Joe Sandbox Cloud BASIC

ID: 528711
Sample Name: Euro invoice.exe
Cookbook: default.jbs
Time: 17:40:23
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

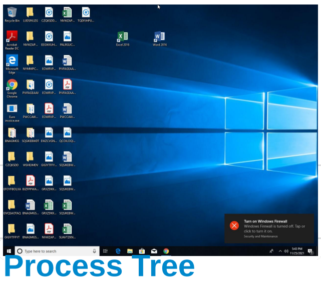
Windows Analysis Report Euro invoice.exe

Overview

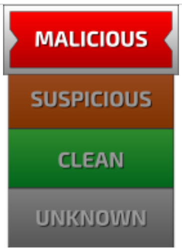
General Information

Sample Name:	Euro invoice.exe
Analysis ID:	528711
MD5:	15f79ec8cfa1ad6..
SHA1:	3b48453cc5680c..
SHA256:	49d22404c910a5..
Tags:	agenttesla exe
Infos:	

Most interesting Screenshot:



Detection



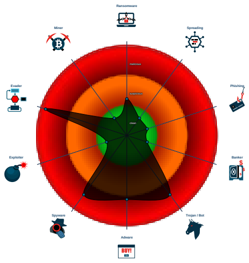
AgentTesla

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Tries to steal Mail credentials (via fil…
- Sigma detected: Bad Opsec Default…
- Initial sample is a PE file and has a …
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Modifies the hosts file
- Tries to detect sandboxes and other…

Classification



Process Tree

- System is w10x64
- Euro invoice.exe (PID: 5764 cmdline: "C:\Users\user\Desktop\Euro invoice.exe" MD5: 15F79EC8CFA1AD6C24767D4CA45AA4CD)
  - RegSvcs.exe (PID: 5620 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
  - RegSvcs.exe (PID: 6692 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
  - RegSvcs.exe (PID: 6980 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- kprUEGC.exe (PID: 7164 cmdline: "C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe" MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 6040 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- kprUEGC.exe (PID: 3932 cmdline: "C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe" MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 5788 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cleanup

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "support25@vrlogistic.net",
  "Password": "support25!@#$",
  "Host": "mail.vrlogistic.net"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000000.301908839.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000000.301908839.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000005.00000000.300860583.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000000.300860583.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.304280819.0000000003430000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.0.RegSvcs.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.0.RegSvcs.exe.400000.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
5.0.RegSvcs.exe.400000.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.0.RegSvcs.exe.400000.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.Euro invoice.exe.43f4370.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 15 entries				

Sigma Overview

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

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

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

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

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

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

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

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 steal Mail credentials (via file / registry access)

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

Tries to harvest and steal ftp login credentials

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

Remote Access Functionality:

