ID: 385300
Sample Name: PAYMENT CONFIRMATION.exe
Cookbook: default.jbs
Time: 09:57:17
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

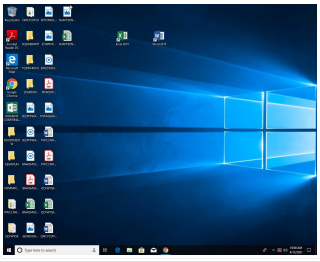
Analysis Report PAYMENT CONFIRMATION.exe

Overview

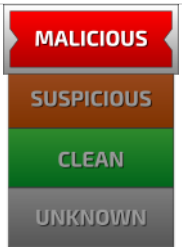
General Information

Sample Name:	PAYMENT CONFIRMATION.exe
Analysis ID:	385300
MD5:	b7724fd635cc9c0..
SHA1:	db18fe9a073456a.
SHA256:	6df1420d84c9c0a..
Tags:	AgentTesla
Infos:	

Most interesting Screenshot:



Detection



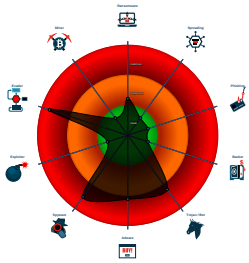
AgentTesla

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …
- Installs a global keyboard hook
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Modifies the hosts file
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**
- PAYMENT CONFIRMATION.exe (PID: 5940 cmdline: 'C:\Users\user\Desktop\PAYMENT CONFIRMATION.exe' MD5: B7724FD635CC9C0AC12AF69468D8F734)
  - PAYMENT CONFIRMATION.exe (PID: 2208 cmdline: {path} MD5: B7724FD635CC9C0AC12AF69468D8F734)
- kprUEGC.exe (PID: 4156 cmdline: 'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe' MD5: B7724FD635CC9C0AC12AF69468D8F734)
  - kprUEGC.exe (PID: 6672 cmdline: {path} MD5: B7724FD635CC9C0AC12AF69468D8F734)
- kprUEGC.exe (PID: 6652 cmdline: 'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe' MD5: B7724FD635CC9C0AC12AF69468D8F734)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

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

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000014.00000002.466854304.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.466852718.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.218173630.00000000035A9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000002.303769479.0000000003CB9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000014.00000002.472291889.0000000002BE1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 10 entries				

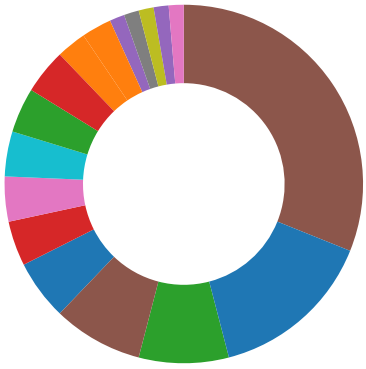
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.PAYMENT CONFIRMATION.exe.37d32c0.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
8.2.kprUEGC.exe.3ee32c0.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
2.2.PAYMENT CONFIRMATION.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
20.2.kprUEGC.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.PAYMENT CONFIRMATION.exe.37d32c0.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Modifies the hosts file

Lowering of HIPS / PFW / Operating System Security Settings:

