ID: 383908
Sample Name: payment details.exe
Cookbook: default.jbs
Time: 12:11:20
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

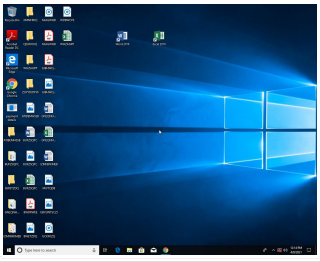
Analysis Report payment details.exe

Overview

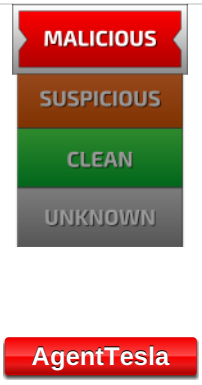
General Information

Sample Name:	payment details.exe
Analysis ID:	383908
MD5:	55191839573ac8..
SHA1:	b9e85e2ab05e4b..
SHA256:	e81d917830f3fab..
Tags:	AgentTesla
Infos:	

Most interesting Screenshot:



Detection

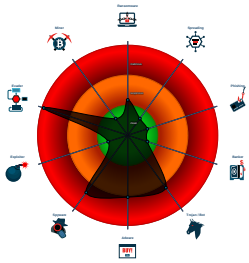


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains method …
- .NET source code contains very larg…
- .NET source code references suspic…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Modifies the hosts file
- Queries sensitive BIOS Information …

Classification



Startup

- **System is w10x64**
- payment details.exe (PID: 7008 cmdline: 'C:\Users\user\Desktop\payment details.exe' MD5: 55191839573AC8FD25655B3561286BC1)
  - payment details.exe (PID: 1320 cmdline: {path} MD5: 55191839573AC8FD25655B3561286BC1)
- kprUEGC.exe (PID: 6692 cmdline: 'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe' MD5: 55191839573AC8FD25655B3561286BC1)
  - kprUEGC.exe (PID: 6932 cmdline: {path} MD5: 55191839573AC8FD25655B3561286BC1)
- kprUEGC.exe (PID: 7132 cmdline: 'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe' MD5: 55191839573AC8FD25655B3561286BC1)
  - kprUEGC.exe (PID: 816 cmdline: {path} MD5: 55191839573AC8FD25655B3561286BC1)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "ho@almasroor.com042264528mail.almasroor.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.916754002.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000013.00000002.916752082.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.690986558.0000000003C59000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000013.00000002.919584190.00000000031F1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000013.00000002.919584190.00000000031F1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 18 entries				

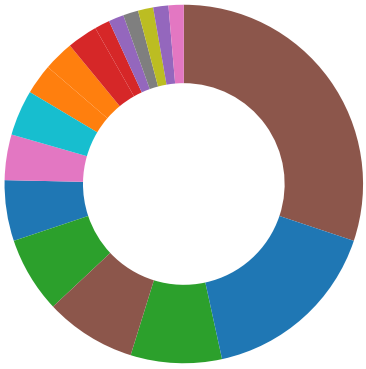
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.payment details.exe.3e052e8.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
15.2.kprUEGC.exe.39952e8.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.2.payment details.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
16.2.kprUEGC.exe.3db52e8.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.payment details.exe.3e052e8.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 4 entries				

Sigma Overview

No Sigma rule has matched

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

Networking:

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

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains method to dynamically call methods (often used by packers)

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:

.NET source code references suspicious native API functions

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:

