EBB783A2036F64992EA982BD
SHA1:	3D41B17EFE57C343E7C40FAD2F14EFEA143CB502
SHA-256:	9BD161BA3D8CD57B581AF3CB7879BCC2FE34A62E2C3BCF3B8CEA9E3FAD9DDCE2
SHA-512:	0707F1A58755FD8E38E22E5352C84FFE372C7F621A3EE48EE389AD5AC35F6AAE64696F59F032148D5B31913100A093777DA331B59FDE3ACA82B3E1549145E70C
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\VMqTMMD\VMqTMMD.exe

Process:	C:\Users\user\Desktop\shipping docs.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	606720
Entropy (8bit):	7.88879203859592
Encrypted:	false
SSDEEP:	12288:ks2kzrbETClbHskFgFwIyXCDl+s30ki9Pi00uSGD6DWzEH:1176ChskFgqIyXoi9Pi00uSTHH
MD5:	6308AE755A893C15A989B1CCF2C56393
SHA1:	00ADA70AA14A5CF26A7F8CECBAAA437267D30A2A
SHA-256:	9DFDB5048599B1083FE534CF5FE5A0440D71EB74B5497E506F0A0A4C23821F40
SHA-512:	E03EAC82BF4174912D63CB8ECEED393320FE957F7A735FF0F720FBF558F9638E6FC051CB80607864CAAA8366CA0EDC2D44028367EF97D8020AD7B6F45EADDCD3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 73%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....U.c.....0.....N... ...`....@.. ..@.....N..W....`.. ....H.....text..... ...0..... ..`.rsrc... ....`.....2.....@..@.rel oc.....@.....@..B.....N.....H.....U.....4...X...(^.....z.(.....}.....(...o!...}....*..0.....{.....3.....(....*.....0.....{..... ,....f.....}.....}.....}.....s....o....}.....}....8.....{....o....}.....{....}.....}.....{.....Y}.....{....-...+H.{.....{....X.{....X .;.|.{....Xa}.....}.....{....o....:q....(....+..(.....}.....(.....*..... .....n..}.....{.....,.{....o....*..{....*.s".

C:\Users\user\AppData\Roaming\VMqTMMD\VMqTMMD.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\shipping docs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\yVGAJfiVEvtg.exe

Process:	C:\Users\user\Desktop\shipping docs.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	606720
Entropy (8bit):	7.88879203859592
Encrypted:	false
SSDEEP:	12288:ks2kzrbETClbHskFgFwIyXCDl+s30ki9Pi00uSGD6DWzEH:1176ChskFgqIyXoi9Pi00uSTHH
MD5:	6308AE755A893C15A989B1CCF2C56393
SHA1:	00ADA70AA14A5CF26A7F8CECBAAA437267D30A2A
SHA-256:	9DFDB5048599B1083FE534CF5FE5A0440D71EB74B5497E506F0A0A4C23821F40

SHA-512:	E03EAC82BF4174912D63CB8ECEED393320FE957F7A735FF0F720FBF558F9638E6FC051CB80607864CAAA8366CA0EDC2D44028367EF97D8020AD7B6F45EADDCD3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 73%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....U.c.....0.....N... ...`....@.. ..... ..@.....N..W....`. ....H.....text..... ...0..... ..`.rsrc... ....`.....2.....@..@.rel oc.....@.....@..B.....N.....H.....U.....4...X...(^.....z.(.....}.....(...o!...}....*..0.....{.....3.....(.....*.....0.....{..... ,....f.....}.....}.....}.....s....o....}.....}....8.....{....o....}.....{....}.....}.....}.....{.....Y}.....{....-...+H.{.....{....X.{....X .;.|.{....Xa}.....}.....{....o....:q....(....+..(.....}.....(.....*..... .....n..}.....{.....,..{....o....*..{....*.s".

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.88879203859592
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	shipping docs.exe
File size:	606720
MD5:	6308ae755a893c15a989b1ccf2c56393
SHA1:	00ada70aa14a5cf26a7f8cecbaaa437267d30a2a
SHA256:	9dfdb5048599b1083fe534cf5fe5a0440d71eb74b5497e506f0a0a4c23821f40
SHA512:	e03eac82bf4174912d63cb8eceed393320fe957f7a735ff0f720fbf558f9638e6fc051cb80607864caaa8366ca0edc2d44028367ef97d8020ad7b6f45eaddcd3
SSDEEP:	12288:ks2kzrbETClbHskFgFwIyXCDl+s30ki9Pi00uSGD6DWzEH:1176ChskFgqIyXoi9Pi00uSTHH
TLSH:	D9D4023C224ABE2FC6BC99B958D296006FF1CD4D6110EF396EEE21D957CB3382741592
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....U.c.....0.....N... ...`....@.. .....@.....

File Icon

Icon Hash:	828282a28c323068

Static PE Info

General

Entrypoint:	0x494eee
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x638455A2 [Mon Nov 28 06:30:58 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x94e94	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x96000	0xc20	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x98000	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	0x92ef4	0x93000	False	0.8968630420918368	data	7.898839095668671	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x96000	0xc20	0xe00	False	0.5340401785714286	data	5.558555904519806	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x98000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x960e8	0x7a7	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0x96890	0x14	data		
RT_VERSION	0x968a4	0x37c	data		

Imports

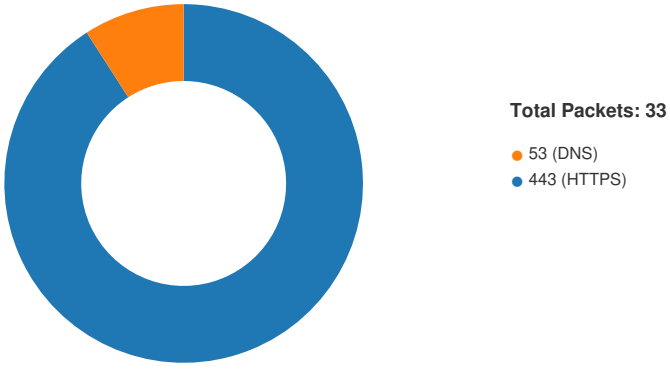
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3149.154.167.220496994432851779 11/29/22-21:19:34.793087	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49699	443	192.168.2.3	149.154.167.220
192.168.2.3149.154.167.220497004432851779 11/29/22-21:20:32.964256	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49700	443	192.168.2.3	149.154.167.220
192.168.2.3149.154.167.220497014432851779 11/29/22-21:20:48.592868	TCP	2851779	ETPRO TROJAN Agent Tesla Telegram Exfil	49701	443	192.168.2.3	149.154.167.220

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 21:19:34.306422949 CET	49699	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:19:34.306468010 CET	443	49699	149.154.167.220	192.168.2.3
Nov 29, 2022 21:19:34.306538105 CET	49699	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:19:34.350533009 CET	49699	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:19:34.350590944 CET	443	49699	149.154.167.220	192.168.2.3
Nov 29, 2022 21:19:34.426537037 CET	443	49699	149.154.167.220	192.168.2.3
Nov 29, 2022 21:19:34.426740885 CET	49699	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:19:34.431344986 CET	49699	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:19:34.431368113 CET	443	49699	149.154.167.220	192.168.2.3
Nov 29, 2022 21:19:34.431643009 CET	443	49699	149.154.167.220	192.168.2.3
Nov 29, 2022 21:19:34.495279074 CET	49699	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:19:34.762609005 CET	49699	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:19:34.762672901 CET	443	49699	149.154.167.220	192.168.2.3
Nov 29, 2022 21:19:34.789762020 CET	443	49699	149.154.167.220	192.168.2.3
Nov 29, 2022 21:19:34.792854071 CET	49699	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:19:34.792897940 CET	443	49699	149.154.167.220	192.168.2.3
Nov 29, 2022 21:19:34.934180021 CET	443	49699	149.154.167.220	192.168.2.3
Nov 29, 2022 21:19:34.934380054 CET	443	49699	149.154.167.220	192.168.2.3
Nov 29, 2022 21:19:34.934495926 CET	49699	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:19:34.941884995 CET	49699	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:20:32.434153080 CET	49700	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:20:32.434236050 CET	443	49700	149.154.167.220	192.168.2.3
Nov 29, 2022 21:20:32.434340954 CET	49700	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:20:32.453962088 CET	49700	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:20:32.454035997 CET	443	49700	149.154.167.220	192.168.2.3
Nov 29, 2022 21:20:32.529711962 CET	443	49700	149.154.167.220	192.168.2.3
Nov 29, 2022 21:20:32.529877901 CET	49700	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:20:32.532382011 CET	49700	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:20:32.532432079 CET	443	49700	149.154.167.220	192.168.2.3
Nov 29, 2022 21:20:32.532835007 CET	443	49700	149.154.167.220	192.168.2.3
Nov 29, 2022 21:20:32.640913963 CET	49700	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:20:32.929069042 CET	49700	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:20:32.929147959 CET	443	49700	149.154.167.220	192.168.2.3
Nov 29, 2022 21:20:32.956907034 CET	443	49700	149.154.167.220	192.168.2.3
Nov 29, 2022 21:20:32.963989973 CET	49700	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:20:32.964052916 CET	443	49700	149.154.167.220	192.168.2.3
Nov 29, 2022 21:20:33.190849066 CET	443	49700	149.154.167.220	192.168.2.3
Nov 29, 2022 21:20:33.191063881 CET	443	49700	149.154.167.220	192.168.2.3
Nov 29, 2022 21:20:33.191247940 CET	49700	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:20:33.191715002 CET	49700	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:20:47.552496910 CET	49701	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:20:47.552612066 CET	443	49701	149.154.167.220	192.168.2.3
Nov 29, 2022 21:20:47.552792072 CET	49701	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:20:47.617912054 CET	49701	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:20:47.617959023 CET	443	49701	149.154.167.220	192.168.2.3
Nov 29, 2022 21:20:47.682044029 CET	443	49701	149.154.167.220	192.168.2.3
Nov 29, 2022 21:20:47.682136059 CET	49701	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:20:47.684530973 CET	49701	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:20:47.684552908 CET	443	49701	149.154.167.220	192.168.2.3
Nov 29, 2022 21:20:47.684855938 CET	443	49701	149.154.167.220	192.168.2.3
Nov 29, 2022 21:20:47.890943050 CET	443	49701	149.154.167.220	192.168.2.3
Nov 29, 2022 21:20:47.891128063 CET	49701	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:20:48.564800978 CET	49701	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:20:48.564868927 CET	443	49701	149.154.167.220	192.168.2.3
Nov 29, 2022 21:20:48.591984034 CET	443	49701	149.154.167.220	192.168.2.3
Nov 29, 2022 21:20:48.592714071 CET	49701	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:20:48.592767954 CET	443	49701	149.154.167.220	192.168.2.3
Nov 29, 2022 21:20:48.679336071 CET	443	49701	149.154.167.220	192.168.2.3
Nov 29, 2022 21:20:48.679500103 CET	443	49701	149.154.167.220	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 21:20:48.679678917 CET	49701	443	192.168.2.3	149.154.167.220
Nov 29, 2022 21:20:48.680298090 CET	49701	443	192.168.2.3	149.154.167.220

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 21:19:34.235759974 CET	49977	53	192.168.2.3	8.8.8.8
Nov 29, 2022 21:19:34.253768921 CET	53	49977	8.8.8.8	192.168.2.3
Nov 29, 2022 21:20:32.392975092 CET	57840	53	192.168.2.3	8.8.8.8
Nov 29, 2022 21:20:32.412163019 CET	53	57840	8.8.8.8	192.168.2.3
Nov 29, 2022 21:20:47.509844065 CET	57990	53	192.168.2.3	8.8.8.8
Nov 29, 2022 21:20:47.527040005 CET	53	57990	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 21:19:34.235759974 CET	192.168.2.3	8.8.8.8	0x7d34	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:20:32.392975092 CET	192.168.2.3	8.8.8.8	0xd170	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:20:47.509844065 CET	192.168.2.3	8.8.8.8	0x8851	Standard query (0)	api.telegram.org	A (IP address)	IN (0x0001)	false

DNS Answers

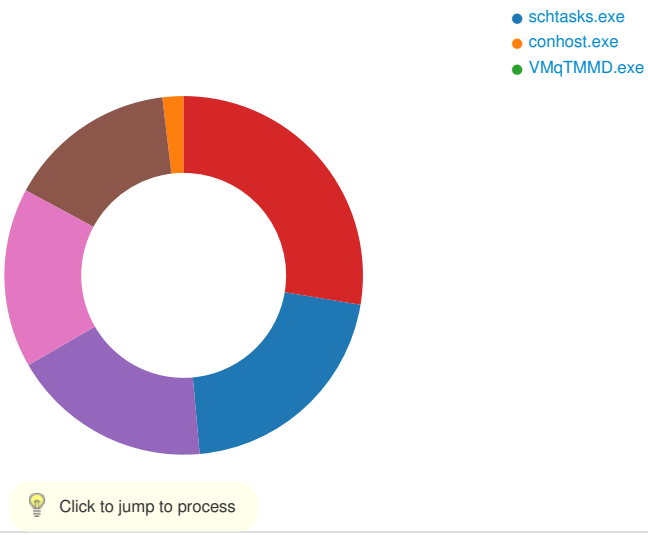
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 21:18:52.397281885 CET	8.8.8.8	192.168.2.3	0x741b	No error (0)	au.c-0001.c-msedge.net	c-0001.c-msedge.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 21:18:52.397281885 CET	8.8.8.8	192.168.2.3	0x741b	No error (0)	c-0001.c-msedge.net		13.107.4.50	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:19:34.253768921 CET	8.8.8.8	192.168.2.3	0x7d34	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:20:32.412163019 CET	8.8.8.8	192.168.2.3	0xd170	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)	false
Nov 29, 2022 21:20:47.527040005 CET	8.8.8.8	192.168.2.3	0x8851	No error (0)	api.telegram.org		149.154.167.220	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- api.telegram.org

Statistics

Behavior



System Behavior

Analysis Process: shipping docs.exe PID: 2400, Parent PID: 3452

General

Target ID:	0
Start time:	21:18:57
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\shipping docs.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\shipping docs.exe
Imagebase:	0x140000
File size:	606720 bytes
MD5 hash:	6308AE755A893C15A989B1CCF2C56393
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.270616747.00000000034A9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.270616747.00000000034A9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.270616747.00000000034A9000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3CCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3CCF06	unknown
C:\Users\user\AppData\Roaming\yVGAJfiVEvtg.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C211E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp7934.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C217038	GetTempFileNameW

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

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7934.tmp	success or wait	1	6C216A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\yVGAJfiVEvtg.exe	0	606720	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 55 fd 63 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 06 00 00 30 09 00 00 10 00 00 00 00 00 00 fd 4e 09 00 00 20 00 00 00 60 09 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 09 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELUc0N `@ @	success or wait	1	6C211B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp7934.tmp	0	1645	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft .com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user </Author> </RegistrationIn	success or wait	1	6C211B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\shipping docs.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 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",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D6DC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C211B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C211B4F	ReadFile
C:\Users\user\Desktop\shipping docs.exe	unknown	606720	success or wait	1	6C211B4F	ReadFile

Analysis Process: schtasks.exe PID: **5248**, Parent PID: **2400**

General

Target ID:	1
Start time:	21:19:08
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\yVGAJfiVEvtg" /XML "C:\Users\user\AppData\Local\Temp\tmp7934.tmp
Imagebase:	0xe0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7934.tmp	unknown	2	success or wait	1	EAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7934.tmp	unknown	1646	success or wait	1	EABD9	ReadFile

Analysis Process: conhost.exe PID: **5220**, Parent PID: **5248**

General

Target ID:	2
Start time:	21:19:08
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: shipping docs.exe PID: **3776**, Parent PID: **2400**

General

Target ID:	3
Start time:	21:19:09
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\shipping docs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xbb0000
File size:	606720 bytes
MD5 hash:	6308AE755A893C15A989B1CCF2C56393
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.262419819.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.262419819.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000003.00000000.262419819.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.518422910.0000000002FA1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000003.00000002.518422910.0000000002FA1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.518422910.0000000002FA1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3CCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3CCF06	unknown
C:\Users\user\AppData\Roaming\VMqTMMD	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C21BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\VMqTMMD\VMqTMMD.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C21DD66	CopyFileW
C:\Users\user\AppData\Roaming\VMqTMMD\VMqTMMD.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C21DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp4957.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C217038	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\VMqTMMD\VMqTMMD.exe:Zone.Identifier	success or wait	1	61F86DA	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\VMqTMMD\VMqTMMD.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 55 fd 63 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 06 00 00 30 09 00 00 10 00 00 00 00 00 00 fd 4e 09 00 00 20 00 00 00 60 09 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 09 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELUc0N `@ @	success or wait	3	6C21DD66	CopyFileW
C:\Users\user\AppData\Roaming\VMqTMMD\VMqTMMD.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	6C21DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3A5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D3A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C211B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C211B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C211B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C211B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C211B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\812f1102-a14c-4a8d-9bed-0b62191d8809	unknown	4096	success or wait	1	6C211B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C211B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	6C211B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

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

Analysis Process: yVGAJfiVEvtg.exe PID: **4552**, Parent PID: **1080**

General

Target ID:	4
Start time:	21:19:09
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\yVGAJfiVEvtg.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\yVGAJfiVEvtg.exe
Imagebase:	0x8f0000
File size:	606720 bytes
MD5 hash:	6308AE755A893C15A989B1CCF2C56393
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.365709519.0000000002CA7000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 73%, 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	6D3CCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3CCF06	unknown
C:\Users\user\AppData\Local\Temp\tmpF5B7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C217038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\yVGAJfiVEvtg.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6DC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF5B7.tmp	success or wait	1	6C216A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF5B7.tmp	0	1645	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationIn	success or wait	1	6C211B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\yVGAJfiVEvtg.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D6DC907	WriteFile

File Read

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

Analysis Process: VMqTMMD.exe PID: **1280**, Parent PID: **3452**

General

Target ID:	14
Start time:	21:19:26
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\VMqTMMD\VMqTMMD.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\VMqTMMD\VMqTMMD.exe"
Imagebase:	0x9a0000
File size:	606720 bytes
MD5 hash:	6308AE755A893C15A989B1CCF2C56393
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000E.00000002.343723068.0000000002D38000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 73%, 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	6D3CCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3CCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\VMqTMMD.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D6DC78D	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\VMqTMMD.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D6DC907	WriteFile

File Read

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C211B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C211B4F	ReadFile

Analysis Process: VMqTMMD.exe PID: **3124**, Parent PID: **3452**

General

Target ID:	15
Start time:	21:19:36
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\VMqTMMD\VMqTMMD.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\VMqTMMD\VMqTMMD.exe"
Imagebase:	0x7f0000
File size:	606720 bytes
MD5 hash:	6308AE755A893C15A989B1CCF2C56393
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3CCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D3CCF06	unknown
C:\Users\user\AppData\Local\Temp\tmp3418.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C217038	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp3418.tmp	success or wait	1	6C216A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp3418.tmp	0	1645	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationIn	success or wait	1	6C211B4F	WriteFile

File Read

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

Analysis Process: schtasks.exe PID: **4792**, Parent PID: **4552**

General

Target ID:	16
Start time:	21:19:41
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\yVGAJfiVEvtg" /XML "C:\Users\user\AppData\Local\Temp\tmpF5B7.tmp
Imagebase:	0xe0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Reputation:	high

Analysis Process: conhost.exe PID: **4536**, Parent PID: **4792**

General	
Target ID:	17
Start time:	21:19:42
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: yVGAJfiVEvtg.exe PID: **3680**, Parent PID: **4552**

General	
Target ID:	18
Start time:	21:19:44
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\yVGAJfiVEvtg.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xaf0000
File size:	606720 bytes
MD5 hash:	6308AE755A893C15A989B1CCF2C56393
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.520653491.00000000030C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000012.00000002.520653491.00000000030C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000002.520653491.00000000030C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: schtasks.exe PID: **4184**, Parent PID: **3124**

General	
Target ID:	19
Start time:	21:19:56
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\yVGAJfiVEvtg" /XML "C:\Users\user\AppData\Local\Temp\tmp3418.tmp
Imagebase:	0xe0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: **4404**, Parent PID: **4184**

General	
Target ID:	20
Start time:	21:19:57
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: VMqTMMD.exe PID: **5228**, Parent PID: **3124**

General	
Target ID:	21
Start time:	21:19:57
Start date:	29/11/2022
Path:	C:\Users\user\AppData\Roaming\VMqTMMD\VMqTMMD.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x9a0000
File size:	606720 bytes
MD5 hash:	6308AE755A893C15A989B1CCF2C56393
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000015.00000002.518773451.0000000002E61000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000015.00000002.518773451.0000000002E61000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000015.00000002.518773451.0000000002E61000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security

Disassembly

No disassembly