Modifies the hosts file

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

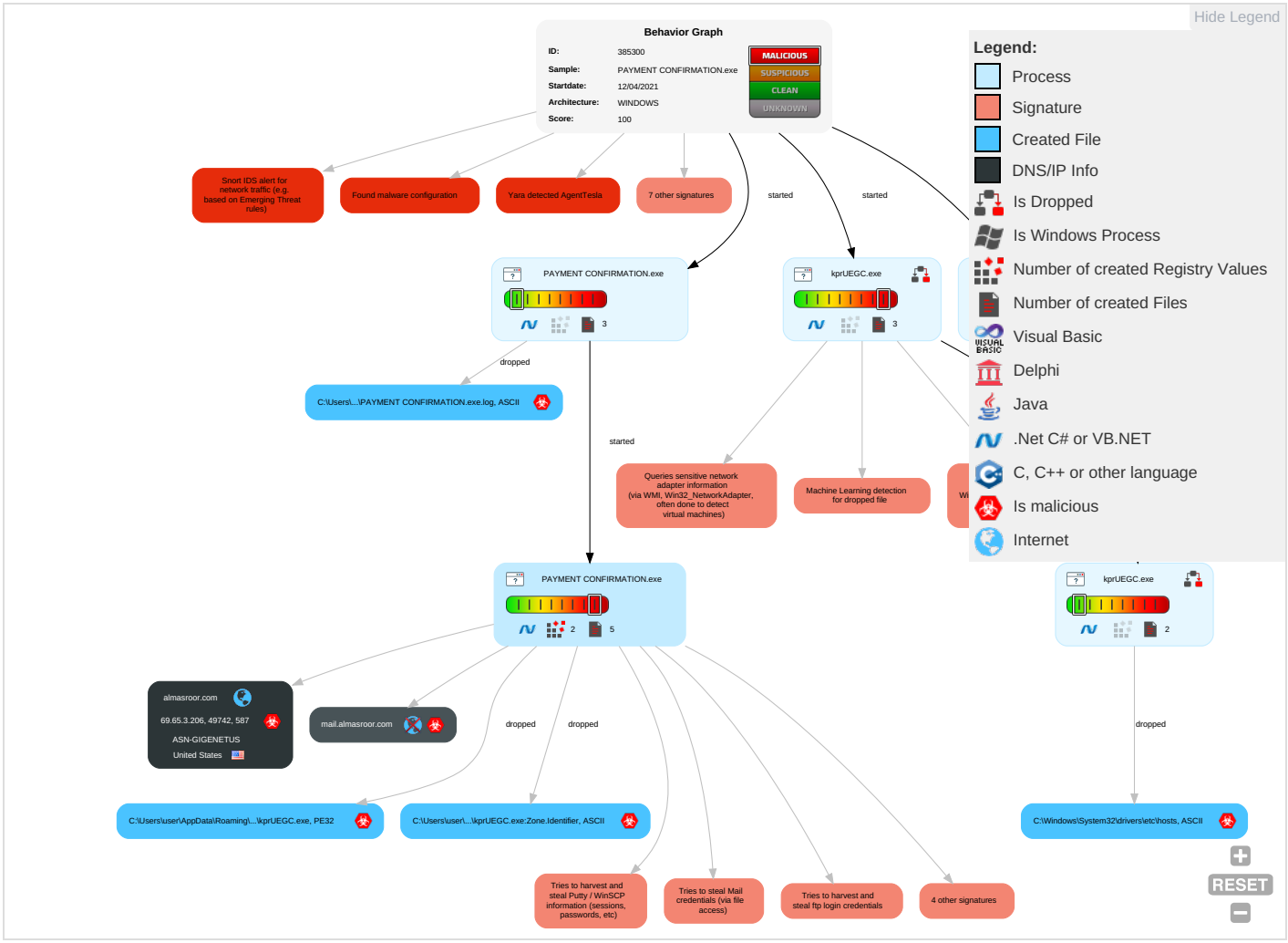
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 1 1	Registry Run Keys / Startup Folder 1	Process Injection 1 2	File and Directory Permissions Modification 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Oth Network Medium
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Disable or Modify Tools 1	Input Capture 1 1 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth

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

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PAYMENT CONFIRMATION.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.PAYMENT CONFIRMATION.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
20.2.kprUEGC.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://almasroor.com	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://IJiNPGixATMzyiVeKdM.org	0%	Avira URL Cloud	safe	
http://bQxorv.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%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://api.ipify.org%0	0%	Avira URL Cloud	safe	
http://mail.almasroor.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