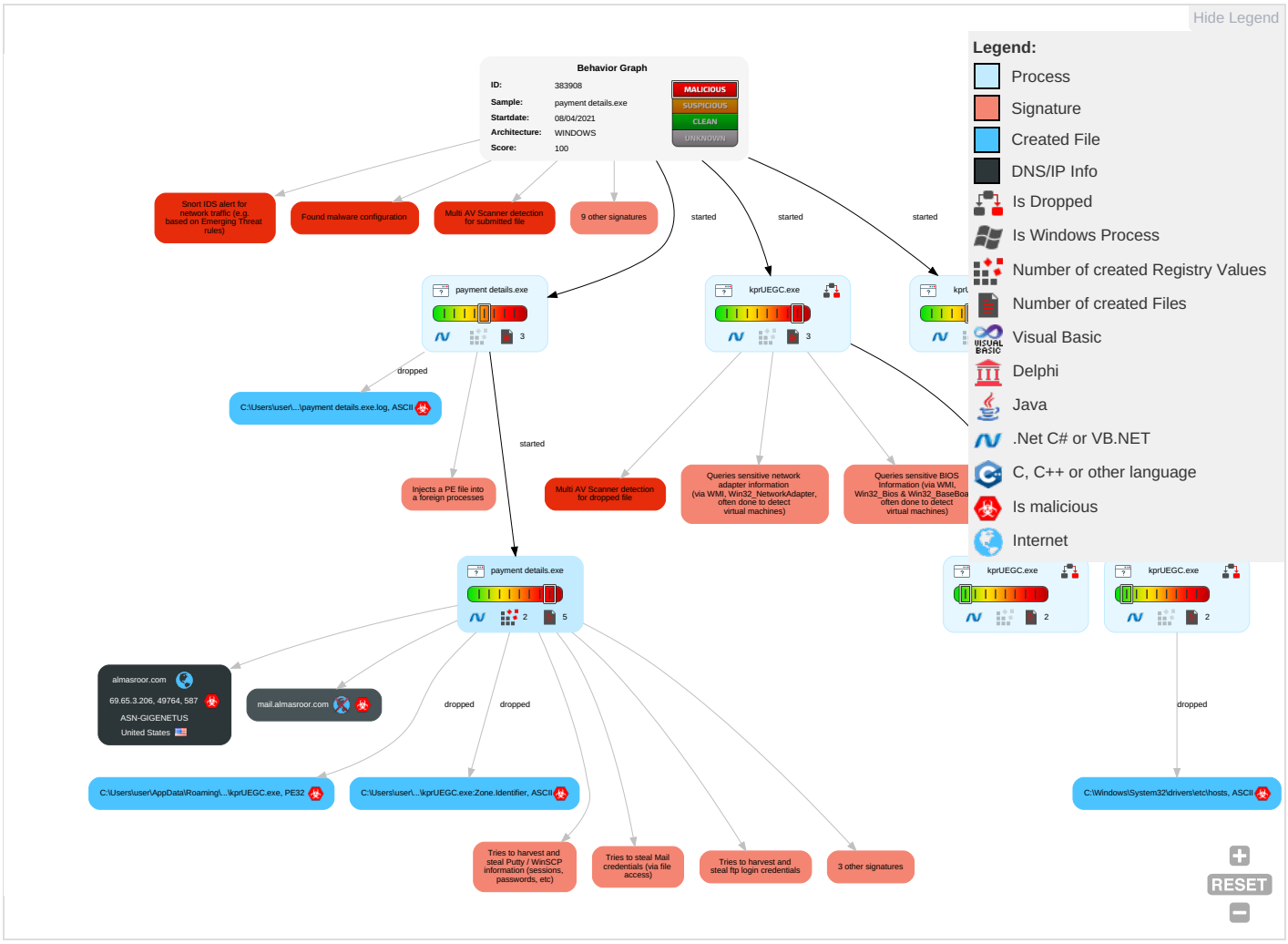
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	File and Directory Permissions Modification 1	OS Credential Dumping 2	System Information Discovery 1 1 4	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Disable or Modify Tools 1	Credentials in Registry 1	Query Registry 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Security Software Discovery 3 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Process Discovery 2	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 3	LSA Secrets	Virtualization/Sandbox Evasion 1 3 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicati
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocol

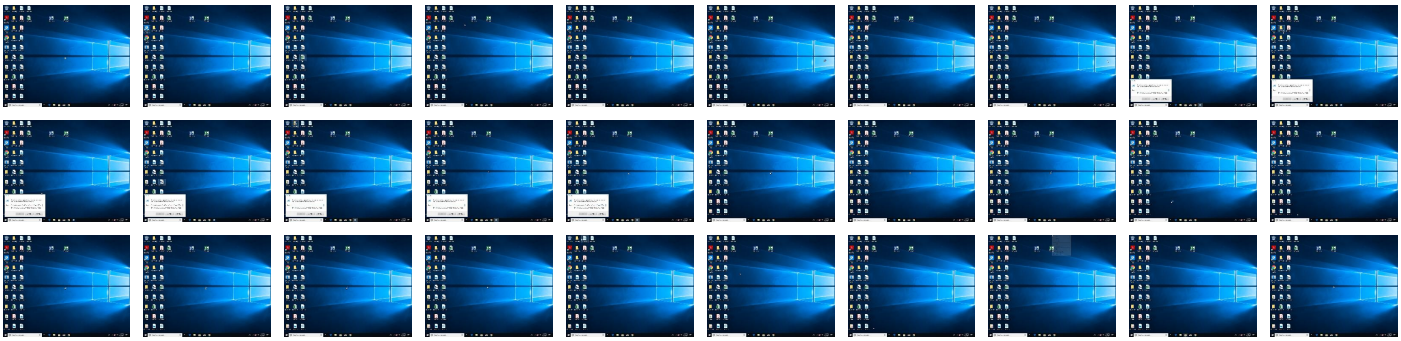
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
payment details.exe	32%	Virustotal		Browse
payment details.exe	33%	ReversingLabs	Win32.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	33%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.payment details.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
18.2.kprUEGC.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
19.2.kprUEGC.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
almasroor.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.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://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://bQxorv.com	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://https://api.ipify.org%$	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.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://almasroor.com	0%	Avira URL Cloud	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.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://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.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	

Source	Detection	Scanner	Label	Link
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://mail.almasroor.com	0%	Avira URL Cloud	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://uDoQcdZGpyqzP0ZwyV.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
almasroor.com	69.65.3.206	true	true	• 0%, Virustotal, Browse	unknown
mail.almasroor.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