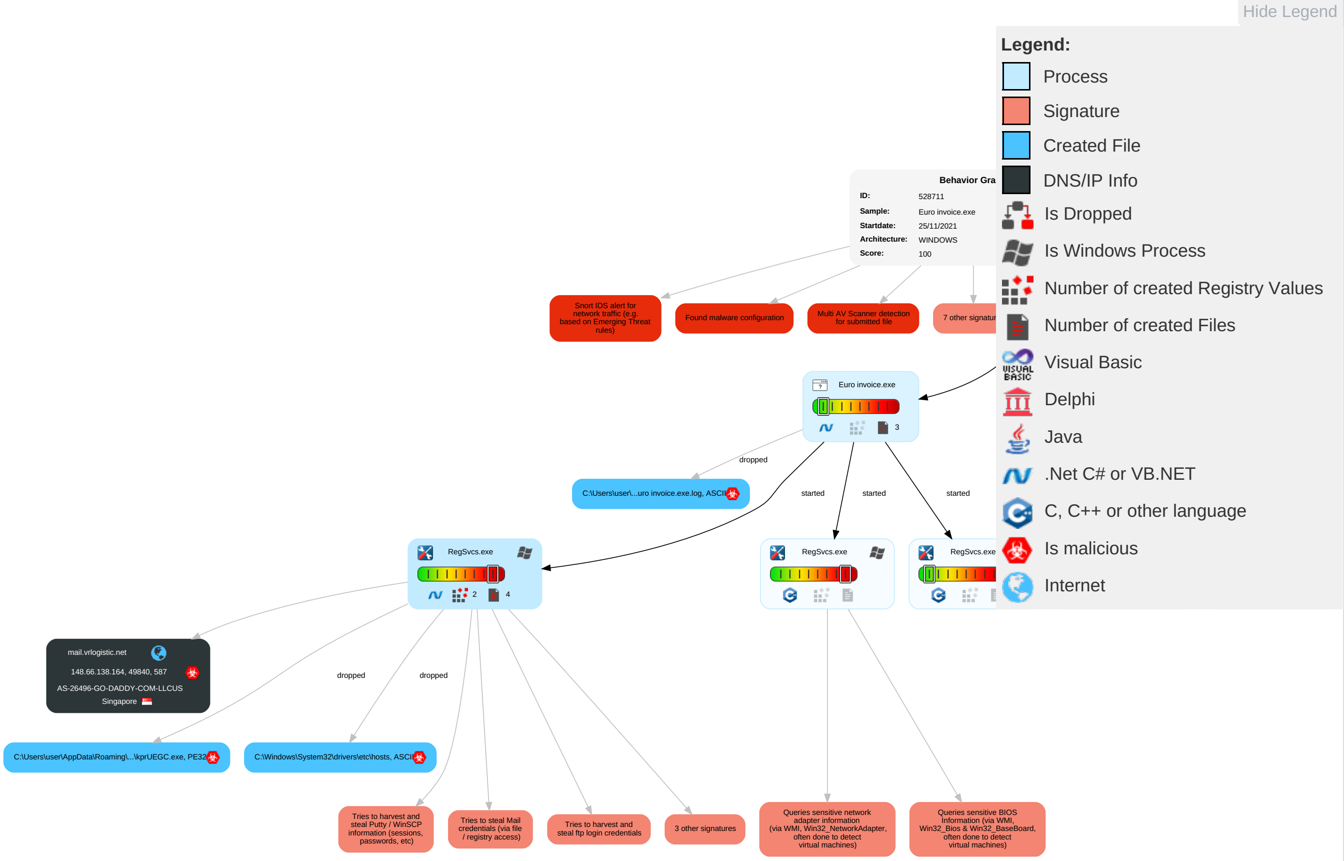
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Registry Run Keys / Startup Folder 1	Process Injection 1 2	File and Directory Permissions Modification 1	OS Credential Dumping 2	System Information Discovery 1 1 4	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Disable or Modify Tools 1	Credentials in Registry 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	Virtualization/Sandbox Evasion 1 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 3	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