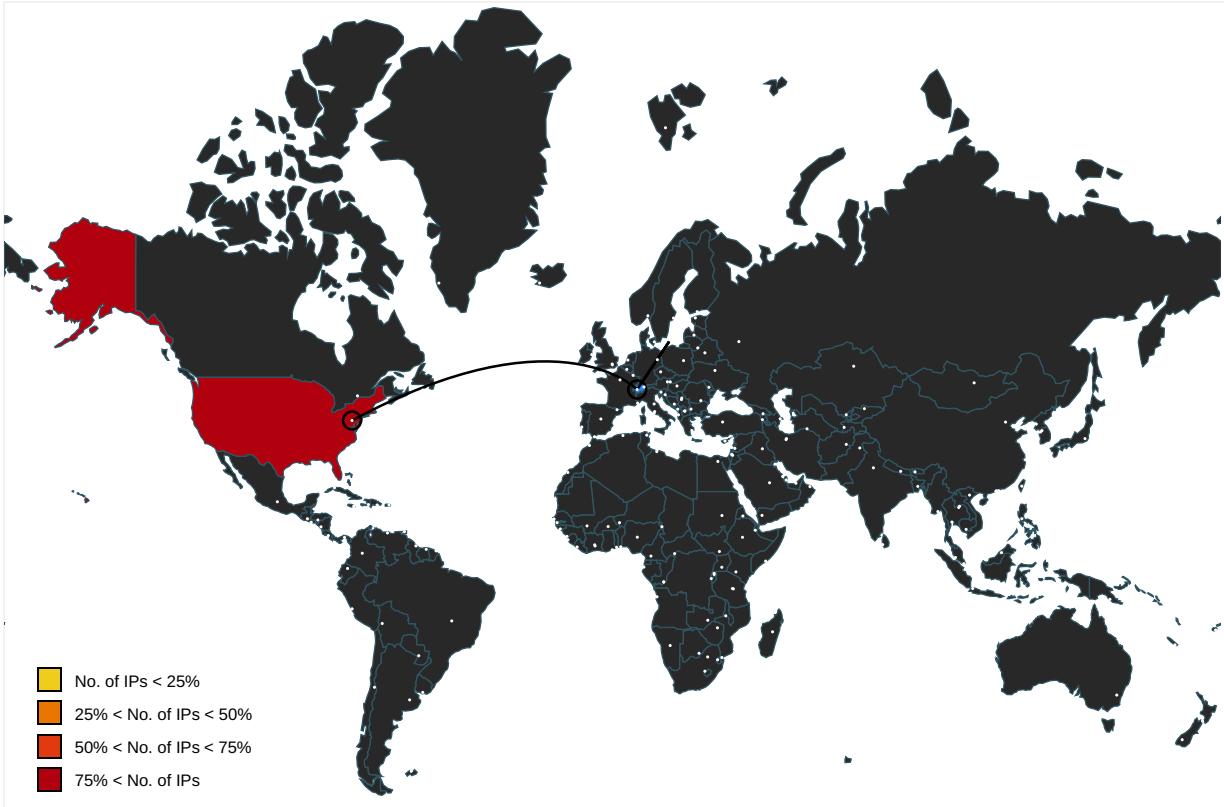
Name	IP	Active	Malicious	Antivirus Detection	Reputation
almasroor.com	69.65.3.206	true	true		unknown
mail.almasroor.com	unknown	unknown	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://almasroor.com	PAYMENT CONFIRMATION.exe, 00000002.00000002.476420854.000000000340C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	PAYMENT CONFIRMATION.exe, 00000002.00000002.473828679.000000000003151000.00000004.00000001.sdmp, kprUEGC.exe, 00000014.00000002.472291889.0000000002BE1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.ipify.org%GETMozilla/5.0	kprUEGC.exe, 00000014.00000002.472291889.0000000002BE1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://DynDns.comDynDNS	kprUEGC.exe, 00000014.00000002.472291889.0000000002BE1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://IJiNPGixATMzyiVeKdM.org	PAYMENT CONFIRMATION.exe, 00000002.00000002.476023319.00000000033D1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://bQxorv.com	kprUEGC.exe, 00000014.00000002.472291889.0000000002BE1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	PAYMENT CONFIRMATION.exe, 00000002.00000002.473828679.0000000003151000.00000004.00000001.sdmp, kprUEGC.exe, 00000014.00000002.472291889.0000000002BE1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%0	PAYMENT CONFIRMATION.exe, 00000002.00000002.473828679.0000000003151000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://mail.almasroor.com	PAYMENT CONFIRMATION.exe, 00000002.00000002.476420854.000000000340C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	PAYMENT CONFIRMATION.exe, 00000001.00000002.218173630.0000000035A9000.00000004.00000001.sdmp, PAYMENT CONFIRMATION.exe, 00000002.00000002.466852718.0000000000402000.00000040.00000001.sdmp, kprUEGC.exe, 00000008.00000002.303769479.0000000003CB9000.00000004.00000001.sdmp, kprUEGC.exe, 00000014.00000002.466854304.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