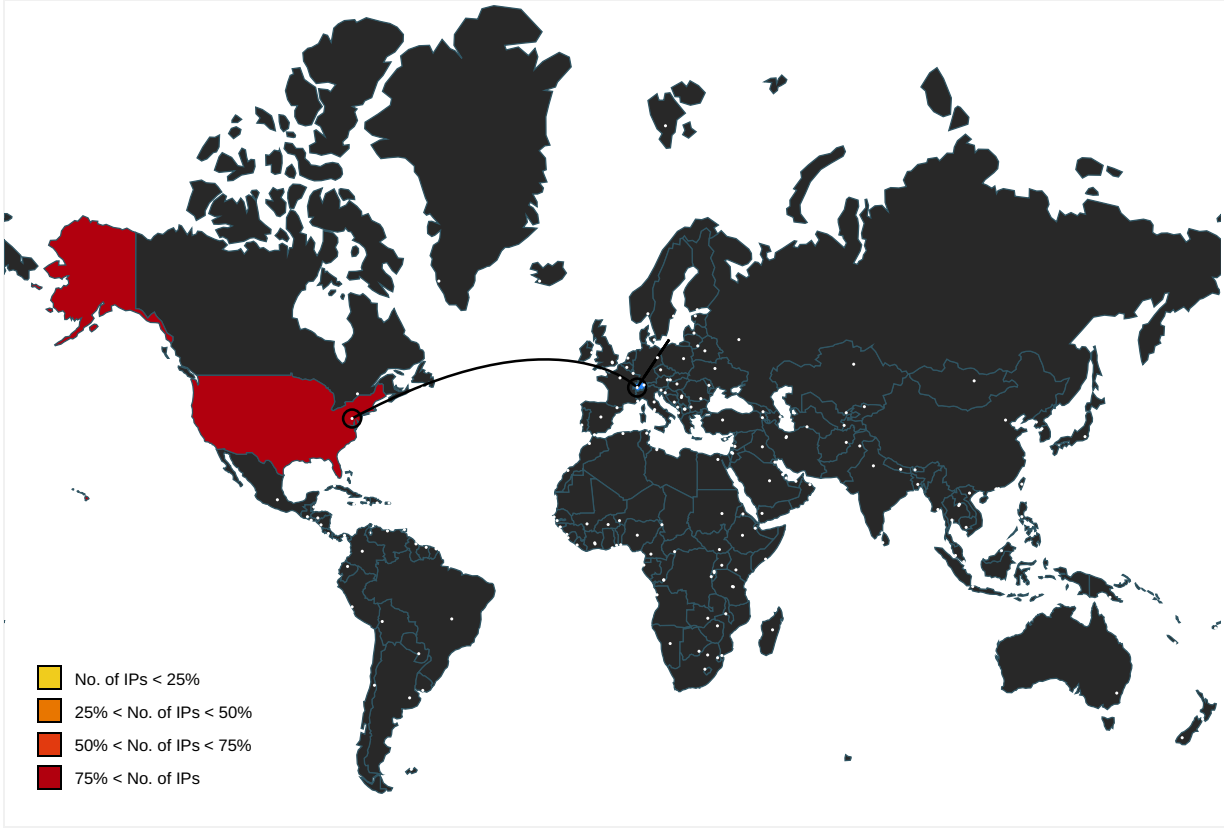
Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	payment details.exe, 00000005.00000002.920699036.00000000029B1000.00000004.00000001.sdmp, kprUEGC.exe, 00000012.00000002.818572720.00000000030F1000.00000004.00000001.sdmp, kprUEGC.exe, 00000013.00000002.919584190.00000000031F1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	payment details.exe, 00000000.00000002.694767298.0000000005BE0000.00000002.00000001.sdmp, kprUEGC.exe, 0000000F.00000002.802621284.0000000005820000.00000002.00000001.sdmp, kprUEGC.exe, 00000010.00000002.823184055.0000000005B40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	payment details.exe, 00000000.00000002.694767298.0000000005BE0000.00000002.00000001.sdmp, kprUEGC.exe, 0000000F.00000002.802621284.0000000005820000.00000002.00000001.sdmp, kprUEGC.exe, 00000010.00000002.823184055.0000000005B40000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	payment details.exe, 00000000.00000002.694767298.0000000005BE0000.00000002.00000001.sdmp, kprUEGC.exe, 0000000F.00000002.802621284.0000000005820000.00000002.00000001.sdmp, kprUEGC.exe, 00000010.00000002.823184055.0000000005B40000.00000002.00000001.sdmp	false		high
http://DynDns.comDynDNS	kprUEGC.exe, 00000013.00000002.919584190.00000000031F1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	payment details.exe, 00000000.00000002.694767298.0000000005BE0000.00000002.00000001.sdmp, kprUEGC.exe, 0000000F.00000002.802621284.0000000005820000.00000002.00000001.sdmp, kprUEGC.exe, 00000010.00000002.823184055.0000000005B40000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	payment details.exe, 00000000.00000002.694767298.0000000005BE0000.00000002.00000001.sdmp, kprUEGC.exe, 0000000F.00000002.802621284.0000000005820000.00000002.00000001.sdmp, kprUEGC.exe, 00000010.00000002.823184055.0000000005B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	payment details.exe, 00000005.00000002.920699036.00000000029B1000.00000004.00000001.sdmp, kprUEGC.exe, 00000012.00000002.818572720.00000000030F1000.00000004.00000001.sdmp, kprUEGC.exe, 00000013.00000002.919584190.00000000031F1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/michel-pi/EasyBot.Net	kprUEGC.exe, payment details.exe	false		high
http://www.fontbureau.com/designers?	payment details.exe, 00000000.00000002.694767298.0000000005BE0000.00000002.00000001.sdmp, kprUEGC.exe, 0000000F.00000002.802621284.0000000005820000.00000002.00000001.sdmp, kprUEGC.exe, 00000010.00000002.823184055.0000000005B40000.00000002.00000001.sdmp	false		high
http://www.tiro.com	kprUEGC.exe, 00000010.00000002.823184055.0000000005B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://bQxorv.com	kprUEGC.exe, 00000013.00000002.919584190.00000000031F1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	kprUEGC.exe, 00000010.00000002.823184055.0000000005B40000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	payment details.exe, 00000000.00000002.694767298.0000000005BE0000.00000002.00000001.sdmp, kprUEGC.exe, 0000000F.00000002.802621284.0000000005820000.00000002.00000001.sdmp, kprUEGC.exe, 00000010.00000002.823184055.0000000005B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%$	payment details.exe, 00000005.00000002.920699036.00000000029B1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.coml	payment details.exe, 00000000.00000002.694767298.0000000005BE0000.00000002.00000001.sdmp, kprUEGC.exe, 0000000F.00000002.802621284.0000000005820000.00000002.00000001.sdmp, kprUEGC.exe, 00000010.00000002.823184055.0000000005B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	payment details.exe, 00000000.00000002.694767298.0000000005BE0000.00000002.00000001.sdmp, kprUEGC.exe, 0000000F.00000002.802621284.0000000005820000.00000002.00000001.sdmp, kprUEGC.exe, 00000010.00000002.823184055.0000000005B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://almasroor.com	payment details.exe, 00000005.00000002.923488347.0000000002D15000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	payment details.exe, 00000000.00000002.694767298.0000000005BE0000.00000002.00000001.sdmp, kprUEGC.exe, 0000000F.00000002.802621284.0000000005820000.00000002.00000001.sdmp, kprUEGC.exe, 00000010.00000002.823184055.0000000005B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.htmlN	payment details.exe, 00000000.00000002.694767298.0000000005BE0000.00000002.00000001.sdmp, kprUEGC.exe, 0000000F.00000002.802621284.0000000005820000.00000002.00000001.sdmp, kprUEGC.exe, 00000010.00000002.823184055.0000000005B40000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	payment details.exe, 00000000.00000002.694767298.0000000005BE0000.00000002.00000001.sdmp, kprUEGC.exe, 0000000F.00000002.802621284.0000000005820000.00000002.00000001.sdmp, kprUEGC.exe, 00000010.00000002.823184055.0000000005B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	payment details.exe, 00000000.00000002.694767298.0000000005BE0000.00000002.00000001.sdmp, kprUEGC.exe, 0000000F.00000002.802621284.0000000005820000.00000002.00000001.sdmp, kprUEGC.exe, 00000010.00000002.823184055.0000000005B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	payment details.exe, 00000000.00000002.694767298.0000000005BE0000.00000002.00000001.sdmp, kprUEGC.exe, 0000000F.00000002.802621284.0000000005820000.00000002.00000001.sdmp, kprUEGC.exe, 00000010.00000002.823184055.0000000005B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	payment details.exe, 00000000.00000002.694767298.0000000005BE0000.00000002.00000001.sdmp, kprUEGC.exe, 0000000F.00000002.802621284.0000000005820000.00000002.00000001.sdmp, kprUEGC.exe, 00000010.00000002.823184055.0000000005B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	payment details.exe, 00000000.00000002.694767298.0000000005BE0000.00000002.00000001.sdmp, kprUEGC.exe, 0000000F.00000002.802621284.0000000005820000.00000002.00000001.sdmp, kprUEGC.exe, 00000010.00000002.823184055.0000000005B40000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	payment details.exe, 00000000.00000002.694767298.0000000005BE0000.00000002.00000001.sdmp, kprUEGC.exe, 0000000F.00000002.802621284.0000000005820000.00000002.00000001.sdmp, kprUEGC.exe, 00000010.00000002.823184055.0000000005B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	payment details.exe, 00000000.00000002.694767298.0000000005BE0000.00000002.00000001.sdmp, kprUEGC.exe, 0000000F.00000002.802621284.0000000005820000.00000002.00000001.sdmp, kprUEGC.exe, 00000010.00000002.823184055.0000000005B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	payment details.exe, 00000000.00000002.694767298.0000000005BE0000.00000002.00000001.sdmp, kprUEGC.exe, 0000000F.00000002.802621284.0000000005820000.00000002.00000001.sdmp, kprUEGC.exe, 00000010.00000002.823184055.0000000005B40000.00000002.00000001.sdmp	false		high