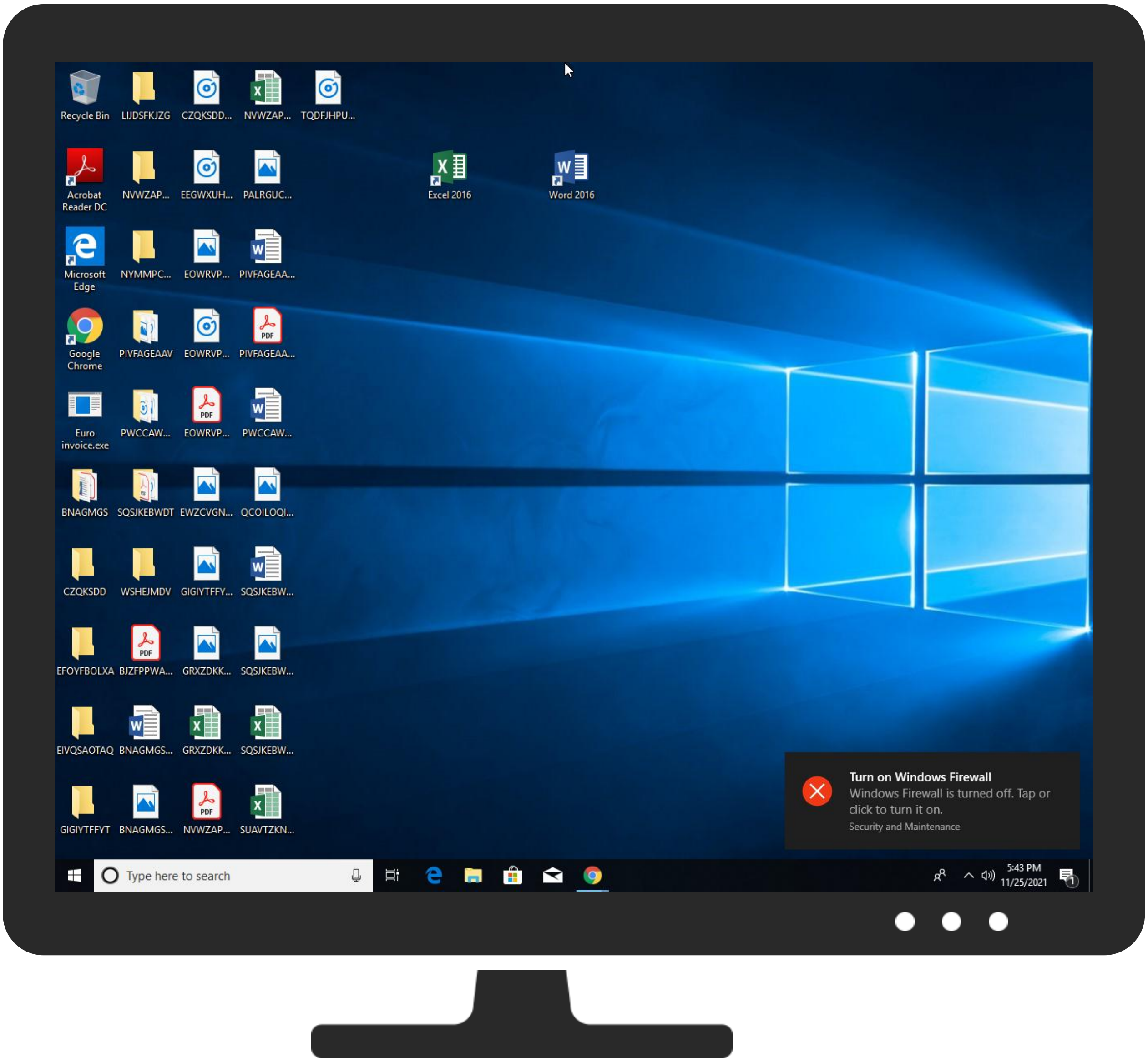
Behavior Graph


Hide Legend
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet
Behavior Gra
ID: 528711
Sample: Euro invoice.exe
Startdate: 25/11/2021
Architecture: WINDOWS
Score: 100
Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
Found malware configuration
Multi AV Scanner detection for submitted file
7 other signatur
Euro invoice.exe
3
dropped
C:\Users\user\...uro invoice.exe.log, ASCII
started
started
started
RegSvcs.exe
2
4
RegSvcs.exe
RegSvcs.exe
mail.vrlogistic.net
148.66.138.164, 49840, 587
AS-26496-GO-DADDY-COM-LLCUS
Singapore
dropped
dropped
C:\Users\user\AppData\Roaming\...\kprUEGC.exe, PE32
C:\Windows\System32\drivers\etc\hosts, ASCII
Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
Tries to steal Mail credentials (via file / registry access)
Tries to harvest and steal ftp login credentials
3 other signatures
Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)
Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Screenshots

Thumbnails

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



Turn on Windows Firewall
Windows Firewall is turned off. Tap or click to turn it on.
Security and Maintenance