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

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385300

Start date:	12.04.2021
Start time:	09:57:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PAYMENT CONFIRMATION.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:	30
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@7/6@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0%) • Quality average: 0% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 92.122.145.220, 204.79.197.200, 13.107.21.200, 52.255.188.83, 40.88.32.150, 20.82.210.154, 184.30.24.56, 92.122.213.247, 92.122.213.194, 93.184.221.240, 13.88.21.125, 52.155.217.156, 20.54.26.129, 104.42.151.234 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:58:05	API Interceptor	723x Sleep call for process: PAYMENT CONFIRMATION.exe modified
09:58:34	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run kprUEGC C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
09:58:42	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run kprUEGC C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
09:58:44	API Interceptor	493x Sleep call for process: kprUEGC.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
69.65.3.206	payment details.exe	Get hash	malicious	Browse	
	payment details.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ASN-GIGENETUS	MT103_Swift_Transfer#452-567-2XXX.exe	Get hash	malicious	Browse	• 45.85.90.86
	4IxLUYjMQ7.exe	Get hash	malicious	Browse	• 172.111.237.51
	payment details.exe	Get hash	malicious	Browse	• 69.65.3.206
	payment details.exe	Get hash	malicious	Browse	• 69.65.3.206
	AWB-9899691012.exe	Get hash	malicious	Browse	• 45.85.90.220
	swift_76567643.exe	Get hash	malicious	Browse	• 70.32.1.32
	BillOfLading.exe	Get hash	malicious	Browse	• 45.85.90.220
	OPEN01929291000_2021-03-15_07-28.exe	Get hash	malicious	Browse	• 45.85.90.188
	INV242-0303.doc	Get hash	malicious	Browse	• 45.85.90.197
	dwg.exe	Get hash	malicious	Browse	• 45.85.90.226
	a55ddff55740467df8dee39a5bbaee32.exe	Get hash	malicious	Browse	• 45.85.90.138
	116e4c42d3948c91eafdcb60a9f37014.exe	Get hash	malicious	Browse	• 45.85.90.138
	771eb3ef5ede516d6ec53ae40b3f888f.exe	Get hash	malicious	Browse	• 45.85.90.138
	Paid Invoice _confirmation_9336639_03993736553.exe	Get hash	malicious	Browse	• 216.38.7.225
	YCVj3q7r5e.exe	Get hash	malicious	Browse	• 70.32.1.32
	VOR001 - McMurray Statements December 2020_8737353 5737522772662626.exe	Get hash	malicious	Browse	• 216.38.7.225
	Customer_Receivables_Aging_20210112_26635353452424 24242.exe	Get hash	malicious	Browse	• 216.38.7.225
	Proforma fatura.exe	Get hash	malicious	Browse	• 216.38.2.215
	Invoice.exe	Get hash	malicious	Browse	• 216.38.2.215
	Purchase Order-34002174,pdf.exe	Get hash	malicious	Browse	• 216.38.7.231

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PAYMENT CONFIRMATION.exe.log	
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kprUEGC.exe.log	
Process:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	
Process:	C:\Users\user\Desktop\PAYMENT CONFIRMATION.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	834048
Entropy (8bit):	7.428971755376777
Encrypted:	false
SSDEEP:	12288:IpKyZu+9vsh+aNW314fEJsMXuLvfm7AAFyKWiFydoKVh8onDA4w:h+arklruLW7ZsKWgydFVWUHw
MD5:	B7724FD635CC9C0AC12AF69468D8F734
SHA1:	DB18FE9A073456A11A8346E510B3D04D6F64ADC9
SHA-256:	6DF1420D84C9C0A1427B91FDF3E9FE8B6245F9F8EA3B00658C430106E72D33D8
SHA-512:	68482D26DE5A521CA4AE2A139C2DEA2EB491381568C344F76C737844162D42F94B117C13C903812EA4CEA5F6D2F130425D5CA869FA8A165AC1D136C25E0C98F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....=_.....0..(.....F... ...`....@.. ..... ..... ..@.....F..O...`.....F..... ....H.....text....'... ...(..... ..`.rsrc.....`.....*.....@..@.reloc..... .....@..B.....F.....H.....4o.....1.....2.....".(....*.r...p.....*..{....*"..}....*..{....*"..}....*"..(....*.0.....r...p.+..*..0.....r...p.+..*"..(....*..{....*"..}....*..{....*"..}....*"..(....*^..}.....(.....(....*..0.....o.....,y.s.....{....o....o.....{....o....o....~.....,...(.....+....(.....,..(....o....s...(.....+..r...p(....&..*....0..5.....o....r..p(.....,..o....r...p(....+....,....+...+..*....0..