http://https://api.ipify.org%GETMozilla/5.0	kprUEGC.exe, 00000013.00000002.919584190.00000000031F1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	payment details.exe, 00000000.00000002.694767298.0000000005BE0000.00000002.00000001.sdmp, kprUEGC.exe, 0000000F.00000002.802621284.0000000005820000.00000002.00000001.sdmp, kprUEGC.exe, 00000010.00000002.823184055.0000000005B40000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	payment details.exe, 00000000.00000002.694767298.0000000005BE0000.00000002.00000001.sdmp, kprUEGC.exe, 0000000F.00000002.802621284.0000000005820000.00000002.00000001.sdmp, kprUEGC.exe, 00000010.00000002.823184055.0000000005B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	payment details.exe, 00000000.00000002.694767298.0000000005BE0000.00000002.00000001.sdmp, kprUEGC.exe, 0000000F.00000002.802621284.0000000005820000.00000002.00000001.sdmp, kprUEGC.exe, 00000010.00000002.823184055.0000000005B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	payment details.exe, 00000000.00000002.694767298.0000000005BE0000.00000002.00000001.sdmp, kprUEGC.exe, 0000000F.00000002.802621284.0000000005820000.00000002.00000001.sdmp, kprUEGC.exe, 00000010.00000002.823184055.0000000005B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	payment details.exe, 00000000.00000002.694767298.0000000005BE0000.00000002.00000001.sdmp, kprUEGC.exe, 0000000F.00000002.802621284.0000000005820000.00000002.00000001.sdmp, kprUEGC.exe, 00000010.00000002.823184055.0000000005B40000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mail.almasroor.com	payment details.exe, 00000005.00000002.923488347.0000000002D15000.00000004.00000001.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	payment details.exe, 00000000.00000002.690986558.0000000003C59000.00000004.00000001.sdmp, payment details.exe, 00000005.00000002.916754002.0000000000402000.00000040.00000001.sdmp, kprUEGC.exe, 0000000F.00000002.795750062.00000000037E9000.00000004.00000001.sdmp, kprUEGC.exe, 00000010.00000002.816268269.0000000003C09000.00000004.00000001.sdmp, kprUEGC.exe, 00000012.00000002.817039638.0000000000402000.00000040.00000001.sdmp, kprUEGC.exe, 00000013.00000002.916752082.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://uDoQcdZGpyqzP0ZwyV.com	payment details.exe, 00000005.00000002.923358633.0000000002CD9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
69.65.3.206	almasroor.com	United States		32181	ASN-GIGENETUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383908
Start date:	08.04.2021
Start time:	12:11:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	payment details.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:	23
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@9/6@2/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 0% (good quality ratio 0%) • Quality average: 51% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 99% • 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): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 23.54.113.53, 52.147.198.201, 104.43.139.144, 13.88.21.125, 13.64.90.137, 20.82.210.154, 23.10.249.26, 23.10.249.43, 23.0.174.185, 23.0.174.200, 52.155.217.156, 20.54.26.129, 20.82.209.183 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.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 NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:12:20	API Interceptor	630x Sleep call for process: payment details.exe modified
12:12:55	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run kprUEGC C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
12:13:03	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run kprUEGC C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
12:13:10	API Interceptor	289x Sleep call for process: kprUEGC.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ASN-GIGENETUS	AWB-9899691012.exe	Get hash	malicious	Browse	• 45.85.90.220
	swift_76567643.exe	Get hash	malicious	Browse	• 70.32.1.32
	BillOfLading.exe	Get hash	malicious	Browse	• 45.85.90.220
	OPEN01929291000_2021-03-15_07-28.exe	Get hash	malicious	Browse	• 45.85.90.188
	INV242-0303.doc	Get hash	malicious	Browse	• 45.85.90.197
	dwg.exe	Get hash	malicious	Browse	• 45.85.90.226
	a55ddff55740467df8dee39a5bbaee32.exe	Get hash	malicious	Browse	• 45.85.90.138
	116e4c42d3948c91eafdcb60a9f37014.exe	Get hash	malicious	Browse	• 45.85.90.138
	771eb3ef5ede516d6ec53ae40b3f888f.exe	Get hash	malicious	Browse	• 45.85.90.138
	Paid Invoice _confirmation_9336639_03993736553.exe	Get hash	malicious	Browse	• 216.38.7.225
	YCVj3q7r5e.exe	Get hash	malicious	Browse	• 70.32.1.32
	VOR001 - McMurray Statements December 2020_8737353 5737522772662626.exe	Get hash	malicious	Browse	• 216.38.7.225
	Customer_Receivables_Aging_20210112_26635353452424 24242.exe	Get hash	malicious	Browse	• 216.38.7.225
	Proforma fatura.exe	Get hash	malicious	Browse	• 216.38.2.215
	Invoice.exe	Get hash	malicious	Browse	• 216.38.2.215
	Purchase Order-34002174,pdf.exe	Get hash	malicious	Browse	• 216.38.7.231
	IT3(b) certificate_846392852289725282735792726639.exe	Get hash	malicious	Browse	• 216.38.7.225
	Customer Remittance Advice 9876627262822662.exe	Get hash	malicious	Browse	• 216.38.7.225
	newbinx.exe	Get hash	malicious	Browse	• 216.38.2.206
	Purchase New Order_101520,pdf.exe	Get hash	malicious	Browse	• 216.38.7.231