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Euro invoice.exe	33%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.RegSvcs.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.RegSvcs.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.RegSvcs.exe.400000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Source	Detection	Scanner	Label	Link	Download
5.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.0.RegSvcs.exe.400000.3.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.microsoft.co)X	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://Fedebu.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://k5CVS3sUuqbD95uELlH.net	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	0%	URL Reputation	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://mail.vrlogistic.net	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.vrlogistic.net	148.66.138.164	true	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
148.66.138.164	mail.vrlogistic.net	Singapore	🇸🇬	26496	AS-26496-GO-DADDY-COM-LLCUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528711
Start date:	25.11.2021
Start time:	17:40:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Euro invoice.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:	27
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@11/6@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.3% (good quality ratio 0.2%) • Quality average: 26% • Quality standard deviation: 26.7%
HCA Information:	• Successful, ratio: 97% • 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

Simulations

Behavior and APIs

Time	Type	Description
17:41:21	API Interceptor	40x Sleep call for process: Euro invoice.exe modified
17:41:35	API Interceptor	752x Sleep call for process: RegSvcs.exe modified
17:41:48	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run kprUEGC C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
17:41:56	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run kprUEGC C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
148.66.138.164	41Scan007.exe	Get hash	malicious	Browse	• innovativewebtechnology.com/dev/Panel/five/fre.php

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.vrlogistic.net	Euro invoice.exe	Get hash	malicious	Browse	• 148.66.138.164
	Euro invoice.exe	Get hash	malicious	Browse	• 148.66.138.164

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-26496-GO-DADDY-COM-LLCUS	Akiru.arm7	Get hash	malicious	Browse	• 192.186.196.248
	xDG1WDcI0o.exe	Get hash	malicious	Browse	• 173.201.185.205
	RFQ_PO-330758290144.xlsx	Get hash	malicious	Browse	• 166.62.110.60
	Arrival Notice, CIA Awb Inv Form.pdf.exe	Get hash	malicious	Browse	• 184.168.98.97
	Euro invoice.exe	Get hash	malicious	Browse	• 148.66.138.164
	New Order778880.exe	Get hash	malicious	Browse	• 173.201.188.238
	c0az1l4js3001lsk4xd9n.x86-20211124-0850	Get hash	malicious	Browse	• 192.169.147.26

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Euro invoice.exe	Get hash	malicious	Browse	- 148.66.138.164
	DHL express 5809439160_pdf.exe	Get hash	malicious	Browse	- 184.168.96.165
	Payment transfer.exe	Get hash	malicious	Browse	- 148.66.138.249
	k6j1IMWw7Q.exe	Get hash	malicious	Browse	- 184.168.119.143
	704.doc	Get hash	malicious	Browse	- 148.72.96.3
	nHSmNKw7PN.exe	Get hash	malicious	Browse	- 184.168.119.143
	New Order 000112221.exe	Get hash	malicious	Browse	- 173.201.188.238
	1711.doc	Get hash	malicious	Browse	- 72.167.40.83
	new order.exe	Get hash	malicious	Browse	- 107.180.56.180
	AD0eMpLdJo81Tjr.exe	Get hash	malicious	Browse	- 184.168.96.165
	202111161629639000582.exe	Get hash	malicious	Browse	- 45.40.150.136
	UNPDMVX63128.vbs	Get hash	malicious	Browse	- 104.238.97.193
	QLTWPAU89862.vbs	Get hash	malicious	Browse	- 104.238.97.193