C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\PAYMENT CONFIRMATION.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

C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe:Zone.Identifier	
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.428971755376777
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	PAYMENT CONFIRMATION.exe
File size:	834048
MD5:	b7724fd635cc9c0ac12af69468d8f734
SHA1:	db18fe9a073456a11a8346e510b3d04d6f64adc9
SHA256:	6df1420d84c9c0a1427b91fdf3e9fe8b6245f9f8ea3b00658c430106e72d33d8
SHA512:	68482d26de5a521ca4ae2a139c2dea2eb491381568c344f76c737844162d42f94b117c13c903812ea4cea5f6d2f130425d5ca869fa8a165ac1d136c25e0c98f7
SSDEEP:	12288:IpKyZu+9vsh+aNW314fEJsMXuLvfm7AAFyKWiFydoKVh8onDA4w:h+arklruLW7ZsKWgydFVWUHw
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....=_.....0..(.....F... ...`....@.. ....@.....

File Icon

Icon Hash:	07d8d8d4d4d85026

Static PE Info

General

Entrypoint:	0x4a46fa
Entrypoint Section:	.text
Digitally signed:	false

General

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:	0xF55F3D02 [Mon Jun 14 12:30:58 2100 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa46a8	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa6000	0x28c80	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd0000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xa468c	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0xa2700	0xa2800	False	0.899269831731	data	7.88580318793	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa6000	0x28c80	0x28e00	False	0.0481293004587	data	2.99758740857	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd0000	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_ICON	0xa62b0	0xc35	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xa6ee8	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 4280119364, next used block 4280119364		
RT_ICON	0xb7710	0x94a8	data		
RT_ICON	0xc0bb8	0x5488	data		
RT_ICON	0xc6040	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xca268	0x25a8	data		
RT_ICON	0xcc810	0x10a8	data		
RT_ICON	0xcd8b8	0x988	data		
RT_ICON	0xce240	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xce6a8	0x84	data		
RT_VERSION	0xce72c	0x366	data		
RT_MANIFEST	0xcea94	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

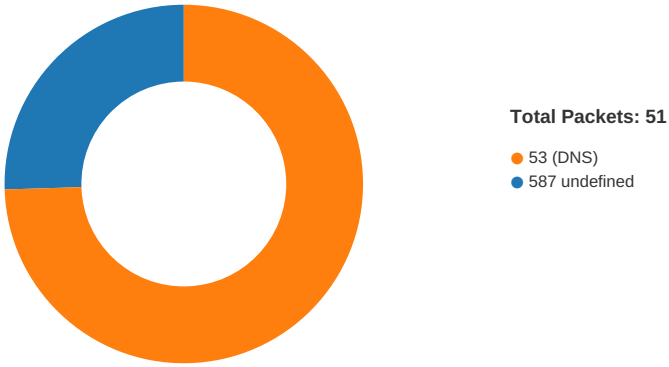
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Integra Wealth
Assembly Version	1.8.9.10
InternalName	48Vu.exe
FileVersion	1.9.1.0
CompanyName	Integra Wealth
LegalTrademarks	
Comments	
ProductName	ReplacementFallback
ProductVersion	1.9.1.0
FileDescription	ReplacementFallback
OriginalFilename	48Vu.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/12/21-09:59:55.552553	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49742	587	192.168.2.3	69.65.3.206

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:59:54.088561058 CEST	49742	587	192.168.2.3	69.65.3.206
Apr 12, 2021 09:59:54.232836962 CEST	587	49742	69.65.3.206	192.168.2.3
Apr 12, 2021 09:59:54.233000040 CEST	49742	587	192.168.2.3	69.65.3.206
Apr 12, 2021 09:59:54.663244963 CEST	587	49742	69.65.3.206	192.168.2.3
Apr 12, 2021 09:59:54.663727045 CEST	49742	587	192.168.2.3	69.65.3.206
Apr 12, 2021 09:59:54.808820009 CEST	587	49742	69.65.3.206	192.168.2.3
Apr 12, 2021 09:59:54.811714888 CEST	49742	587	192.168.2.3	69.65.3.206
Apr 12, 2021 09:59:54.956993103 CEST	587	49742	69.65.3.206	192.168.2.3
Apr 12, 2021 09:59:54.957669020 CEST	49742	587	192.168.2.3	69.65.3.206
Apr 12, 2021 09:59:55.113687992 CEST	587	49742	69.65.3.206	192.168.2.3
Apr 12, 2021 09:59:55.114670038 CEST	49742	587	192.168.2.3	69.65.3.206
Apr 12, 2021 09:59:55.259448051 CEST	587	49742	69.65.3.206	192.168.2.3
Apr 12, 2021 09:59:55.259762049 CEST	49742	587	192.168.2.3	69.65.3.206
Apr 12, 2021 09:59:55.405204058 CEST	587	49742	69.65.3.206	192.168.2.3
Apr 12, 2021 09:59:55.405466080 CEST	49742	587	192.168.2.3	69.65.3.206
Apr 12, 2021 09:59:55.549216032 CEST	587	49742	69.65.3.206	192.168.2.3
Apr 12, 2021 09:59:55.549290895 CEST	587	49742	69.65.3.206	192.168.2.3
Apr 12, 2021 09:59:55.552552938 CEST	49742	587	192.168.2.3	69.65.3.206
Apr 12, 2021 09:59:55.552654028 CEST	49742	587	192.168.2.3	69.65.3.206
Apr 12, 2021 09:59:55.552716970 CEST	49742	587	192.168.2.3	69.65.3.206
Apr 12, 2021 09:59:55.552788019 CEST	49742	587	192.168.2.3	69.65.3.206
Apr 12, 2021 09:59:55.698920012 CEST	587	49742	69.65.3.206	192.168.2.3
Apr 12, 2021 09:59:55.698946953 CEST	587	49742	69.65.3.206	192.168.2.3
Apr 12, 2021 09:59:56.236152887 CEST	587	49742	69.65.3.206	192.168.2.3
Apr 12, 2021 09:59:56.290321112 CEST	49742	587	192.168.2.3	69.65.3.206