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	false
Reputation:	high, very likely benign file

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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\payment details.exe.log	
Process:	C:\Users\user\Desktop\payment details.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:	**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\Roaming\kprUEGC\kprUEGC.exe	
Process:	C:\Users\user\Desktop\payment details.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	729600
Entropy (8bit):	7.8860851483500385
Encrypted:	false
SSDEEP:	12288:wfBr6Pu2iNXNKJSjlVQp9Tjj7pqA8C8veXh+R7QrRLqQsm2T8TJjHEM0Eyxf3:+ruu1lNhK9Tn7YESQK0rR6f8TJuV3
MD5:	55191839573AC8FD25655B3561286BC1
SHA1:	B9E85E2AB05E4B027A3F522FD690B097AA4A4AAD
SHA-256:	E81D917830F3FABCA0557B899267EBE84ECC6FCBB5E1CD649284D1370D8A8876
SHA-512:	3488AB665AEDFEC80B744E403C8A0772097608C679E62B4CCE77103B2B3EFDAD262E41CDA0F579533C4D8C061AACF9963A61AB90053FBDF58F70F67685A69C84
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 33%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...WZn`.....0.....6... ...@....@.. ..... .....@.....5..O....@.....`..... ....H.....text...4.... ....`.rsrc.....@..... ..@..@.reloc.....`..... .....@..B.....5.....H.....h.....IZ..X.....^..}.....(.....(.....*..*..0..+.....,.{.....+.....,.{....o.....(.....*..0..... (....s.....s....}.....s....}.....s....}.....s....}.....s....}.....s ...}.....s!...}.....s"...}.....{....o#.....{....o$.....(#.....{.....o%.....{....o&....."...Bs'...o(...&.{....o&....."...Bs'...o(...&.{....o)....{.....o*.....{....o)....{.....o*.....{....o)....{.....o*.....{....o)....{.....o*.....{....o