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	NEW ORDER EN31628 EN31630.exe	Get hash	malicious	Browse	
	purchase order.exe	Get hash	malicious	Browse	
	TS#U007e039873663-30987637393.exe	Get hash	malicious	Browse	
	ERIG_0983763673-093876536783.exe	Get hash	malicious	Browse	
	Euro invoice.exe	Get hash	malicious	Browse	
	Shipping Document BL Draft.exe	Get hash	malicious	Browse	
	incorrect payment information.exe	Get hash	malicious	Browse	
	TransactionSummary_22-11-2021.exe	Get hash	malicious	Browse	
	SWIFT COPY.exe	Get hash	malicious	Browse	
	TT COPY.exe	Get hash	malicious	Browse	
	Payment Advice 50053945.exe	Get hash	malicious	Browse	
	750845PaymentReceipt.exe	Get hash	malicious	Browse	
	Copy BL and Debit Note.exe	Get hash	malicious	Browse	
	QUOTATION.exe	Get hash	malicious	Browse	
	PO_SBK4128332S.exe	Get hash	malicious	Browse	
	New order - C.S.I No. 0987.exe	Get hash	malicious	Browse	
	Bank payment swift message.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	HSBC Payment Advice.exe	Get hash	malicious	Browse	

Created / dropped Files

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

Process:	C:\Users\user\Desktop\Euro invoice.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2239
Entropy (8bit):	5.354287817410997
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjntHoxHhAHKzvr1qHXHK2HKgmHKovjHKs:iqXeqm00YqhQnouRqjntIxHeqzTw3q2W
MD5:	913D1EEA179415C6D08FB255AE42B99D
SHA1:	E994C612C0596994AAE55FBCE35B7A4FBE312FD7
SHA-256:	473B4000084ACF4C7D701CE72EBF71BD304054231B3BDF7CAF49898A1FDA13D0
SHA-512:	768045C288CEEE8FE1A099FC8CEA713B685F6ED3FD8BFA1C8E64CA09F7AF9FEBEA90F5277B28444AFF8F2AC7CD857DFCDF7D3A98CD86288925DB7A4A4234685
Malicious:	**true**
Reputation:	moderate, very likely benign file

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

Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",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,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

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:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WglAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczlAFXMWTyAGCDLIP12MUAvvw
MD5:	8C0458BB9EA02D50565175E38D577E35
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0F
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	768:bBbSoy+SdIBf0k2dsYyV6Iq87PiU9FViaLmf:EoOIBf0ddsYy8LUjVBC
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D0 B42
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: NEW ORDER EN31628 EN31630.exe, Detection: malicious, Browse • Filename: purchase order.exe, Detection: malicious, Browse • Filename: TS#U007e039873663-30987637393.exe, Detection: malicious, Browse • Filename: ERIG_0983763673-093876536783.exe, Detection: malicious, Browse • Filename: Euro invoice.exe, Detection: malicious, Browse • Filename: Shipping Document BL Draft.exe, Detection: malicious, Browse • Filename: incorrect payment information.exe, Detection: malicious, Browse • Filename: TransactionSummary_22-11-2021.exe, Detection: malicious, Browse • Filename: SWIFT COPY.exe, Detection: malicious, Browse • Filename: TT COPY.exe, Detection: malicious, Browse • Filename: Payment Advice 50053945.exe, Detection: malicious, Browse • Filename: 750845PaymentReceipt.exe, Detection: malicious, Browse • Filename: Copy BL and Debit Note.exe, Detection: malicious, Browse • Filename: QUOTATION.exe, Detection: malicious, Browse • Filename: PO_SBK4128332S.exe, Detection: malicious, Browse • Filename: New order - C.S.I No. 0987.exe, Detection: malicious, Browse • Filename: Bank payment swift message.exe, Detection: malicious, Browse • Filename: SOA.exe, Detection: malicious, Browse • Filename: SOA.exe, Detection: malicious, Browse • Filename: HSBC Payment Advice.exe, Detection: malicious, Browse
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...zX.Z..............0..d..........V.... ....@.. ....".....`......................................O.......8............r..`>... ....H............text...\c... ...d.................. ..`.rsrc...8............f..............@..@.reloc...............p..............@..B................8.......H........+...S.........\|...P..r...p(....*2.(....(....*z..r...p(....(....(......}....*..{....*.s.........*.0..{...........Q.-.s.....+i~....o....(.....s.......o.....r!..p..(....Q.P,:.P.....(....o....o ....(....o!...o".....,..o#...t......*..0..(....... ....s$........o%....X..(....-..*.o&...*.0...........('......&.....*.*...................0...........(.......&.....*...................0............(.....(....~....,.(....~....o....9]...