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:57:55.587584972 CEST	60985	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:57:55.638468027 CEST	50200	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:57:55.639493942 CEST	53	60985	8.8.8.8	192.168.2.3
Apr 12, 2021 09:57:55.704214096 CEST	53	50200	8.8.8.8	192.168.2.3
Apr 12, 2021 09:57:56.377810001 CEST	51281	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:57:56.440128088 CEST	53	51281	8.8.8.8	192.168.2.3
Apr 12, 2021 09:57:56.450364113 CEST	49199	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:57:56.498913050 CEST	53	49199	8.8.8.8	192.168.2.3
Apr 12, 2021 09:57:57.269068956 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:57:57.317923069 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 12, 2021 09:57:58.068525076 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:57:58.120682001 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 12, 2021 09:57:58.821706057 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:57:58.870714903 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 12, 2021 09:57:59.638966084 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:57:59.687730074 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 12, 2021 09:58:00.577747107 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:58:00.626516104 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 12, 2021 09:58:30.339270115 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:58:30.390690088 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 12, 2021 09:58:31.080108881 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:58:31.128791094 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 12, 2021 09:58:34.399143934 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:58:34.457848072 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 12, 2021 09:58:48.740354061 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:58:48.804146051 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 12, 2021 09:58:51.585805893 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:58:51.645958900 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 12, 2021 09:59:03.086510897 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:59:03.138180017 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 12, 2021 09:59:06.837461948 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:59:06.909998894 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 12, 2021 09:59:07.632153034 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:59:07.692271948 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 12, 2021 09:59:08.284568071 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:59:08.382776976 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 12, 2021 09:59:08.687506914 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:59:08.756638050 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 12, 2021 09:59:08.792792082 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:59:08.895992994 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 12, 2021 09:59:09.449558973 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:59:09.509342909 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 12, 2021 09:59:10.151315928 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:59:10.213434935 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 12, 2021 09:59:10.714092970 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:59:10.762897015 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 12, 2021 09:59:11.785434008 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:59:11.843231916 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 12, 2021 09:59:12.802987099 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:59:12.828646898 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:59:12.853539944 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 12, 2021 09:59:12.887991905 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 12, 2021 09:59:13.582056999 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:59:13.647248983 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 12, 2021 09:59:35.013001919 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:59:35.064810991 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 12, 2021 09:59:35.850492954 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:59:35.899192095 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 12, 2021 09:59:39.907916069 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:59:39.958430052 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 12, 2021 09:59:41.477659941 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:59:41.529227972 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 12, 2021 09:59:43.152086973 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:59:43.200777054 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 12, 2021 09:59:43.928356886 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:59:43.977123976 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 12, 2021 09:59:45.453090906 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:59:45.525468111 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 12, 2021 09:59:52.986248970 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:59:53.037791014 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 12, 2021 09:59:53.629669905 CEST	63619	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:59:53.803836107 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 12, 2021 09:59:53.826715946 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:59:53.999140978 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 12, 2021 09:59:59.819197893 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:59:59.867813110 CEST	53	61946	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 09:59:53.629669905 CEST	192.168.2.3	8.8.8.8	0x449c	Standard query (0)	mail.almasroor.com	A (IP address)	IN (0x0001)
Apr 12, 2021 09:59:53.826715946 CEST	192.168.2.3	8.8.8.8	0xd0dd	Standard query (0)	mail.almasroor.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 09:59:53.803836107 CEST	8.8.8.8	192.168.2.3	0x449c	No error (0)	mail.almasroor.com	almasroor.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 09:59:53.803836107 CEST	8.8.8.8	192.168.2.3	0x449c	No error (0)	almasroor.com		69.65.3.206	A (IP address)	IN (0x0001)
Apr 12, 2021 09:59:53.999140978 CEST	8.8.8.8	192.168.2.3	0xd0dd	No error (0)	mail.almasroor.com	almasroor.com		CNAME (Canonical name)	IN (0x0001)
Apr 12, 2021 09:59:53.999140978 CEST	8.8.8.8	192.168.2.3	0xd0dd	No error (0)	almasroor.com		69.65.3.206	A (IP address)	IN (0x0001)

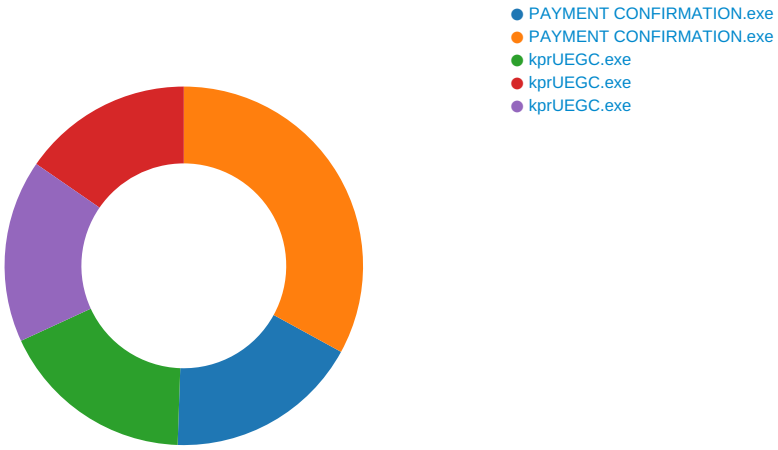
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Apr 12, 2021 09:59:54.663244963 CEST	587	49742	69.65.3.206	192.168.2.3	220-server302.webhostingpad.com ESMTP Exim 4.93 #2 Mon, 12 Apr 2021 02:59:54 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Apr 12, 2021 09:59:54.663727045 CEST	49742	587	192.168.2.3	69.65.3.206	EHLO 347688
Apr 12, 2021 09:59:54.808820009 CEST	587	49742	69.65.3.206	192.168.2.3	250-server302.webhostingpad.com Hello 347688 [84.17.52.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Apr 12, 2021 09:59:54.811714888 CEST	49742	587	192.168.2.3	69.65.3.206	AUTH login aG9AYWxtYXNyb29yLmNvbQ==
Apr 12, 2021 09:59:54.956993103 CEST	587	49742	69.65.3.206	192.168.2.3	334 UGFzc3dvcmQ6
Apr 12, 2021 09:59:55.113687992 CEST	587	49742	69.65.3.206	192.168.2.3	235 Authentication succeeded
Apr 12, 2021 09:59:55.114670038 CEST	49742	587	192.168.2.3	69.65.3.206	MAIL FROM:<ho@almasroor.com>
Apr 12, 2021 09:59:55.259448051 CEST	587	49742	69.65.3.206	192.168.2.3	250 OK
Apr 12, 2021 09:59:55.259762049 CEST	49742	587	192.168.2.3	69.65.3.206	RCPT TO:<ho@almasroor.com>
Apr 12, 2021 09:59:55.405204058 CEST	587	49742	69.65.3.206	192.168.2.3	250 Accepted
Apr 12, 2021 09:59:55.405466080 CEST	49742	587	192.168.2.3	69.65.3.206	DATA
Apr 12, 2021 09:59:55.549290895 CEST	587	49742	69.65.3.206	192.168.2.3	354 Enter message, ending with "." on a line by itself
Apr 12, 2021 09:59:55.552788019 CEST	49742	587	192.168.2.3	69.65.3.206	.
Apr 12, 2021 09:59:56.236152887 CEST	587	49742	69.65.3.206	192.168.2.3	250 OK id=1lVrUB-0005PN-Fi