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

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

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**
Reputation:	moderate, very likely benign file
Preview:	..127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.8860851483500385
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:	payment details.exe
File size:	729600
MD5:	55191839573ac8fd25655b3561286bc1
SHA1:	b9e85e2ab05e4b027a3f522fd690b097aa4a4aad
SHA256:	e81d917830f3fabca0557b899267ebe84ecc6fcbb5e1cd649284d1370d8a8876
SHA512:	3488ab665aedfec80b744e403c8a0772097608c679e62b4cce77103b2b3efdad262e41cda0f579533c4d8c061aacf9963a61ab90053fbdf58f70f67685a69c84
SSDEEP:	12288:wfBr6Pu2iNXNKJSjlVQp9Tjj7pqA8C8veXh+R7QrRLqQsm2T8TJjHEM0Eyxf3:+ruu1lNhK9Tn7YESQK0rR6f8TJuV3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...WZn`.....0.....6... ...@....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4b3616
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui

General	
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x606E5A57 [Thu Apr 8 01:20:23 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]
mov dword ptr [eax+4Eh], edx
inc edi
or eax, 000A1A0Ah
add byte ptr [eax], al
add byte ptr [ecx+45h], cl
dec esi
inc esp
scasb
inc edx
pushad
add byte ptr [eax], 00000000h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb35c4	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb4000	0x5bc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb6000	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	

Name	Virtual Address	Virtual Size	Is in Section
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	0xb1634	0xb1800	False	0.90361328125	data	7.89257156143	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb4000	0x5bc	0x600	False	0.430338541667	data	4.18044919538	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb6000	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	0xb4090	0x32c	data		
RT_MANIFEST	0xb43cc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

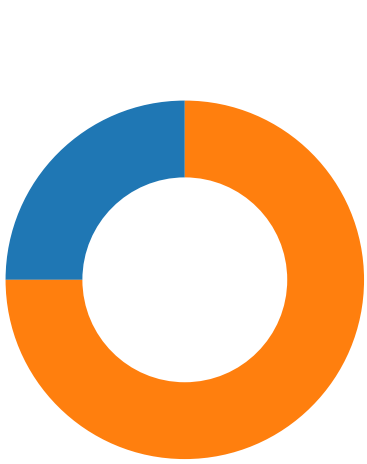
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018 - 2021
Assembly Version	3.1.0.5
InternalName	E7.exe
FileVersion	3.1.0.5
CompanyName	
LegalTrademarks	
Comments	
ProductName	Image Manager
ProductVersion	3.1.0.5
FileDescription	Image Manager
OriginalFilename	E7.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-12:13:03.957380	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
04/08/21-12:14:14.478900	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49764	587	192.168.2.4	69.65.3.206

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:14:13.416610003 CEST	49764	587	192.168.2.4	69.65.3.206
Apr 8, 2021 12:14:13.529042006 CEST	587	49764	69.65.3.206	192.168.2.4
Apr 8, 2021 12:14:13.529160023 CEST	49764	587	192.168.2.4	69.65.3.206
Apr 8, 2021 12:14:13.782218933 CEST	587	49764	69.65.3.206	192.168.2.4
Apr 8, 2021 12:14:13.783303976 CEST	49764	587	192.168.2.4	69.65.3.206
Apr 8, 2021 12:14:13.896219969 CEST	587	49764	69.65.3.206	192.168.2.4
Apr 8, 2021 12:14:13.897735119 CEST	49764	587	192.168.2.4	69.65.3.206
Apr 8, 2021 12:14:14.012175083 CEST	587	49764	69.65.3.206	192.168.2.4
Apr 8, 2021 12:14:14.012785912 CEST	49764	587	192.168.2.4	69.65.3.206
Apr 8, 2021 12:14:14.135514021 CEST	587	49764	69.65.3.206	192.168.2.4
Apr 8, 2021 12:14:14.136495113 CEST	49764	587	192.168.2.4	69.65.3.206
Apr 8, 2021 12:14:14.248852015 CEST	587	49764	69.65.3.206	192.168.2.4
Apr 8, 2021 12:14:14.249553919 CEST	49764	587	192.168.2.4	69.65.3.206
Apr 8, 2021 12:14:14.362612963 CEST	587	49764	69.65.3.206	192.168.2.4
Apr 8, 2021 12:14:14.363524914 CEST	49764	587	192.168.2.4	69.65.3.206
Apr 8, 2021 12:14:14.475619078 CEST	587	49764	69.65.3.206	192.168.2.4
Apr 8, 2021 12:14:14.475667953 CEST	587	49764	69.65.3.206	192.168.2.4
Apr 8, 2021 12:14:14.478899956 CEST	49764	587	192.168.2.4	69.65.3.206
Apr 8, 2021 12:14:14.479218006 CEST	49764	587	192.168.2.4	69.65.3.206
Apr 8, 2021 12:14:14.479986906 CEST	49764	587	192.168.2.4	69.65.3.206
Apr 8, 2021 12:14:14.480148077 CEST	49764	587	192.168.2.4	69.65.3.206
Apr 8, 2021 12:14:14.591240883 CEST	587	49764	69.65.3.206	192.168.2.4
Apr 8, 2021 12:14:14.591269016 CEST	587	49764	69.65.3.206	192.168.2.4
Apr 8, 2021 12:14:15.217732906 CEST	587	49764	69.65.3.206	192.168.2.4
Apr 8, 2021 12:14:15.270230055 CEST	49764	587	192.168.2.4	69.65.3.206

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:12:03.064060926 CEST	65298	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:12:03.077512980 CEST	53	65298	8.8.8.8	192.168.2.4
Apr 8, 2021 12:12:03.845468998 CEST	59123	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:12:03.858165026 CEST	53	59123	8.8.8.8	192.168.2.4
Apr 8, 2021 12:12:04.593974113 CEST	54531	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:12:04.606405020 CEST	53	54531	8.8.8.8	192.168.2.4
Apr 8, 2021 12:12:05.538863897 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:12:05.558337927 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 8, 2021 12:12:05.890345097 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:12:05.903453112 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 8, 2021 12:12:06.565275908 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:12:06.578464985 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 8, 2021 12:12:07.659887075 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:12:07.673106909 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 8, 2021 12:12:08.621151924 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:12:08.633485079 CEST	53	62389	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:12:09.517817974 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:12:09.530227900 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 8, 2021 12:12:10.398554087 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:12:10.411314964 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 8, 2021 12:12:11.768969059 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:12:11.781416893 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 8, 2021 12:12:29.372864962 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:12:29.385481119 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 8, 2021 12:12:30.782634020 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:12:30.798058033 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 8, 2021 12:12:31.834743023 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:12:31.846843004 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 8, 2021 12:12:32.547606945 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:12:32.561222076 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 8, 2021 12:12:33.321407080 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:12:33.334260941 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 8, 2021 12:12:34.282865047 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:12:34.296099901 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 8, 2021 12:12:35.276427031 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:12:35.289624929 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 8, 2021 12:12:37.214466095 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:12:37.227308035 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 8, 2021 12:12:40.079788923 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:12:40.092431068 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 8, 2021 12:12:45.115417957 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:12:45.135452986 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 8, 2021 12:12:56.673142910 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:12:56.691920042 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 8, 2021 12:13:01.490715027 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:13:01.625912905 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 8, 2021 12:13:02.216861963 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:13:02.229913950 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 8, 2021 12:13:02.821137905 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:13:03.873179913 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:13:03.886499882 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 8, 2021 12:13:03.957209110 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 8, 2021 12:13:04.867223978 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:13:04.880508900 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 8, 2021 12:13:06.228488922 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:13:06.326831102 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 8, 2021 12:13:06.883766890 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:13:06.896733046 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 8, 2021 12:13:07.279181004 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:13:07.292699099 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 8, 2021 12:13:07.457143068 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:13:07.470500946 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 8, 2021 12:13:08.050573111 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:13:08.063374996 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 8, 2021 12:13:09.544285059 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:13:09.557113886 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 8, 2021 12:13:09.907948017 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:13:09.923392057 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 8, 2021 12:13:19.272897005 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:13:19.290817976 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 8, 2021 12:13:57.243844986 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:13:57.279443979 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 8, 2021 12:14:02.344350100 CEST	50183	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:14:02.371304035 CEST	53	50183	8.8.8.8	192.168.2.4
Apr 8, 2021 12:14:12.552082062 CEST	61531	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:14:12.682018995 CEST	53	61531	8.8.8.8	192.168.2.4
Apr 8, 2021 12:14:13.157211065 CEST	49228	53	192.168.2.4	8.8.8.8
Apr 8, 2021 12:14:13.277036905 CEST	53	49228	8.8.8.8	192.168.2.4

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Apr 8, 2021 12:13:03.957380056 CEST	192.168.2.4	8.8.8.8	d138	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 12:14:12.552082062 CEST	192.168.2.4	8.8.8.8	0xb2dd	Standard query (0)	mail.almasroor.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:14:13.157211065 CEST	192.168.2.4	8.8.8.8	0x70e6	Standard query (0)	mail.almasroor.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 12:14:12.682018995 CEST	8.8.8.8	192.168.2.4	0xb2dd	No error (0)	mail.almasroor.com	almasroor.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:14:12.682018995 CEST	8.8.8.8	192.168.2.4	0xb2dd	No error (0)	almasroor.com		69.65.3.206	A (IP address)	IN (0x0001)
Apr 8, 2021 12:14:13.277036905 CEST	8.8.8.8	192.168.2.4	0x70e6	No error (0)	mail.almasroor.com	almasroor.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:14:13.277036905 CEST	8.8.8.8	192.168.2.4	0x70e6	No error (0)	almasroor.com		69.65.3.206	A (IP address)	IN (0x0001)

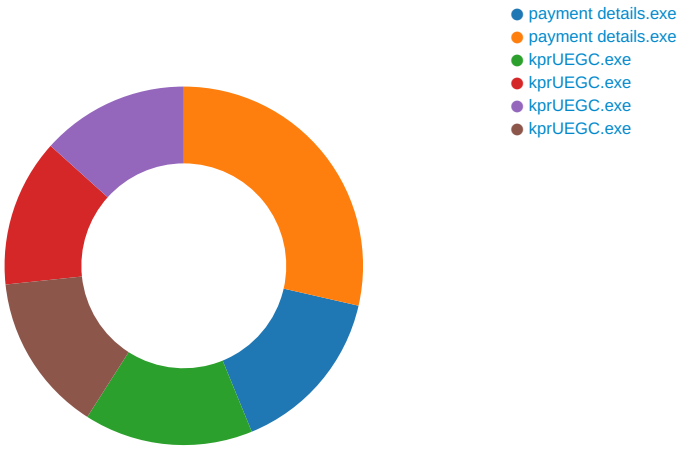
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 8, 2021 12:14:13.782218933 CEST	587	49764	69.65.3.206	192.168.2.4	220-server302.webhostingpad.com ESMTP Exim 4.93 #2 Thu, 08 Apr 2021 05:14:13 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Apr 8, 2021 12:14:13.783303976 CEST	49764	587	192.168.2.4	69.65.3.206	EHLO 247525
Apr 8, 2021 12:14:13.896219969 CEST	587	49764	69.65.3.206	192.168.2.4	250-server302.webhostingpad.com Hello 247525 [185.32.222.8] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Apr 8, 2021 12:14:13.897735119 CEST	49764	587	192.168.2.4	69.65.3.206	AUTH login aG9AYWxtYXNyb29yLmNvbQ==
Apr 8, 2021 12:14:14.012175083 CEST	587	49764	69.65.3.206	192.168.2.4	334 UGFzc3dvcmQ6
Apr 8, 2021 12:14:14.135514021 CEST	587	49764	69.65.3.206	192.168.2.4	235 Authentication succeeded
Apr 8, 2021 12:14:14.136495113 CEST	49764	587	192.168.2.4	69.65.3.206	MAIL FROM:<ho@almasroor.com>
Apr 8, 2021 12:14:14.248852015 CEST	587	49764	69.65.3.206	192.168.2.4	250 OK
Apr 8, 2021 12:14:14.249553919 CEST	49764	587	192.168.2.4	69.65.3.206	RCPT TO:<ho@almasroor.com>
Apr 8, 2021 12:14:14.362612963 CEST	587	49764	69.65.3.206	192.168.2.4	250 Accepted
Apr 8, 2021 12:14:14.363524914 CEST	49764	587	192.168.2.4	69.65.3.206	DATA
Apr 8, 2021 12:14:14.475667953 CEST	587	49764	69.65.3.206	192.168.2.4	354 Enter message, ending with "." on a line by itself
Apr 8, 2021 12:14:14.480148077 CEST	49764	587	192.168.2.4	69.65.3.206	.
Apr 8, 2021 12:14:15.217732906 CEST	587	49764	69.65.3.206	192.168.2.4	250 OK id=1lURfy-0003vO-DX

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: payment details.exe PID: 7008 Parent PID: 5908

General

Start time:	12:12:11
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\payment details.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\payment details.exe'
Imagebase:	0x800000
File size:	729600 bytes
MD5 hash:	55191839573AC8FD25655B3561286BC1
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: 00000000.00000002.690986558.0000000003C59000.00000004.00000001.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	6D1CCF06	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	6D1CCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\payment details.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D4DC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\payment details.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	6D4DC907	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	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile

Analysis Process: payment details.exe PID: 1320 Parent PID: 7008

General

Start time:	12:12:25
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\payment details.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x620000
File size:	729600 bytes
MD5 hash:	55191839573AC8FD25655B3561286BC1
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: 00000005.00000002.916754002.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.920699036.00000000029B1000.00000004.00000001.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	6D1CCF06	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	6D1CCF06	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	6C01BEFF	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	6C01DD66	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	6C01DD66	CopyFileW

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\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 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 57 5a 6e 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 18 0b 00 00 08 00 00 00 00 00 00 16 36 0b 00 00 20 00 00 00 40 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 0b 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 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...WZn`.......... ....0..............6... ...@....@.. ....@.................	success or wait	3	6C01DD66	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	6C01DD66	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	6C011B4F	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	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C011B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\3077ea46-2415-405d-bbef-e858905f2c49	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6C011B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C011B4F	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	6C01646A	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	6C01DE2E	RegSetValueExW

Analysis Process: kprUEGC.exe PID: 6692 Parent PID: 3424

General

Start time:	12:13:03
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe'
Imagebase:	0x3c0000
File size:	729600 bytes
MD5 hash:	55191839573AC8FD25655B3561286BC1
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: 0000000F.00000002.795750062.00000000037E9000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 33%, 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	6D1CCF06	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	6D1CCF06	unknown
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	6D4DC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\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	6D4DC907	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	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile

Analysis Process: kprUEGC.exe PID: 7132 Parent PID: 3424

General

Start time:	12:13:11
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe'
Imagebase:	0x7f0000
File size:	729600 bytes
MD5 hash:	55191839573AC8FD25655B3561286BC1
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: 00000010.00000002.816268269.0000000003C09000.00000004.00000001.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	6D1CCF06	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	6D1CCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile

Analysis Process: kprUEGC.exe PID: 6932 Parent PID: 6692

General

Start time:	12:13:16
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xc40000
File size:	729600 bytes
MD5 hash:	55191839573AC8FD25655B3561286BC1
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: 00000012.00000002.818572720.00000000030F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000002.818572720.00000000030F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.817039638.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1CCF06	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	6D1CCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile

Analysis Process: kprUEGC.exe PID: 816 Parent PID: 7132

General

Start time:	12:13:25
Start date:	08/04/2021
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xc00000
File size:	729600 bytes
MD5 hash:	55191839573AC8FD25655B3561286BC1
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: 00000013.00000002.916752082.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000013.00000002.919584190.00000000031F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000013.00000002.919584190.00000000031F1000.00000004.00000001.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	6D1CCF06	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	6D1CCF06	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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	6C011B4F	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	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile

Disassembly

Code Analysis