ID: 876162
Sample Name:
shipmentReceipt(22kb).pdf__customInvoice12074408.exe
Cookbook: default.jbs
Time: 11:39:13
Date: 26/05/2023
Version: 37.1.0 Beryl

Table of Contents

Copyright Joe Security LLC 2023

Copyright Joe Security LLC 2023

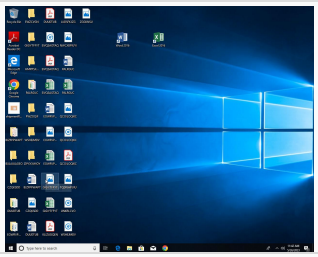
Windows Analysis Report

shipmentReceipt(22kb).pdf__customInvoice12074408.exe

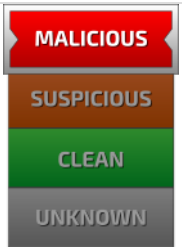
Overview

General Information

Sample Name:	shipmentReceipt(22kb).pdf__customInvoice12074408.exe
Analysis ID:	876162
MD5:	278d48d9ea2fe..
SHA1:	30a693e39b77…
SHA256:	53823b0378b9…
Tags:	exe
Infos:	



Detection



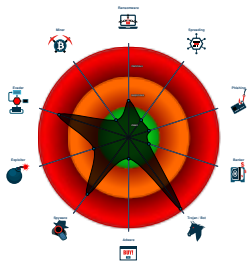
AgentTesla, zgRAT

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected zgRAT
- Malicious sample detected (through…
- Yara detected Telegram RAT
- Yara detected AgentTesla
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fi…
- Initial sample is a PE file and has a…

Classification



Process Tree

- **System is w10x64**
- shipmentReceipt(22kb).pdf__customInvoice12074408.exe (PID: 6492 cmdline: C:\Users\user\Desktop\shipmentReceipt(22kb).pdf__customInvoice12074408.exe MD5: 278D48D9EA2FE8350796279E5D08A72A)
  - shipmentReceipt(22kb).pdf__customInvoice12074408.exe (PID: 6684 cmdline: C:\Users\user\Desktop\shipmentReceipt(22kb).pdf__customInvoice12074408.exe MD5: 278D48D9EA2FE8350796279E5D08A72A)
  - shipmentReceipt(22kb).pdf__customInvoice12074408.exe (PID: 6672 cmdline: C:\Users\user\Desktop\shipmentReceipt(22kb).pdf__customInvoice12074408.exe MD5: 278D48D9EA2FE8350796279E5D08A72A)
  - shipmentReceipt(22kb).pdf__customInvoice12074408.exe (PID: 6764 cmdline: C:\Users\user\Desktop\shipmentReceipt(22kb).pdf__customInvoice12074408.exe MD5: 278D48D9EA2FE8350796279E5D08A72A)
- kmk.exe (PID: 2400 cmdline: "C:\Users\user\AppData\Roaming\kmk\kmk.exe" MD5: 278D48D9EA2FE8350796279E5D08A72A)
  - kmk.exe (PID: 4588 cmdline: C:\Users\user\AppData\Roaming\kmk\kmk.exe MD5: 278D48D9EA2FE8350796279E5D08A72A)
- kmk.exe (PID: 3276 cmdline: "C:\Users\user\AppData\Roaming\kmk\kmk.exe" MD5: 278D48D9EA2FE8350796279E5D08A72A)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Agent Tesla, AgentTesla	A .NET based keylogger and RAT readily available to actors. Logs keystrokes and the host's clipboard and beacons this information back to the C2.	• SWEED	http://blog.nsfocus.net/sweed-611/http://l1v1ngc0d3.wordpress.com/2021/11/12/agenttesla-dropped-via-nsis-installer/http://www.secureworks.com/research/threat-profiles/gold-galleonhttps://asec.ahnlab.com/ko/29133/https://blog.apnic.net/2022/03/31/how-to-detect-and-prevent-common-data-exfiltration-attacks/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.agent_tesla

Name	Description	Attribution	Blogpost URLs	Link

Name	Description	Attribution	Blogpost URLs	Link
zgRAT		No Attribution	http://https://bazaar.abuse.ch/browse/signature/zgRAT/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.zgrat

Malware Configuration

Threatname: Telegram RAT


```
{
  "C2 url": "https://api.telegram.org/bot1360033246:AAF6H8m6YrL09doyxtsvJzZ_cIl__BCF4aU/sendMessage"
}
```