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: PAYMENT CONFIRMATION.exe PID: 5940 Parent PID: 5700

General

Start time:	09:58:04
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\PAYMENT CONFIRMATION.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PAYMENT CONFIRMATION.exe'
Imagebase:	0x170000
File size:	834048 bytes
MD5 hash:	B7724FD635CC9C0AC12AF69468D8F734
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: 00000001.00000002.218173630.00000000035A9000.00000004.00000001.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	6E0ACF06	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	6E0ACF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PAYMENT CONFIRMATION.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3BC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PAYMENT CONFIRMATION.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E3BC907	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	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile

Analysis Process: PAYMENT CONFIRMATION.exe PID: 2208 Parent PID: 5940

General

Start time:	09:58:11
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\PAYMENT CONFIRMATION.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xd50000
File size:	834048 bytes
MD5 hash:	B7724FD635CC9C0AC12AF69468D8F734
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: 00000002.00000002.466852718.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.473828679.0000000003151000.00000004.00000001.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	6E0ACF06	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	6E0ACF06	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	6CEFBEFF	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	6CEFDD66	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	6CEFDD66	CopyFileW

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 02 3d 5f f5 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 28 0a 00 00 90 02 00 00 00 00 00 fa 46 0a 00 00 20 00 00 00 60 0a 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 0d 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..(...........F... ...`....@.. ....@................	success or wait	4	6CEFDD66	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	6CEFDD66	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	6CEF1B4F	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	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11168	success or wait	1	6CEF1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\c83ff6ed-de12-410b-845f-d450d93af7a4	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11168	success or wait	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CEF1B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	kprUEGC	unicode	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	success or wait	1	6CEF646A	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	6CEFDE2E	RegSetValueExW

Analysis Process: kprUEGC.exe PID: 4156 Parent PID: 3388

General

Start time:	09:58:42
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe'
Imagebase:	0x7f0000
File size:	834048 bytes
MD5 hash:	B7724FD635CC9C0AC12AF69468D8F734
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: 00000008.00000002.303769479.0000000003CB9000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
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	6E0ACF06	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	6E0ACF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kprUEGC.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3BC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kprUEGC.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E3BC907	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	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile

Analysis Process: kprUEGC.exe PID: 6652 Parent PID: 3388

General

Start time:	09:58:50
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe'
Imagebase:	0x570000
File size:	834048 bytes
MD5 hash:	B7724FD635CC9C0AC12AF69468D8F734
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	6E0ACF06	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	6E0ACF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile

Analysis Process: kprUEGC.exe PID: 6672 Parent PID: 4156

General

Start time:	09:58:51
Start date:	12/04/2021
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x6e0000
File size:	834048 bytes
MD5 hash:	B7724FD635CC9C0AC12AF69468D8F734
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000014.00000002.466854304.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000014.00000002.472291889.0000000002BE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000014.00000002.472291889.0000000002BE1000.00000004.00000001.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	6E0ACF06	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	6E0ACF06	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	6CEF1B4F	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	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile

Disassembly

Code Analysis