C:\Windows\System32\drivers\etc\hosts

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	835

C:\Windows\System32\drivers\etc\hosts

Entropy (8bit):	4.694294591169137
Encrypted:	false
SSDEEP:	24:QWDZh+ragzMZfuMMs1L/JU5fFCkK8T1rTt8:vDZhyoZWM9rU5fFcP
MD5:	6EB47C1CF858E25486E42440074917F2
SHA1:	6A63F93A95E1AE831C393A97158C526A4FA0FAAE
SHA-256:	9B13A3EA948A1071A81787AAC1930B89E30DF22CE13F8FF751F31B5D83E79FFB
SHA-512:	08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FA2
Malicious:	**true**
Preview:	# Copyright (c) 1993-2009 Microsoft Corp...#..# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...#..# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...#..# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...#..# For example:..#..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host....# localhost name resolution is handled within DNS itself...#.127.0.0.1 localhost..#.::1 localhost....127.0.0.1

\Device\ConDrv

Process:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1141
Entropy (8bit):	4.44831826838854
Encrypted:	false
SSDEEP:	24:zKLXkb4DObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0b4DQntKKH1MqJC
MD5:	1AEB3A784552CFD2AEDEDC1D43A97A4F
SHA1:	804286AB9F8B3DE053222826A69A7CDA3492411A
SHA-256:	0BC438F4B1208E1390C12D375B6CBB08BF47599D1F24BD07799BB1DF384AA293
SHA-512:	5305059BA86D5C2185E590EC036044B2A17ED9FD9863C2E3C7E7D8035EF0C79E53357AF5AE735F7D432BC70156D4BD3ACB42D100CFB05C2FB669EA22368F141
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [options] AssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp Expect an existing application... /tlb:<tlbfile> Filename for the exported type library... /appname:<name> Use the specified name for the target application... /parname:<name> Use the specified name or id for the target partition... /extlb Use an existing type library... /reconfig Reconfigure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo Suppress logo output... /quiet Suppress logo output and success output... /c

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.903234436272546
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% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Euro invoice.exe
File size:	508416
MD5:	15f79ec8cfa1ad6c24767d4ca45aa4cd
SHA1:	3b48453cc5680c048880bb0c4f0f19f34fdf1da7
SHA256:	49d22404c910a5bd1b6e13d92bb411b826edfc42fd680cf aa90ffb23ecc3a195
SHA512:	47a0d71ee92b6b34c98a7ce908de5495e83eec21d0899 beb267bea12e754235bbd666b5b96e074b1f8fa1457ed2 bb02b97ee8c195225825d4a3aa83b129da8
SSDEEP:	12288:AzCrhpHHt1znKv04ixBFmPJ3slZjzgtYGUPFJxN2wrRs4EKBDWkJwXQzEs1tZf4A:OCrhpHHt1znKv04i1its7stYGUtJxIsB
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...>M.a...........................2.... ....@.. ....@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x47d732
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x619F4D3E [Thu Nov 25 08:45:50 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x7b738	0x7b800	False	0.907718797444	data	7.91256606252	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x7e000	0x5b8	0x600	False	0.432291666667	data	4.34905710586	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x80000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/21-17:43:03.379334	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49840	587	192.168.2.3	148.66.138.164