Threatname: Agenttesla


```
{
  "Exfil Mode": "Telegram",
  "Telegram Url": "https://api.telegram.org/bot1360033246:AAF6H8m6YrL09doyxtsvJzZ_cIl__BCF4aU/sendDocumentsendMessage?chat_id=document"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.799586620.0000000000430000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x1696:$a11: get_securityProfile • 0x1537:$a12: get_useSeparateFolderTree • 0x1946:$a14: get_archivingScope • 0x176e:$a15: get_providerName • 0x12fd:$a20: get_LastAccessed • 0x19e0:$a21: get_avatarType • 0x17eb:$a26: set_accountName • 0xc94:$a28: set_bindingConfigurationUID • 0x1846:$a31: set_username • 0x13e8:$a33: get_Clipboard • 0x13f6:$a34: get_Keyboard • 0x1403:$a37: get_Password
00000005.00000002.804401224.0000000003012000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.804401224.0000000003012000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.573264210.0000000004D80000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.573264210.0000000004D80000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 30 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.shipmentReceipt(22kb).pdf__customInvoice12074408.exe.44d1788.5.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.shipmentReceipt(22kb).pdf__customInvoice12074408.exe.44d1788.5.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.shipmentReceipt(22kb).pdf__customInvoice12074408.exe.44d1788.5.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x2e600:$s1: get_kbok • 0x2ef34:$s2: get_CHoo • 0x2fb8f:$s3: set_passwordIsSet • 0x2e404:$s4: get_enableLog • 0x32b27:$s8: torbrowser • 0x3150a:$s10: logins • 0x30dd8:$s11: credential • 0x2d7e8:$g1: get_Clipboard • 0x2d7f6:$g2: get_Keyboard • 0x2d803:$g3: get_Password • 0x2ede2:$g4: get_CtrlKeyDown • 0x2edf2:$g5: get_ShiftKeyDown • 0x2ee03:$g6: get_AltKeyDown

Copyright Joe Security LLC 2023

Source	Rule	Description	Author	Strings
0.2.shipmentReceipt(22kb).pdf__customInvoice12074408.exe.44d1788.5.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x2eb45:$a3: MailAccountConfiguration • 0x2eb5e:$a5: SmtpAccountConfiguration • 0x2eb25:$a8: set_BindingAccountConfiguration • 0x2da96:$a11: get_securityProfile • 0x2d937:$a12: get_useSeparateFolderTree • 0x2f288:$a13: get_DnsResolver • 0x2dd46:$a14: get_archivingScope • 0x2db6e:$a15: get_providerName • 0x30273:$a17: get_priority • 0x2f847:$a18: get_advancedParameters • 0x2ec5f:$a19: get_disabledByRestriction • 0x2d6fd:$a20: get_LastAccessed • 0x2dde0:$a21: get_avatarType • 0x2f95e:$a22: get_signaturePresets • 0x2e404:$a23: get_enableLog • 0x2dbeb:$a26: set_accountName • 0x2fda9:$a27: set_InternalServerPort • 0x2d094:$a28: set_bindingConfigurationUID • 0x2f924:$a29: set_IdnAddress • 0x30127:$a30: set_GuidMasterKey • 0x2dc46:$a31: set_username
0.2.shipmentReceipt(22kb).pdf__customInvoice12074408.exe.449bf68.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 48 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Antivirus / Scanner detection for submitted sample
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropped file
- Machine Learning detection for sample
- Machine Learning detection for dropped file

Networking

- Yara detected Generic Downloader

Key, Mouse, Clipboard, Microphone and Screen Capturing

- Installs a global keyboard hook

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, 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 zgRAT

Yara detected Telegram RAT

Yara detected AgentTesla

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

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

Remote Access Functionality

Yara detected zgRAT

Yara detected Telegram RAT

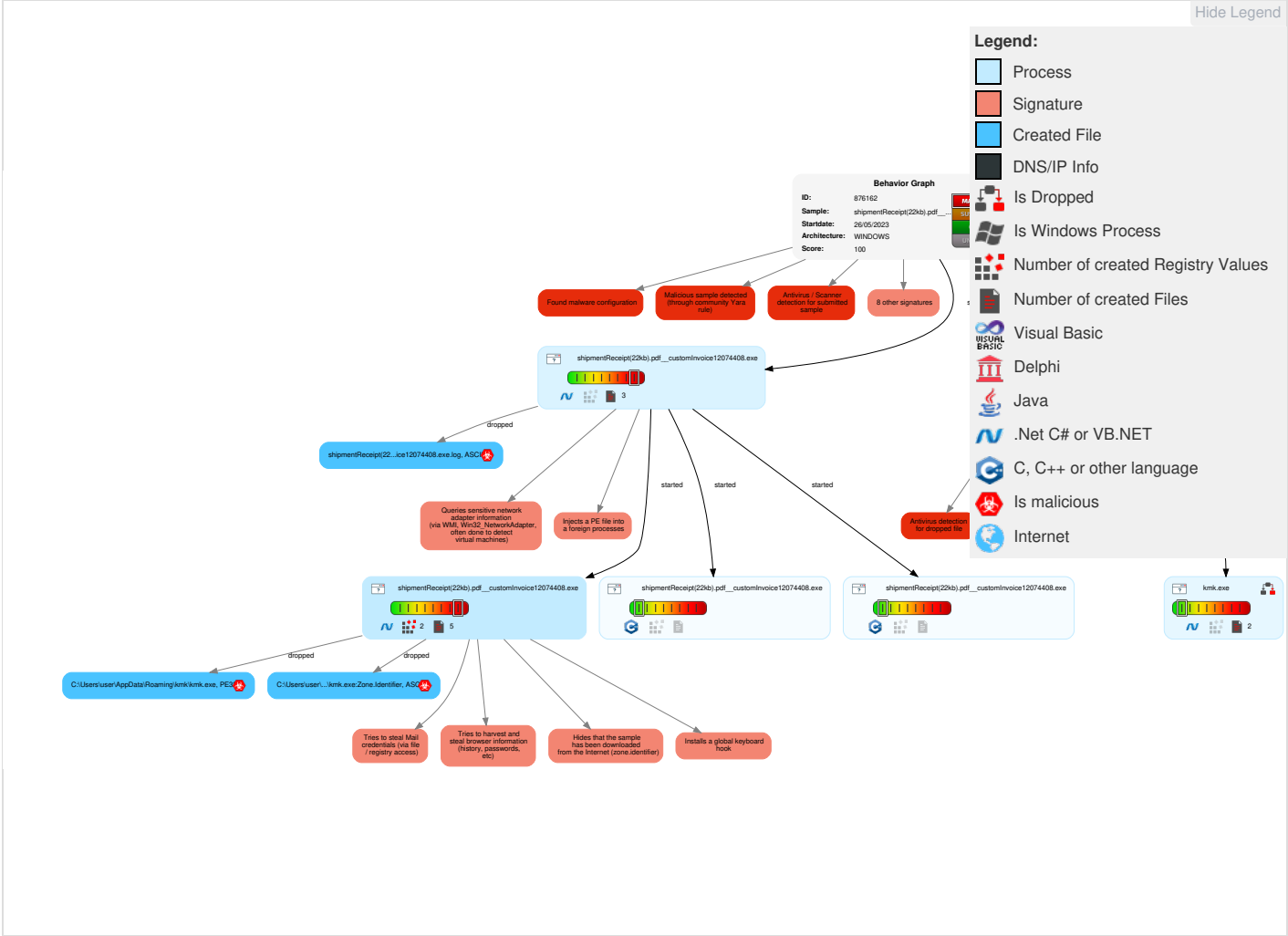
Yara detected AgentTesla

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	1 2 1 Windows Management Instrumentation	1 Registry Run Keys / Startup Folder	1 1 1 Process Injection	1 Masquerading	1 OS Credential Dumping	2 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 Disable or Modify Tools	1 1 1 Input Capture	1 Process Discovery	Remote Desktop Protocol	1 1 1 Input Capture	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 3 1 Virtualization/Sandbox Evasion	Security Account Manager	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Archive Collected Data	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	1 Data from Local System	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Hidden Files and Directories	LSA Secrets	2 4 System Information Discovery	SSH	1 Clipboard Data	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	3 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	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 2 Software Packing	DCSync	Network Sniffing	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 Timestomp	Proc Filesystem	Network Service Scanning	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

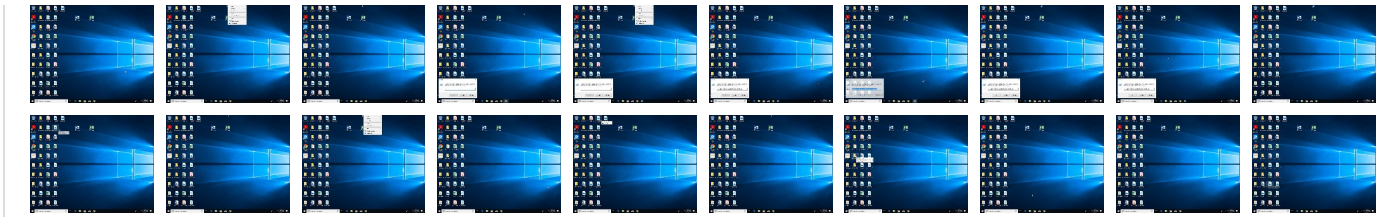


Screenshots

Thumbnails

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

Copyright Joe Security LLC 2023



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
shipmentReceipt(22kb).pdf__customInvoice12074408.exe	17%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	
shipmentReceipt(22kb).pdf__customInvoice12074408.exe	27%	Virustotal		Browse
shipmentReceipt(22kb).pdf__customInvoice12074408.exe	100%	Avira	HEUR/AGEN.1309734	
shipmentReceipt(22kb).pdf__customInvoice12074408.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\kmk\kmk.exe	100%	Avira	HEUR/AGEN.1309734	

Copyright Joe Security LLC 2023

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\kmk\kmk.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\kmk\kmk.exe	17%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cnN	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.comes	0%	URL Reputation	safe	
http://www.carterandcone.comdol	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.fontbureau.comdia	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://www.founder.com.cn/cnr-t	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/on	0%	URL Reputation	safe	
http://www.carterandcone.comg	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Sue	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn(	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.fontbureau.commpKF	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/uG	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp//r$	0%	Avira URL Cloud	safe	
http://en.wikiphD	0%	Avira URL Cloud	safe	
http://UZQtUP.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/CK	0%	Avira URL Cloud	safe	
http://www.carterandcone.comams/R	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp//r$	0%	Virustotal		Browse
http://www.fontbureau.commTTF	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/.Kp	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/yKM	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/oK?	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/fK(	0%	Avira URL Cloud	safe	

Copyright Joe Security LLC 2023

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cnsk	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/%Ki	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cnN	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000003.53910372 8.00000000064EC000.00000004.00000020.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://127.0.0.1:HTTP/1.1	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000005.00000002.80440122 4.0000000002F51000.00000004.00000800.000 20000.00000000.sdmp, kmk.exe, 00000007.0 0000002.803741749.0000000002D11000.00000 004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000002.57784884 7.0000000007632000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000002.57784884 7.0000000007632000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000002.57784884 7.0000000007632000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.commpKF	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000003.54748211 2.00000000064E3000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/uG	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000003.53923078 2.00000000064EC000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comes	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000003.53969349 2.00000000064E3000.00000004.00000020.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000002.57784884 7.0000000007632000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://UZQtUP.com	kmk.exe, 00000007.00000002.803741749.000 0000002D11000.00000004.00000800.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comdol	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000003.53969349 2.00000000064E3000.00000004.00000020.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000002.57784884 7.0000000007632000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp//r$	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000003.54033370 7.00000000064E7000.00000004.00000020.000 20000.00000000.sdmp, shipmentReceipt(22k b).pdf__customInvoice12074408.exe, 00000 000.00000003.540184473.00000000064E7000. 00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000002.57784884 7.0000000007632000.00000004.00000800.000 20000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.goodfont.co.kr	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000002.57784884 7.0000000007632000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.wikiphD	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000003.53864966 6.00000000064EE000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000002.57784884 7.0000000007632000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comdia	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000003.54748211 2.00000000064E3000.00000004.00000020.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000002.57784884 7.0000000007632000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000002.57784884 7.0000000007632000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/CK	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000003.54033370 7.00000000064E7000.00000004.00000020.000 20000.00000000.sdmp, shipmentReceipt(22k b).pdf__customInvoice12074408.exe, 00000 000.00000003.540184473.00000000064E7000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000002.57784884 7.0000000007632000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000002.57784884 7.0000000007632000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comams/R	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000003.53969349 2.00000000064E3000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnr-t	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000003.53910372 8.00000000064EC000.00000004.00000020.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000002.57784884 7.0000000007632000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000002.57784884 7.0000000007632000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.sandoll.co.kr	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000002.57784884 7.0000000007632000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000002.57784884 7.0000000007632000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000002.57784884 7.0000000007632000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000002.57784884 7.0000000007632000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.commTTF	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000003.55354033 5.00000000064E4000.00000004.00000020.000 20000.00000000.sdmp, shipmentReceipt(22k b).pdf__customInvoice12074408.exe, 00000 000.00000003.547482112.00000000064E3000. 00000004.00000020.00020000.00000000.sdmp, shipmentReceipt(22kb).pdf__customInvoice12074408 .exe, 00000000.00000003.553420022.000000 00064E3000.00000004.00000020.00020000.00 000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot1360033246:AAF6H8m6YrL09doyxtsvJzZ_cII__BCF4aU/sendDocumentdocument-----	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000005.00000002.80440122 4.0000000002F51000.00000004.00000800.000 20000.00000000.sdmp, kmk.exe, 00000007.0 0000002.803741749.0000000002D11000.00000 004.00000800.00020000.00000000.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000002.57326421 0.0000000004D80000.00000004.00000800.000 20000.00000000.sdmp, shipmentReceipt(22k b).pdf__customInvoice12074408.exe, 00000 000.00000002.573264210.0000000004462000. 00000004.00000800.00020000.00000000.sdmp, kmk.exe, 00000006.00000002.658231003.0 000000003C4C000.00000004.00000800.000200 00.00000000.sdmp, kmk.exe, 00000007.0000 0002.799586439.0000000000436000.00000040 .00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000002.57784884 7.0000000007632000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.fontbureau.com	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000003.54748211 2.00000000064E3000.00000004.00000020.000 20000.00000000.sdmp, shipmentReceipt(22k b).pdf__customInvoice12074408.exe, 00000 000.00000002.577848847.0000000007632000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://DynDns.comDynDNS	kmk.exe, 00000007.00000002.803741749.000 0000002D11000.00000004.00000800.00020000 .00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000005.00000002.80440122 4.0000000002F51000.00000004.00000800.000 20000.00000000.sdmp, kmk.exe, 00000007.0 0000002.803741749.0000000002D11000.00000 004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/.Kp	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000003.54033370 7.00000000064E7000.00000004.00000020.000 20000.00000000.sdmp, shipmentReceipt(22k b).pdf__customInvoice12074408.exe, 00000 000.00000003.540184473.00000000064E7000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/yKM	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000003.54033370 7.00000000064E7000.00000004.00000020.000 20000.00000000.sdmp, shipmentReceipt(22k b).pdf__customInvoice12074408.exe, 00000 000.00000003.540184473.00000000064E7000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000003.54033370 7.00000000064E7000.00000004.00000020.000 20000.00000000.sdmp, shipmentReceipt(22k b).pdf__customInvoice12074408.exe, 00000 000.00000003.540184473.00000000064E7000. 00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/on	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000003.54033370 7.00000000064E7000.00000004.00000020.000 20000.00000000.sdmp, shipmentReceipt(22k b).pdf__customInvoice12074408.exe, 00000 000.00000003.540184473.00000000064E7000. 00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comg	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000003.53969349 2.00000000064E3000.00000004.00000020.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/Sue	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000003.54033370 7.00000000064E7000.00000004.00000020.000 20000.00000000.sdmp, shipmentReceipt(22k b).pdf__customInvoice12074408.exe, 00000 000.00000003.540184473.00000000064E7000. 00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000002.57784884 7.0000000007632000.00000004.00000800.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/fK(	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000003.54033370 7.00000000064E7000.00000004.00000020.000 20000.00000000.sdmp, shipmentReceipt(22k b).pdf__customInvoice12074408.exe, 00000 000.00000003.540184473.00000000064E7000. 00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000002.57784884 7.0000000007632000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000002.57784884 7.0000000007632000.00000004.00000800.000 20000.00000000.sdmp, shipmentReceipt(22k b).pdf__customInvoice12074408.exe, 00000 000.00000003.539103728.00000000064EC000. 00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000002.57784884 7.0000000007632000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/s	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000003.54033370 7.00000000064E7000.00000004.00000020.000 20000.00000000.sdmp, shipmentReceipt(22k b).pdf__customInvoice12074408.exe, 00000 000.00000003.540184473.00000000064E7000. 00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/%Ki	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000003.54018447 3.00000000064E7000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000003.54033370 7.00000000064E7000.00000004.00000020.000 20000.00000000.sdmp, shipmentReceipt(22k b).pdf__customInvoice12074408.exe, 00000 000.00000003.540184473.00000000064E7000. 00000004.00000020.00020000.00000000.sdmp, shipmentReceipt(22kb).pdf__customInvoice12074408 .exe, 00000000.00000002.577848847.000000 0007632000.00000004.00000800.00020000.00 000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000002.57784884 7.0000000007632000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://www.founder.com.cn/cnsk	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000003.53910372 8.00000000064EC000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn(	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000003.53910372 8.00000000064EC000.00000004.00000020.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http:// https://api.telegram.org/bot1360033246:AAF6H8m6YrL 09doyxtsvJzZ_cIl__BCF4aU/	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000002.57326421 0.0000000004D80000.00000004.00000800.000 20000.00000000.sdmp, shipmentReceipt(22k b).pdf__customInvoice12074408.exe, 00000 000.00000002.573264210.0000000004462000. 00000004.00000800.00020000.00000000.sdmp, kmk.exe, 00000006.00000002.658231003.0 000000003C4C000.00000004.00000800.000200 00.00000000.sdmp, kmk.exe, 00000007.0000 0002.799586439.0000000000434000.00000040 .00000400.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/oK?	shipmentReceipt(22kb).pdf__customInvoice 12074408.exe, 00000000.00000003.54018447 3.00000000064E7000.00000004.00000020.000 20000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	876162
Start date and time:	2023-05-26 11:39:13 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
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:	9
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
Sample file name:	shipmentReceipt(22kb).pdf__customInvoice12074408.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@11/4@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 98% • 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): audiodg.exe, WMIADAP.exe
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- 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.

Simulations

Behavior and APIs

Time	Type	Description
11:40:15	API Interceptor	698x Sleep call for process: shipmentReceipt(22kb).pdf__customInvoice12074408.exe modified
11:40:42	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run kmk C:\Users\user\AppData\Roaming\kmk\kmk.exe
11:40:50	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run kmk C:\Users\user\AppData\Roaming\kmk\kmk.exe

Time	Type	Description
11:40:56	API Interceptor	400x Sleep call for process: kmk.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\kmk.exe.log

Process:	C:\Users\user\AppData\Roaming\kmk\kmk.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1302
Entropy (8bit):	5.3499841584777394
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4bE4K5AE4Kzr7RKDE4KhK3VZ9pKhPKIE4oKFKHKorE4x84j:MIHK5HKXE1qHbHK5AHKzvRYHKhQnoPtW
MD5:	E2C3A19FF3EBB1649BF9F41DFE3B7E8F
SHA1:	5DA8AB9561D3C096BB9103413F64EE6E50D5AD88
SHA-256:	18E921771341555EF6167DEBBD7C83727518897E9B4B3545B7CCDB48E2043B74
SHA-512:	6B62A68EC358699D55E4CCD0BBDD4ADDC0F38641D82A019697893CEB503E853A5F087FAF9F4408425AD6631C9CBA31C3354FD98B45F051F2F59A0ECC3CA2FA06
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",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\assem

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\shipmentReceipt(22kb).pdf__customInvoice12074408.exe.log

Process:	C:\Users\user\Desktop\shipmentReceipt(22kb).pdf__customInvoice12074408.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1302
Entropy (8bit):	5.3499841584777394
Encrypted:	false

SSDEEP:	24:MLUE4K5E4Ks2E1qE4bE4K5AE4Kzr7RKDE4KhK3VZ9pKhPKIE4oKFKHKorE4x84j:MIHK5HKXE1qHbHK5AHKzvRYHKhQnoPtW
MD5:	E2C3A19FF3EBB1649BF9F41DFE3B7E8F
SHA1:	5DA8AB9561D3C096BB9103413F64EE6E50D5AD88
SHA-256:	18E921771341555EF6167DEBBD7C83727518897E9B4B3545B7CCDB48E2043B74
SHA-512:	6B62A68EC358699D55E4CCD0BBDD4ADDC0F38641D82A019697893CEB503E853A5F087FAF9F4408425AD6631C9CBA31C3354FD98B45F051F2F59A0ECC3CA2FA06
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",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\assem

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

Process:	C:\Users\user\Desktop\shipmentReceipt(22kb).pdf__customInvoice12074408.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	740864
Entropy (8bit):	7.721307853882747
Encrypted:	false
SSDEEP:	12288:1KK7z5GoJiGaq5aub+2QsKn/KOOfyXuKMu+h3pLGU+arbVifvHehJes:z5GoR5aa+jHOA4h/+cVifvH8
MD5:	278D48D9EA2FE8350796279E5D08A72A
SHA1:	30A693E39B775DE6AFBD146722D07BBA0E4F16BF
SHA-256:	53823B0378B9A17181FEF455B3625E7909E703D600B480FFCCC9A1C6D4232C4A
SHA-512:	2522BBD936BCE6A0849892FE5C49850C74C0BECEA7567D21E27C0B8A314C29E44BBCB20B5D6E6AD8B44D0009A4304A4C64A8C935BD2284BD98931FABA93B34D
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 17%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....~.....0..2.....Q... ...`....@.. .....@.....BQ..O....`.....0..p..... ....H.....text....1... ...2..... ..`.rsrc.....`.....4.....@..@.reloc.....L.....@..B.....vQ.....H.....T...l^.....m.....8.....^..}.....(.....(.....*&..(.....*&..(.....*.0..+.....,..{.....+.....,..{....o.....(.....*..0.....s....}.....{....s....}.....(.....{.....o.....{.... ....o.....{.....s....o.....".@"..PAs....(.....(!.....o"..... ....s#...($.....o%.....r...p(&.....r...po'.....s....((.....()....*".(*....*".(*....*.0.....{.....+..*&...}....*...0.....{.....+..*&...}...

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

Process:	C:\Users\user\Desktop\shipmentReceipt(22kb).pdf__customInvoice12074408.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**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

Entropy (8bit):	7.721307853882747
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:	shipmentReceipt(22kb).pdf__customInvoice12074408.exe
File size:	740864
MD5:	278d48d9ea2fe8350796279e5d08a72a
SHA1:	30a693e39b775de6afbd146722d07bba0e4f16bf
SHA256:	53823b0378b9a17181fef455b3625e7909e703d600b480ffccc9a1c6d4232c4a
SHA512:	2522bbd936bce6a0849892fe5c49850c74c0becea7567d21e27c0b8a314c29e44bbcb20b5d6e6ad8b44d0009a4304a4c64a8c935bd2284bd98931faba93b324d
SSDEEP:	12288:1KK7z5GoJiGaq5aub+2QsKn/KOOfyXuKMu+h3pLGU+arbVifvHehJes:z5GoR5aa+jHOA4h/+cVifvH8
TLSH:	28F4028472A98B07F1BA3BF552429AB017F6BD67B070E20A0DD233DF5AB1F049651B47
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....~.....0..2.....Q... ...`....@.. .....@.....

File Icon

Icon Hash:	05292b2323232b00

Static PE Info

General

Entrypoint:	0x4b5196
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0xB67E188C [Sat Jan 8 12:58:52 2067 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

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

Copyright Joe Security LLC 2023

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb5142	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb6000	0x1710	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xb30b8	0x70	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb319c	0xb3200	False	0.9080273028611305	data	7.743534616199072	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xb6000	0x1710	0x1800	False	0.2373046875	data	3.7239302603938516	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb8000	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	0xb6130	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096		

Name	RVA	Size	Type	Language	Country
RT_GROUP_ICON	0xb71d8	0x14	data		
RT_VERSION	0xb71ec	0x338	data		
RT_MANIFEST	0xb7524	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

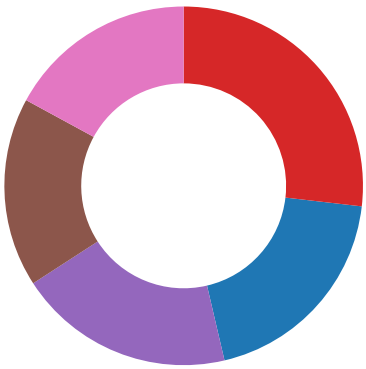
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

No network behavior found

Statistics

Behavior



- shipmentReceipt(22kb).pdf__custom.
- shipmentReceipt(22kb).pdf__custom.
- shipmentReceipt(22kb).pdf__custom.
- shipmentReceipt(22kb).pdf__custom.
- kmk.exe
- kmk.exe
- kmk.exe

Click to jump to process

System Behavior

Analysis Process: shipmentReceipt(22kb).pdf__customInvoice12074408.exe PID: 6492, Parent PID: 3528

General

Target ID:	0
Start time:	11:40:05
Start date:	26/05/2023
Path:	C:\Users\user\Desktop\shipmentReceipt(22kb).pdf__customInvoice12074408.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\shipmentReceipt(22kb).pdf__customInvoice12074408.exe
Imagebase:	0xe50000
File size:	740864 bytes
MD5 hash:	278D48D9EA2FE8350796279E5D08A72A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2023

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.573264210.0000000004D80000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.573264210.0000000004D80000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.573264210.0000000004D80000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.573264210.0000000004462000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.573264210.0000000004462000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.573264210.0000000004462000.00000004.00000800.00020000.00000000.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	72E1CF06	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	72E1CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\shipmentReceipt(22kb).pdf__customInvoice12074408.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7312C78D	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\shipmentReceipt(22kb).pdf__customInvoice12074408.exe.log	0	1302	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	7312C907	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	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C61B4F	ReadFile

Analysis Process: shipmentReceipt(22kb).pdf__customInvoice12074408.exe PID: **6684**, Parent PID: **6492**

General

Target ID:	3
Start time:	11:40:17
Start date:	26/05/2023
Path:	C:\Users\user\Desktop\shipmentReceipt(22kb).pdf__customInvoice12074408.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\shipmentReceipt(22kb).pdf__customInvoice12074408.exe
Imagebase:	0x80000
File size:	740864 bytes
MD5 hash:	278D48D9EA2FE8350796279E5D08A72A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: shipmentReceipt(22kb).pdf__customInvoice12074408.exe PID: **6672**, Parent PID: **6492**

General

Target ID:	4
Start time:	11:40:17
Start date:	26/05/2023
Path:	C:\Users\user\Desktop\shipmentReceipt(22kb).pdf__customInvoice12074408.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\shipmentReceipt(22kb).pdf__customInvoice12074408.exe
Imagebase:	0x130000
File size:	740864 bytes
MD5 hash:	278D48D9EA2FE8350796279E5D08A72A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: shipmentReceipt(22kb).pdf__customInvoice12074408.exe PID: **6764**, Parent PID: **6492**

General

Target ID:	5
Start time:	11:40:17
Start date:	26/05/2023
Path:	C:\Users\user\Desktop\shipmentReceipt(22kb).pdf__customInvoice12074408.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\shipmentReceipt(22kb).pdf__customInvoice12074408.exe
Imagebase:	0xbc0000

File size:	740864 bytes
MD5 hash:	278D48D9EA2FE8350796279E5D08A72A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000005.00000002.799586620.0000000000430000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.804401224.0000000003012000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.804401224.0000000003012000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.804401224.0000000002F51000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000005.00000002.804401224.0000000002F51000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.804401224.0000000002F51000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 00000005.00000002.804401224.0000000002F51000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
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	72E1CF06	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	72E1CF06	unknown
C:\Users\user\AppData\Roaming\kmk	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71C6BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\kmk\kmk.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	71C6DD66	CopyFileW
C:\Users\user\AppData\Roaming\kmk\kmk.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	71C6DD66	CopyFileW

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\kmk\kmk.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 18 7e fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 32 0b 00 00 1a 00 00 00 00 00 00 fd 51 0b 00 00 20 00 00 00 60 0b 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 0b 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.$PEL~02Q `@ @	success or wait	3	71C6DD66	CopyFileW
C:\Users\user\AppData\Roaming\kmk\kmk.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	71C6DD66	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	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	71C61B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	kmk	unicode	C:\Users\user\AppData\Roaming\kmk\kmk.exe	success or wait	1	71C6646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	kmk	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	71C6DE2E	RegSetValueExW

Copyright Joe Security LLC 2023

Analysis Process: kmk.exe PID: **2400**, Parent PID: **3528**

General

Target ID:	6
Start time:	11:40:50
Start date:	26/05/2023
Path:	C:\Users\user\AppData\Roaming\kmk\kmk.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\kmk\kmk.exe"
Imagebase:	0x560000
File size:	740864 bytes
MD5 hash:	278D48D9EA2FE8350796279E5D08A72A
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: 00000006.00000002.658231003.0000000003C4C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000002.658231003.0000000003C4C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000006.00000002.658231003.0000000003C4C000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 17%, 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	72E1CF06	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	72E1CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kmk.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7312C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kmk.exe.log	0	1302	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	7312C907	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	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C61B4F	ReadFile

Analysis Process: kmk.exe PID: **4588**, Parent PID: **2400**

General

Target ID:	7
Start time:	11:40:58
Start date:	26/05/2023
Path:	C:\Users\user\AppData\Roaming\kmk\kmk.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\kmk\kmk.exe
Imagebase:	0x8d0000
File size:	740864 bytes
MD5 hash:	278D48D9EA2FE8350796279E5D08A72A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000007.00000002.799586439.0000000000432000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.803741749.0000000002D11000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000007.00000002.803741749.0000000002D11000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.803741749.0000000002D11000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 00000007.00000002.803741749.0000000002D11000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
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	72E1CF06	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	72E1CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C61B4F	ReadFile

Analysis Process: kmk.exe PID: **3276**, Parent PID: **3528**

General

Target ID:	8
Start time:	11:40:59
Start date:	26/05/2023
Path:	C:\Users\user\AppData\Roaming\kmk\kmk.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\kmk\kmk.exe"
Imagebase:	0xa60000
File size:	740864 bytes
MD5 hash:	278D48D9EA2FE8350796279E5D08A72A
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	72E1CF06	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	72E1CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C61B4F	ReadFile

Disassembly

No disassembly