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 17:43:01.202821970 CET	192.168.2.3	8.8.8.8	0x73c	Standard query (0)	mail.vrlogistic.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 17:43:01.252684116 CET	8.8.8.8	192.168.2.3	0x73c	No error (0)	mail.vrlogistic.net		148.66.138.164	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 25, 2021 17:43:01.787379980 CET	587	49840	148.66.138.164	192.168.2.3	220-sg3plcpnl0131.prod.sin3.secureserver.net ESMTP Exim 4.94.2 #2 Thu, 25 Nov 2021 09:43:01 -0700 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 25, 2021 17:43:01.787694931 CET	49840	587	192.168.2.3	148.66.138.164	EHLO 715575
Nov 25, 2021 17:43:02.043184996 CET	587	49840	148.66.138.164	192.168.2.3	250-sg3plcpnl0131.prod.sin3.secureserver.net Hello 715575 [84.17.52.63] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-CHUNKING 250-STARTTLS 250-SMTPUTF8 250 HELP
Nov 25, 2021 17:43:02.043586969 CET	49840	587	192.168.2.3	148.66.138.164	AUTH login c3VwcG9ydDI1QHZybG9naXN0aWMubmV0
Nov 25, 2021 17:43:02.299767017 CET	587	49840	148.66.138.164	192.168.2.3	334 UGFzc3dvcmQ6
Nov 25, 2021 17:43:02.565695047 CET	587	49840	148.66.138.164	192.168.2.3	235 Authentication succeeded
Nov 25, 2021 17:43:02.570029020 CET	49840	587	192.168.2.3	148.66.138.164	MAIL FROM:<support25@vrlogistic.net>
Nov 25, 2021 17:43:02.827512980 CET	587	49840	148.66.138.164	192.168.2.3	250 OK
Nov 25, 2021 17:43:02.828058004 CET	49840	587	192.168.2.3	148.66.138.164	RCPT TO:<support25@vrlogistic.net>
Nov 25, 2021 17:43:03.120738983 CET	587	49840	148.66.138.164	192.168.2.3	250 Accepted
Nov 25, 2021 17:43:03.121268988 CET	49840	587	192.168.2.3	148.66.138.164	DATA
Nov 25, 2021 17:43:03.377239943 CET	587	49840	148.66.138.164	192.168.2.3	354 Enter message, ending with "." on a line by itself
Nov 25, 2021 17:43:03.380752087 CET	49840	587	192.168.2.3	148.66.138.164	.
Nov 25, 2021 17:43:03.743999958 CET	587	49840	148.66.138.164	192.168.2.3	250 OK id=1mqHpv-003rLX-6j

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Euro invoice.exe PID: 5764 Parent PID: 5248

General

Start time:	17:41:19
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\Euro invoice.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Euro invoice.exe"
Imagebase:	0xe70000
File size:	508416 bytes
MD5 hash:	15F79EC8CFA1AD6C24767D4CA45AA4CD
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: 00000001.00000002.304280819.0000000003430000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.304085723.00000000032EA000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.304736532.00000000043F4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.304736532.00000000043F4000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: RegSvcs.exe PID: 5620 Parent PID: 5764

General

Start time:	17:41:22
Start date:	25/11/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x100000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 6692 Parent PID: 5764

General

Start time:	17:41:24
Start date:	25/11/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x3b0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 6980 Parent PID: 5764

General

Start time:	17:41:25
Start date:	25/11/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x7c0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.301908839.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.301908839.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.300860583.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.300860583.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.555012812.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000002.555012812.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.301228318.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.301228318.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.301544844.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.301544844.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.557211337.0000000002B61000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.557211337.0000000002B61000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: kprUEGC.exe PID: 7164 Parent PID: 3352

General

Start time:	17:41:56
Start date:	25/11/2021
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe"
Imagebase:	0xa10000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 6040 Parent PID: 7164

General

Start time:	17:41:57
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: kprUEGC.exe PID: 3932 Parent PID: 3352

General

Start time:	17:42:04
Start date:	25/11/2021
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe"

Imagebase:	0x8b0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Written

File Read

Analysis Process: conhost.exe PID: 5788 Parent PID: 3932

General

Start time:	17:42:05
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis