ID: 355200
Sample Name: POEA ADVISORY ON DELISTED AGENCIES.pdf.exe
Cookbook: default.jbs
Time: 08:27:44
Date: 19/02/2021
Version: 31.0.0 Emerald

Table of Contents

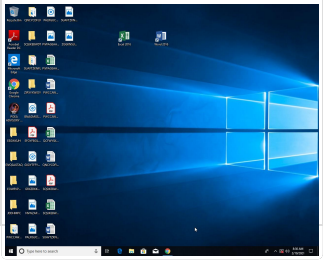
Analysis Report POEA ADVISORY ON DELISTED AGEN…

Overview

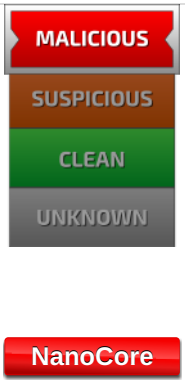
General Information

Sample Name:	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe
Analysis ID:	355200
MD5:	afcc0c7f6fadf419..
SHA1:	c1562634e7d393..
SHA256:	7dc65cb43a6491..
Tags:	exe NanoCore RAT

Most interesting Screenshot:



Detection



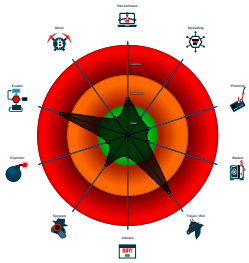
NanoCore

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Sigma detected: Suspicious Double …
- Snort IDS alert for network traffic (e….
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …
- Machine Learning detection for dropp…

Classification



Startup

- **System is w10x64**
- POEA ADVISORY ON DELISTED AGENCIES.pdf.exe (PID: 2412 cmdline: 'C:\Users\user\Desktop\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe' MD5: AFCC0C7F6FADF41949E66C9325B9F843)
  - schtasks.exe (PID: 5592 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\gVFZdFg' /XML 'C:\Users\user\AppData\Local\Temp\tmpF515.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5596 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - POEA ADVISORY ON DELISTED AGENCIES.pdf.exe (PID: 3492 cmdline: {path} MD5: AFCC0C7F6FADF41949E66C9325B9F843)
    - schtasks.exe (PID: 5580 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpA223.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 1380 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- POEA ADVISORY ON DELISTED AGENCIES.pdf.exe (PID: 5904 cmdline: 'C:\Users\user\Desktop\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe' 0 MD5: AFCC0C7F6FADF41949E66C9325B9F843)
  - schtasks.exe (PID: 5704 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\gVFZdFg' /XML 'C:\Users\user\AppData\Local\Temp\tmp5650.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5528 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - POEA ADVISORY ON DELISTED AGENCIES.pdf.exe (PID: 2592 cmdline: {path} MD5: AFCC0C7F6FADF41949E66C9325B9F843)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "c4cca249-81f6-4232-9f14-01569e09f5f0",
  "Group": "JANUARY",
  "Domain1": "shahzad73.casacam.net",
  "Domain2": "shahzad73.ddns.net",
  "Port": 9036,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4#=qs2bxKs1SDbteFYTMsjthM8IIAMC9Avo9uFWUE1JbxpU=",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000012.00000002.327116738.0000000002E0 9000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x31577:$a: NanoCore • 0x315d0:$a: NanoCore • 0x3160d:$a: NanoCore • 0x31686:$a: NanoCore • 0x315d9:$b: ClientPlugin • 0x31616:$b: ClientPlugin • 0x31f14:$b: ClientPlugin • 0x31f21:$b: ClientPlugin • 0x276fa:$e: KeepAlive • 0x31a61:$g: LogClientMessage • 0x319e1:$i: get_Connected • 0x219ad:$j: #=q • 0x219dd:$j: #=q • 0x21a19:$j: #=q • 0x21a41:$j: #=q • 0x21a71:$j: #=q • 0x21aa1:$j: #=q • 0x21ad1:$j: #=q • 0x21b01:$j: #=q • 0x21b1d:$j: #=q • 0x21b4d:$j: #=q
00000012.00000002.325925653.000000000040 2000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000012.00000002.325925653.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000012.00000002.325925653.000000000040 2000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000012.00000002.327064470.0000000002DD 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 12 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
18.2.POEA ADVISORY ON DELISTED AGENCIES. pdf.exe.2e39798.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
18.2.POEA ADVISORY ON DELISTED AGENCIES. pdf.exe.2e39798.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
18.2.POEA ADVISORY ON DELISTED AGENCIES. pdf.exe.3e20624.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0x287a1:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost • 0x287ce:$x2: IClientNetworkHost
18.2.POEA ADVISORY ON DELISTED AGENCIES. pdf.exe.3e20624.4.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x287a1:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0x2987c:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost • 0x287bb:$s5: IClientLoggingHost
18.2.POEA ADVISORY ON DELISTED AGENCIES. pdf.exe.3e20624.4.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 43 entries				

Sigma Overview

System Summary:

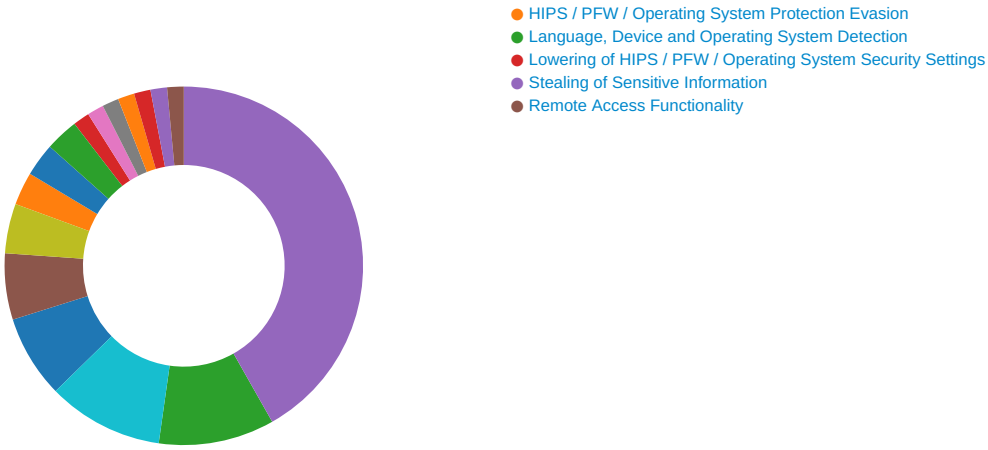
Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Sigma detected: Suspicious Double Extension

Signature Overview

- AV Detection
- Compliance
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging



Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

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)

Uses an obfuscated file name to hide its real file extension (double extension)

Stealing of Sensitive Information:

Yara detected Nanocore RAT

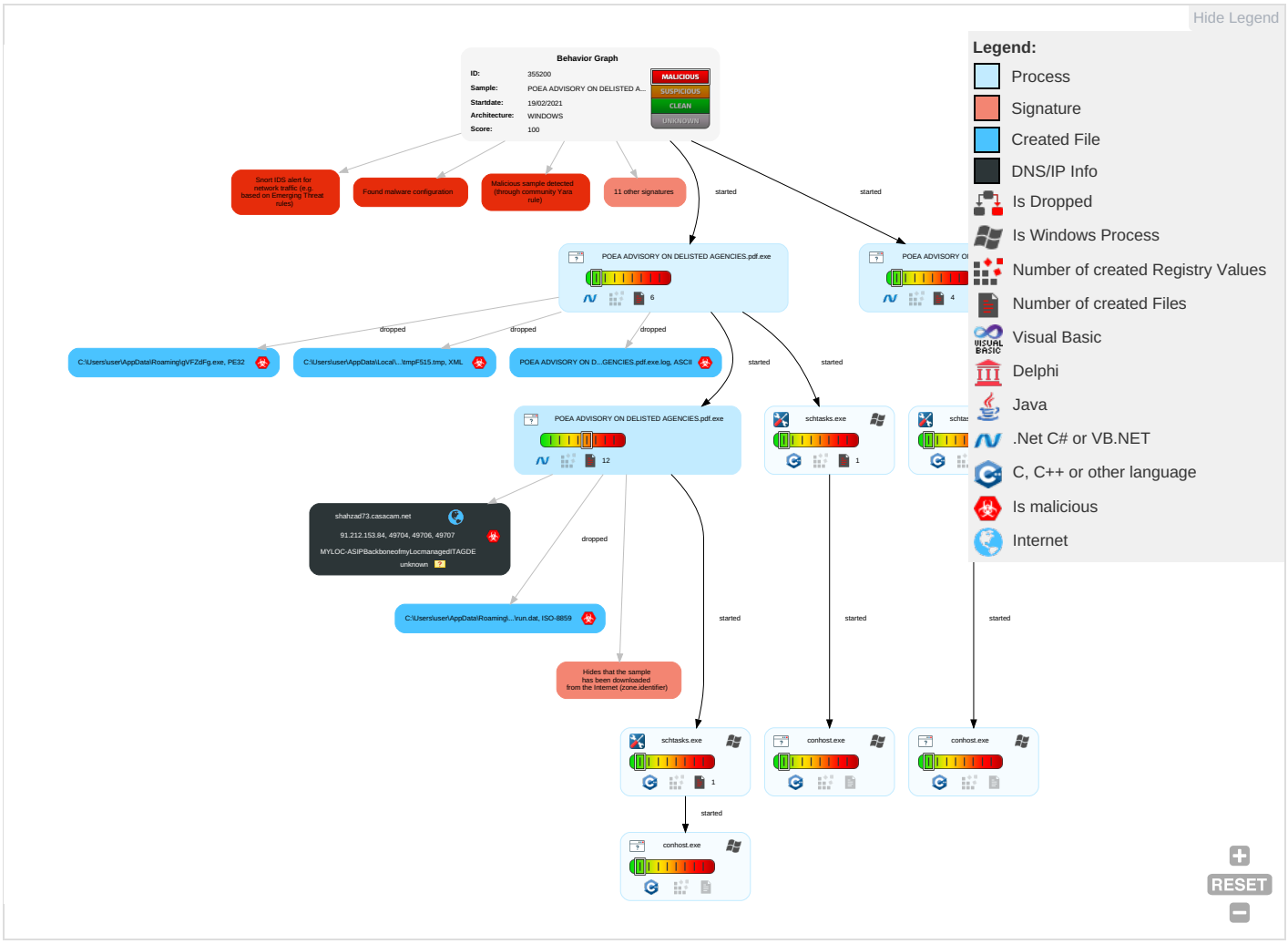
Remote Access Functionality:

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 1 1	Masquerading 1 1	OS Credential Dumping	Security Software Discovery 2 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdr Insecure Network Commur
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1	SIM Car Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commur
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial o Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access I
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure 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
POEA ADVISORY ON DELISTED AGENCIES.pdf.exe	9%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	
POEA ADVISORY ON DELISTED AGENCIES.pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\gVFZdFg.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\gVFZdFg.exe	9%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.POEA ADVISORY ON DELISTED AGENCIES.pdf.exe.48128e8.2.unpack	100%	Avira	HEUR/AGEN.1110362		Download File
18.2.POEA ADVISORY ON DELISTED AGENCIES.pdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
shahzad73.casacam.net	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
shahzad73.ddns.net	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comFB	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/5	0%	Avira URL Cloud	safe	
http://www.fontbureau.comFM	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/5	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://en.wB$	0%	Avira URL Cloud	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.com5	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
shahzad73.casacam.net	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cned	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comue	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.founder.com.cn/cnemM	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcomd	0%	URL Reputation	safe	
http://www.fontbureau.comcomd	0%	URL Reputation	safe	
http://www.fontbureau.comcomd	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/vno	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/M	0%	Avira URL Cloud	safe	
http://www.fontbureau.comueTF	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/va	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/q	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/o	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/o	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/o	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/es-e	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/i	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/i	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/i	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
shahzad73.casacam.net	91.212.153.84	true	true	• 5%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
shahzad73.ddns.net	true	• Avira URL Cloud: safe	unknown
shahzad73.casacam.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

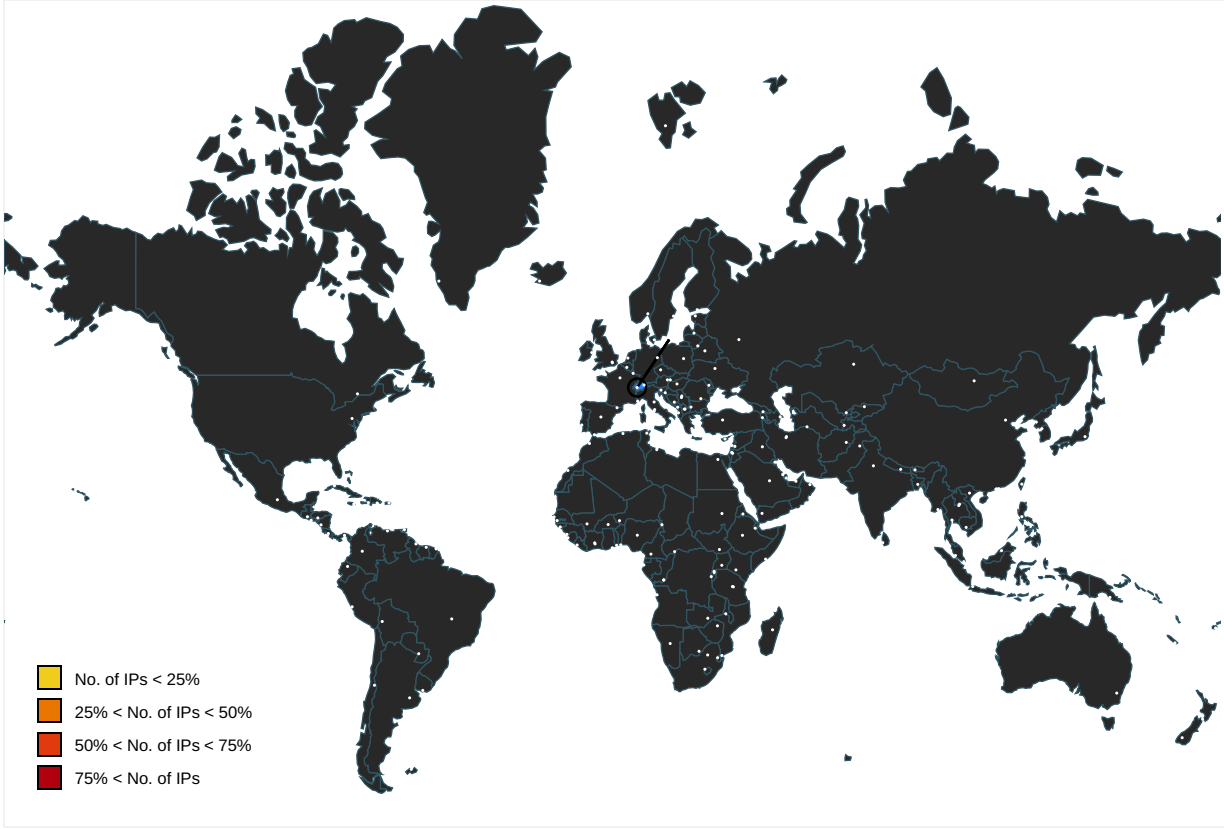
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.262105618.00000000064D0000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.262105618.00000000064D0000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.262105618.00000000064D0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.262105618.00000000064D0000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.262105618.00000000064D0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.262105618.00000000064D0000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.comFB	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.261954858.00000000063E0000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.262105618.00000000064D0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/5	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 3.207384617.00000000063E6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comFM	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 3.209218281.00000000063E6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.262105618.00000000064D0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.262105618.00000000064D0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.262105618.00000000064D0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.262105618.00000000064D0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.262105618.00000000064D0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/5	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 3.207101535.00000000063E6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.262105618.00000000064D0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 3.207384617.00000000063E6000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://en.wB$	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 3.206587822.00000000063F2000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.comgrito	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.261954858.00000000063E0000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.262105618.00000000064D0000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.262105618.00000000064D0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com5	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 3.210240222.00000000063E6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.262105618.00000000064D0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.286188722.000000000C020000.0 0000002.00000001.sdmp, POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.00000002.26210 5618.00000000064D0000.00000002 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.262105618.00000000064D0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cned	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 3.205634366.00000000063E4000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.262105618.00000000064D0000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.262105618.00000000064D0000.0 0000002.00000001.sdmp	false		high
http://www.galapagosdesign.com/	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 3.211063461.00000000063E6000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comue	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 3.210240222.00000000063E6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comF	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 3.210240222.00000000063E6000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnemM	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 3.205634366.00000000063E4000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comcomd	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 3.210240222.00000000063E6000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/vno	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 3.207101535.00000000063E6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/M	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 3.207384617.00000000063E6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comueTF	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 3.210240222.00000000063E6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 3.207384617.00000000063E6000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.coma	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.261954858.00000000063E0000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.262105618.00000000064D0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.262105618.00000000064D0000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.262105618.00000000064D0000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.262105618.00000000064D0000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/va	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 3.207384617.00000000063E6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 3.209891258.0000000006426000.0 0000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/q	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 3.207384617.00000000063E6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/o	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 3.207101535.00000000063E6000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 3.207101535.00000000063E6000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/es-e	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 3.207101535.00000000063E6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/i	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 3.207101535.00000000063E6000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 2.262105618.00000000064D0000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.comals	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 3.210240222.00000000063E6000.0 0000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/_	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe, 00000000.0000000 3.207101535.00000000063E6000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.212.153.84	unknown	unknown	?	24961	MYLOC-ASIPBackboneofmyLocmanagedITAGDE	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	355200
Start date:	19.02.2021
Start time:	08:27:44
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@15/11@17/1

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 • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 52.255.188.83, 104.43.139.144, 184.30.24.56 • Excluded domains from analysis (whitelisted): skypedataprdcoleus15.cloudapp.net, skypedataprdcoleus17.cloudapp.net, fs.microsoft.com, blobcollector.events.data.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:28:39	API Interceptor	921x Sleep call for process: POEA ADVISORY ON DELISTED AGENCIES.pdf.exe modified
08:29:00	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\POEA ADVISORY ON DELISTED AGENCIES .pdf.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
91.212.153.84	POEA ADVISORY NO 450 2021.pdf.exe	Get hash	malicious	Browse	
	POEA DELISTED AGENCIES (BATCH A).PDF.exe	Get hash	malicious	Browse	
	POEA MEMORANDUM N0 056.exe	Get hash	malicious	Browse	
	Protected.exe	Get hash	malicious	Browse	
	Protected.2.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
shahzad73.casacam.net	POEA ADVISORY NO 450 2021.pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA DELISTED AGENCIES (BATCH A).PDF.exe	Get hash	malicious	Browse	• 91.212.153.84

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	POEA MEMORANDUM N0 056.exe	Get hash	malicious	Browse	• 91.212.153.84
	Protected.exe	Get hash	malicious	Browse	• 91.212.153.84
	Protected.2.exe	Get hash	malicious	Browse	• 91.212.153.84

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MYLOC-ASIPBackboneofmyLocmanagedITAGDE	POEA ADVISORY NO 450 2021.pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA DELISTED AGENCIES (BATCH A).PDF.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA MEMORANDUM N0 056.exe	Get hash	malicious	Browse	• 91.212.153.84
	Swift_Payment_jpeg.exe	Get hash	malicious	Browse	• 62.141.37.17
	Protected.exe	Get hash	malicious	Browse	• 91.212.153.84
	Protected.2.exe	Get hash	malicious	Browse	• 91.212.153.84
	FickerStealer.exe	Get hash	malicious	Browse	• 89.163.225.172
	Documentaci#U00f3n.doc	Get hash	malicious	Browse	• 89.163.210.141
	SecuriteInfo.com.Trojan.DownLoader36.34557.26355.exe	Get hash	malicious	Browse	• 89.163.140.102
	TaskAudio Driver.exe	Get hash	malicious	Browse	• 193.111.198.220
	Z8363664.doc	Get hash	malicious	Browse	• 89.163.210.141
	OhGodAnETHlargementPill2.exe	Get hash	malicious	Browse	• 193.111.198.220
	godflex-r2.exe	Get hash	malicious	Browse	• 193.111.198.220
	PolarisBiosEditor-master.exe	Get hash	malicious	Browse	• 193.111.198.220
	NKsplucdAu.exe	Get hash	malicious	Browse	• 85.114.134.88
	lZVNh1BPxm.exe	Get hash	malicious	Browse	• 85.114.134.88
	qG5E4q8Cv5.exe	Get hash	malicious	Browse	• 85.114.134.88
	SecuriteInfo.com.BehavesLike.Win32.Generic.cc.exe	Get hash	malicious	Browse	• 85.114.134.88
	http://lecomptoirdusushi.com/commandes/menu-sushi-saumon/	Get hash	malicious	Browse	• 81.30.158.195
	klzBd4IEfv.exe	Get hash	malicious	Browse	• 85.114.134.130

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe.log	
Process:	C:\Users\user\Desktop\POEA ADVISORY ON DELISTED AGENCIES.pdf.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

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp5650.tmp	
Process:	C:\Users\user\Desktop\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1640
Entropy (8bit):	5.1929793820733705
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBrrtn:cbh47TlNQ//rydbz9I3YODOLNdq3lp
MD5:	777992096A9A67A264806BC484673046
SHA1:	B3ABDCA7929B2F4177810B5DCB140B168B9C0F88
SHA-256:	83AB2C79DD7FDD193DA964ADD86534E8EC7D0EC73485107B44DE9453D15A6974
SHA-512:	04754FFEFF30AA98F34EF3E0CDBE2B1BE5FF484365F95438350D7F2FB24CF7287F22AA85F6411F8902A84325BA0B5A64643D9C76CECD9B9C38E5DC51F454B0DC
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmpA223.tmp	
Process:	C:\Users\user\Desktop\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1328
Entropy (8bit):	5.143109702372082
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mw4mrYxtn:cbk4oL600QydbQxlYODOLedq3sxrYj
MD5:	DB01E81FC21BAD2017D4CB7505FF46F7
SHA1:	B5B5BF431C4C0E36EBA26B235FA9A7632F3CAE94
SHA-256:	442D9A3AD817160E10905025C72E9DD9810B7179ADC27884B7AFF86A1B1905C5
SHA-512:	3982F415F065F84C243A5444F5CF9D51DC715B8B5DD2781A0E048E1CBC808846CE3FA1795A282DF452BCD024A4664CBC63DDF0C0A7C5F7608E176CDEC9B91AE
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpF515.tmp	
Process:	C:\Users\user\Desktop\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1640
Entropy (8bit):	5.1929793820733705
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBrrtn:cbh47TlNQ//rydbz9I3YODOLNdq3lp
MD5:	777992096A9A67A264806BC484673046
SHA1:	B3ABDCA7929B2F4177810B5DCB140B168B9C0F88
SHA-256:	83AB2C79DD7FDD193DA964ADD86534E8EC7D0EC73485107B44DE9453D15A6974
SHA-512:	04754FFEFF30AA98F34EF3E0CDBE2B1BE5FF484365F95438350D7F2FB24CF7287F22AA85F6411F8902A84325BA0B5A64643D9C76CECD9B9C38E5DC51F454B0DC
Malicious:	**true**
Reputation:	low

C:\Users\user\AppData\Local\Temp\tmpF515.tmp

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

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat

Process:	C:\Users\user\Desktop\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	1856
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	48:IknjhUknjhUknjhUknjhUknjhUknjhUknjhL:HjhDjhDjhDjhDjhDjhDjhL
MD5:	30D23CC577A89146961915B57F408623
SHA1:	9B5709D6081D8E0A570511E6E0AAE96FA041964F
SHA-256:	E2130A72E55193D402B5F43F7F3584ECF6B423F8EC4B1B1B69AD693C7E0E5A9E
SHA-512:	2D5C5747FD04F8326C2CC1FB313925070BC01D3352AFA6C36C167B72757A15F58B6263D96BD606338DA055812E69DDB628A6E18D64DD59697C2F42D1C58CC68
Malicious:	false
Reputation:	low
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....~f.G0^..;....W2.=...K.~.L..&f...p............:7rH}..../H......L...?...A.K...J.=8x!....+.2e'..E?.G......[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....~f.G0^..;....W2.=...K.~.L..&f...p............:7rH}..../H......L...?...A.K...J.=8x!....+.2e'..E?.G......[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....~f.G0^..;....W2.=...K.~.L..&f...p............:7rH}..../H......L...?...A.K...J.=8x!....+.2e'..E?.G......[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....~f.G0^..;....W2.=...K.~.L..&f...p............:7rH}..../H......L...?...A.K...J.=8x!....+.2e'..E?.G......[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat

Process:	C:\Users\user\Desktop\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:gPn:gPn
MD5:	4E39023B090D611298C362113E4E31DE
SHA1:	511F5BCEF4D04F53C758ECA4F218A86D89955189
SHA-256:	98426645A5E77C9AF58584E1DD9B61C57E84A477F4E4C75CB58B89725A66D943
SHA-512:	3D658E57F46E31C55EF1CDDB85E4451045424677C8110A1B771B653B3CD00B95C52B9E824CCD944DD7243A2C69D1640C489BB443F6654451E97C063453B0F342
Malicious:	**true**
Reputation:	low
Preview:	...u...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak

Process:	C:\Users\user\Desktop\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	4.501629167387823
Encrypted:	false
SSDEEP:	3:9bzY6oRDIvYk:RzWDI3
MD5:	ACD3FB4310417DC77FE06F15B0E353E6
SHA1:	80E7002E655EB5765FDEB21114295CB96AD9D5EB
SHA-256:	DC3AE604991C9BB8FF8BC4502AE3D0DB8A3317512C0F432490B103B89C1A4368
SHA-512:	DA46A917DB6276CD4528CFE4AD113292D873CA2EBE53414730F442B83502E5FAF3D1AE87BFA295ADF01E3B44FDBCE239E21A318BFB2CCD1F4753846CB21F6F 97
Malicious:	false
Preview:	9iH...}Z.4..f..J".C;"a

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin

Process:	C:\Users\user\Desktop\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	64

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Entropy (8bit):	5.320159765557392
Encrypted:	false
SSDEEP:	3:9bzY6oRDIvYVsRLY6oRDT6P2bfVn1:RzWDIfRWDT621
MD5:	BB0F9B9992809E733EFFF8B0E562CFD6
SHA1:	F0BAB3CF73A04F5A689E6AFC764FEE9276992742
SHA-256:	C48F04FE7525AA3A3F9540889883F649726233DE021724823720A59B4F37CEAC
SHA-512:	AE4280AA460DC1C0301D458A3A443F6884A0BE37481737B2ADAFD72C33C55F09BED88ED239C91FE6F19CA137AC3CD7C9B8454C21D3F8E759687F701C8B3C7A6
Malicious:	false
Preview:	9iH...}Z.4..f..J".C;"a9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	327768
Entropy (8bit):	**7.999367066417797**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3PlZmqze1d1wI8lkWmtjJ/3Exi:LkjbU7LjGxi
MD5:	2E52F446105FBF828E63CF808B721F9C
SHA1:	5330E54F238F46DC04C1AC62B051DB4FCD7416FB
SHA-256:	2F7479AA2661BD259747BC89106031C11B3A3F79F12190E7F19F5DF65B7C15C8
SHA-512:	C08BA0E3315E2314ECBEF38722DF834C2CB8412446A9A310F41A8F83B4AC5984FCC1B26A1D8B0D58A730FDBDD885714854BDFD04DCDF7F582FC125F552D5C3A
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i..........J.5b7}..fK..HV.,...0.... ....n.w6PMl.....v."".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&.jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<..._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...I.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. I..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	65
Entropy (8bit):	4.801074305563008
Encrypted:	false
SSDEEP:	3:oNWXp5v1qgkFKqEqrFOXxghog2TJ:oNWXpFggKEQ4xgrOJ
MD5:	31C782D11864C78B5699327A3EABC56E
SHA1:	1970AECA390F142254BB6293D88A496593995289
SHA-256:	CA168D61590B2EBD98CEDA22CE747CF805691B00F312CFE7A9A4F77655634D0B
SHA-512:	9B7211D30F16FA10C951DEACE071734194930E1B926DB96610680F03FC33CB90491F0F207809F2D8EFF656CF9B325B7B0508C048256E216CFE69338509F2F9DA
Malicious:	false
Preview:	C:\Users\user\Desktop\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe

C:\Users\user\AppData\Roaming\gVFZdFg.exe	
Process:	C:\Users\user\Desktop\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	737280
Entropy (8bit):	7.456420940298375
Encrypted:	false
SSDEEP:	12288:2X9kXkXenHgjxJNmtOjaMohwWGVYMdyE2oApCJWX0HSx59B:CzfvaMomDVYMduXp8WX0yxV
MD5:	AFCC0C7F6FADF41949E66C9325B9F843
SHA1:	C1562634E7D393B54606731BECAD8D4D11FCBA39
SHA-256:	7DC65CB43A6491E7DA09935A8E8D20C33873FC75E370B9A701AEA0A660E85B80
SHA-512:	E80CB56E77D3A9532A6174A11ADC476CFEE7246D86AA47A9BF7A86DDFB23C8DCFE8C5CD580E998AEA4F1E8B324B55A9205091FEE89B1EFCCC37DD8E1829E22AA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 9%

C:\Users\user\AppData\Roaming\gVFZdFg.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...R]/`.....0..2.....NQ... ...`....@.. .....@.....P..O....`..T..... ..... ..H.....text...T1... ...2..... ..`.rsrc...T....`.....4.....@..@.rel oc.....>.....@..B.....0Q.....H.....$...H.....l.....0.....{.....+..*&...}....*...0.....{.....+..*&...}....*...0.....{.....+..*&...}....*...0.....{.....+..*&...}....*...0.....{.....+..*&...}....*...0.....{.....+..*&...}....*...0.....{.....+..*&...}....*...0.....{.....+..*&...}....*...0.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.456420940298375
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:	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe
File size:	737280
MD5:	afcc0c7f6fadf41949e66c9325b9f843
SHA1:	c1562634e7d393b54606731becad8d4d11fcba39
SHA256:	7dc65cb43a6491e7da09935a8e8d20c33873fc75e370b9a701aea0a660e85b80
SHA512:	e80cb56e77d3a9532a6174a11adc476cfee7246d86aa47a9bf7a86ddfb23c8dcfe8c5cd580e998aea4f1e8b324b55a9205091fee89b1efccc37dd8e1829e22aa
SSDEEP:	12288:2X9kXkXenHgjxJNmtOjaMohwWGVYMdyE2oApCJWX0HSx59B:CzfvaMomDVYMduXp8WX0yxV
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...R]/`.....0..2.....NQ... ...`....@.. .....@.....

File Icon

Icon Hash:	60c8ada8f2f0f8b1

Static PE Info

General

Entrypoint:	0x48514e
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:	0x602F5D52 [Fri Feb 19 06:40:18 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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x850fc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x86000	0x30954	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x83154	0x83200	False	0.759942504766	data	7.55881445378	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x86000	0x30954	0x30a00	False	0.759715416131	data	6.98866635189	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb8000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x861c0	0x172f0	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x9d4c0	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xadcf8	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 65535, next used block 4294901760		
RT_ICON	0xb1f30	0x25a8	data		
RT_ICON	0xb44e8	0x10a8	data		
RT_ICON	0xb55a0	0x988	data		
RT_ICON	0xb5f38	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xb63b0	0x68	data		
RT_VERSION	0xb6428	0x32c	data		
RT_MANIFEST	0xb6764	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	2017-2021
Assembly Version	4.4.2.0
InternalName	gWyum.exe
FileVersion	4.3.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	
ProductVersion	4.3.0.0
FileDescription	
OriginalFilename	gWyum.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/19/21-08:29:02.061101	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49704	9036	192.168.2.3	91.212.153.84
02/19/21-08:29:10.080046	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49706	9036	192.168.2.3	91.212.153.84
02/19/21-08:29:16.963290	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49707	9036	192.168.2.3	91.212.153.84
02/19/21-08:29:22.141016	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49708	9036	192.168.2.3	91.212.153.84
02/19/21-08:29:29.045681	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49709	9036	192.168.2.3	91.212.153.84
02/19/21-08:29:35.289931	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49710	9036	192.168.2.3	91.212.153.84
02/19/21-08:29:41.351260	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49711	9036	192.168.2.3	91.212.153.84
02/19/21-08:29:46.711502	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49712	9036	192.168.2.3	91.212.153.84
02/19/21-08:29:53.506531	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49713	9036	192.168.2.3	91.212.153.84
02/19/21-08:30:00.348934	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59349	8.8.8.8	192.168.2.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/19/21-08:30:00.409002	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49714	9036	192.168.2.3	91.212.153.84
02/19/21-08:30:06.563861	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49715	9036	192.168.2.3	91.212.153.84
02/19/21-08:30:13.530474	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49716	9036	192.168.2.3	91.212.153.84
02/19/21-08:30:20.851223	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49717	9036	192.168.2.3	91.212.153.84
02/19/21-08:30:26.882120	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49718	9036	192.168.2.3	91.212.153.84
02/19/21-08:30:33.073518	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49719	9036	192.168.2.3	91.212.153.84
02/19/21-08:30:40.144853	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49720	9036	192.168.2.3	91.212.153.84
02/19/21-08:30:45.115632	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49721	9036	192.168.2.3	91.212.153.84

Network Port Distribution

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 19, 2021 08:29:01.919277906 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:01.973613024 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:01.973773003 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.061100960 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.131288052 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.143557072 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.200113058 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.223546028 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.313024044 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.330741882 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.330770016 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.330789089 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.330801964 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.330866098 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.330903053 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.385577917 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.385646105 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.385723114 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.385737896 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.385773897 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.385821104 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.385822058 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.385863066 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.385905027 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.385941029 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.385945082 CET	9036	49704	91.212.153.84	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 19, 2021 08:29:02.385991096 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.405123949 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.440217018 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.440247059 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.440263987 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.440284967 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.440310001 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.440325975 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.440336943 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.440351009 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.440361023 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.440382004 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.440397024 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.440406084 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.440417051 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.440419912 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.440443039 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.440447092 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.440473080 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.440473080 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.440494061 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.440509081 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.440521955 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.440536022 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.440546036 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.440589905 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.440613985 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.487221003 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.496881008 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.496916056 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.496939898 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.496963024 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.496989965 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497013092 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497013092 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.497037888 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497039080 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.497061014 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497080088 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497100115 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497121096 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497147083 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497168064 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.497172117 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497196913 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.497216940 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497239113 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497263908 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497288942 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497293949 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.497309923 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497319937 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.497338057 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497363091 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.497364044 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497409105 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497438908 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497462034 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497487068 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497512102 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497535944 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.497536898 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497562885 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497570992 CET	49704	9036	192.168.2.3	91.212.153.84

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 19, 2021 08:29:02.497591972 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497592926 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.497618914 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497642994 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497667074 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497690916 CET	9036	49704	91.212.153.84	192.168.2.3
Feb 19, 2021 08:29:02.497693062 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.497736931 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.497757912 CET	49704	9036	192.168.2.3	91.212.153.84
Feb 19, 2021 08:29:02.555321932 CET	9036	49704	91.212.153.84	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 19, 2021 08:28:27.224858999 CET	54130	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:28:27.273535967 CET	53	54130	8.8.8.8	192.168.2.3
Feb 19, 2021 08:28:27.997459888 CET	56961	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:28:28.048942089 CET	53	56961	8.8.8.8	192.168.2.3
Feb 19, 2021 08:28:28.863488913 CET	59353	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:28:28.912303925 CET	53	59353	8.8.8.8	192.168.2.3
Feb 19, 2021 08:28:29.780390024 CET	52238	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:28:29.829252005 CET	53	52238	8.8.8.8	192.168.2.3
Feb 19, 2021 08:28:30.740947962 CET	49873	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:28:30.798202038 CET	53	49873	8.8.8.8	192.168.2.3
Feb 19, 2021 08:28:31.648437977 CET	53196	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:28:31.705548048 CET	53	53196	8.8.8.8	192.168.2.3
Feb 19, 2021 08:28:32.460208893 CET	56777	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:28:32.509670973 CET	53	56777	8.8.8.8	192.168.2.3
Feb 19, 2021 08:28:33.398242950 CET	58643	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:28:33.447192907 CET	53	58643	8.8.8.8	192.168.2.3
Feb 19, 2021 08:28:34.237569094 CET	60985	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:28:34.286365986 CET	53	60985	8.8.8.8	192.168.2.3
Feb 19, 2021 08:28:35.094224930 CET	50200	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:28:35.142950058 CET	53	50200	8.8.8.8	192.168.2.3
Feb 19, 2021 08:28:36.064620972 CET	51281	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:28:36.116375923 CET	53	51281	8.8.8.8	192.168.2.3
Feb 19, 2021 08:28:36.900111914 CET	49199	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:28:36.951569080 CET	53	49199	8.8.8.8	192.168.2.3
Feb 19, 2021 08:28:37.739857912 CET	50620	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:28:37.788585901 CET	53	50620	8.8.8.8	192.168.2.3
Feb 19, 2021 08:28:38.581501961 CET	64938	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:28:38.634124994 CET	53	64938	8.8.8.8	192.168.2.3
Feb 19, 2021 08:28:39.479787111 CET	60152	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:28:39.532752037 CET	53	60152	8.8.8.8	192.168.2.3
Feb 19, 2021 08:28:40.411381960 CET	57544	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:28:40.460160017 CET	53	57544	8.8.8.8	192.168.2.3
Feb 19, 2021 08:28:41.224673986 CET	55984	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:28:41.276295900 CET	53	55984	8.8.8.8	192.168.2.3
Feb 19, 2021 08:28:42.049659967 CET	64185	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:28:42.098371983 CET	53	64185	8.8.8.8	192.168.2.3
Feb 19, 2021 08:29:01.675496101 CET	65110	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:29:01.887367964 CET	53	65110	8.8.8.8	192.168.2.3
Feb 19, 2021 08:29:02.817702055 CET	58361	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:29:02.878144026 CET	53	58361	8.8.8.8	192.168.2.3
Feb 19, 2021 08:29:09.924968958 CET	63492	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:29:09.982163906 CET	53	63492	8.8.8.8	192.168.2.3
Feb 19, 2021 08:29:16.821532965 CET	60831	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:29:16.878875017 CET	53	60831	8.8.8.8	192.168.2.3
Feb 19, 2021 08:29:21.874450922 CET	60100	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:29:22.083720922 CET	53	60100	8.8.8.8	192.168.2.3
Feb 19, 2021 08:29:28.810173988 CET	53195	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:29:28.986932993 CET	53	53195	8.8.8.8	192.168.2.3
Feb 19, 2021 08:29:35.175757885 CET	50141	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:29:35.232852936 CET	53	50141	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 19, 2021 08:29:41.236505985 CET	53023	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:29:41.293612957 CET	53	53023	8.8.8.8	192.168.2.3
Feb 19, 2021 08:29:46.592783928 CET	49563	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:29:46.654160023 CET	53	49563	8.8.8.8	192.168.2.3
Feb 19, 2021 08:29:53.388196945 CET	51352	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:29:53.447899103 CET	53	51352	8.8.8.8	192.168.2.3
Feb 19, 2021 08:30:00.291894913 CET	59349	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:30:00.348933935 CET	53	59349	8.8.8.8	192.168.2.3
Feb 19, 2021 08:30:06.291666031 CET	57084	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:30:06.506647110 CET	53	57084	8.8.8.8	192.168.2.3
Feb 19, 2021 08:30:13.401871920 CET	58823	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:30:13.452063084 CET	53	58823	8.8.8.8	192.168.2.3
Feb 19, 2021 08:30:20.736202002 CET	57568	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:30:20.793597937 CET	53	57568	8.8.8.8	192.168.2.3
Feb 19, 2021 08:30:26.761276007 CET	50540	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:30:26.818576097 CET	53	50540	8.8.8.8	192.168.2.3
Feb 19, 2021 08:30:32.958008051 CET	54366	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:30:33.015305996 CET	53	54366	8.8.8.8	192.168.2.3
Feb 19, 2021 08:30:39.961554050 CET	53034	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:30:40.018662930 CET	53	53034	8.8.8.8	192.168.2.3
Feb 19, 2021 08:30:45.000926971 CET	57762	53	192.168.2.3	8.8.8.8
Feb 19, 2021 08:30:45.054364920 CET	53	57762	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 19, 2021 08:29:01.675496101 CET	192.168.2.3	8.8.8.8	0x727b	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 19, 2021 08:29:09.924968958 CET	192.168.2.3	8.8.8.8	0x190f	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 19, 2021 08:29:16.821532965 CET	192.168.2.3	8.8.8.8	0x9f6d	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 19, 2021 08:29:21.874450922 CET	192.168.2.3	8.8.8.8	0x23c4	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 19, 2021 08:29:28.810173988 CET	192.168.2.3	8.8.8.8	0x394b	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 19, 2021 08:29:35.175757885 CET	192.168.2.3	8.8.8.8	0x8e9b	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 19, 2021 08:29:41.236505985 CET	192.168.2.3	8.8.8.8	0xa15a	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 19, 2021 08:29:46.592783928 CET	192.168.2.3	8.8.8.8	0xb63b	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 19, 2021 08:29:53.388196945 CET	192.168.2.3	8.8.8.8	0x5312	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 19, 2021 08:30:00.291894913 CET	192.168.2.3	8.8.8.8	0x8a94	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 19, 2021 08:30:06.291666031 CET	192.168.2.3	8.8.8.8	0x7d5e	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 19, 2021 08:30:13.401871920 CET	192.168.2.3	8.8.8.8	0xc0d7	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 19, 2021 08:30:20.736202002 CET	192.168.2.3	8.8.8.8	0x7b91	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 19, 2021 08:30:26.761276007 CET	192.168.2.3	8.8.8.8	0x12a4	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 19, 2021 08:30:32.958008051 CET	192.168.2.3	8.8.8.8	0x8845	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 19, 2021 08:30:39.961554050 CET	192.168.2.3	8.8.8.8	0x8c6e	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 19, 2021 08:30:45.000926971 CET	192.168.2.3	8.8.8.8	0x8ae	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)

DNS Answers

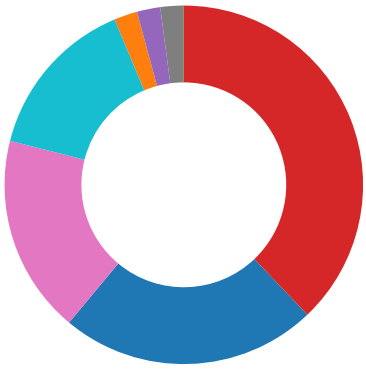
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 19, 2021 08:29:01.887367964 CET	8.8.8.8	192.168.2.3	0x727b	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 19, 2021 08:29:09.982163906 CET	8.8.8.8	192.168.2.3	0x190f	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 19, 2021 08:29:16.878875017 CET	8.8.8.8	192.168.2.3	0x9f6d	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 19, 2021 08:29:22.083720922 CET	8.8.8.8	192.168.2.3	0x23c4	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 19, 2021 08:29:28.986932993 CET	8.8.8.8	192.168.2.3	0x394b	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 19, 2021 08:29:35.232852936 CET	8.8.8.8	192.168.2.3	0x8e9b	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 19, 2021 08:29:41.293612957 CET	8.8.8.8	192.168.2.3	0xa15a	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 19, 2021 08:29:46.654160023 CET	8.8.8.8	192.168.2.3	0xb63b	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 19, 2021 08:29:53.447899103 CET	8.8.8.8	192.168.2.3	0x5312	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 19, 2021 08:30:00.348933935 CET	8.8.8.8	192.168.2.3	0x8a94	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 19, 2021 08:30:06.506647110 CET	8.8.8.8	192.168.2.3	0x7d5e	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 19, 2021 08:30:13.452063084 CET	8.8.8.8	192.168.2.3	0xc0d7	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 19, 2021 08:30:20.793597937 CET	8.8.8.8	192.168.2.3	0x7b91	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 19, 2021 08:30:26.818576097 CET	8.8.8.8	192.168.2.3	0x12a4	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 19, 2021 08:30:33.015305996 CET	8.8.8.8	192.168.2.3	0x8845	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 19, 2021 08:30:40.018662930 CET	8.8.8.8	192.168.2.3	0x8c6e	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 19, 2021 08:30:45.054364920 CET	8.8.8.8	192.168.2.3	0x8ae	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: POEA ADVISORY ON DELISTED AGENCIES.pdf.exe PID: 2412
Parent PID: 5624

General

Start time:	08:28:32
Start date:	19/02/2021
Path:	C:\Users\user\Desktop\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe'
Imagebase:	0xf70000
File size:	737280 bytes
MD5 hash:	AFCC0C7F6FADF41949E66C9325B9F843
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.255992771.0000000004429000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.255992771.0000000004429000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.255992771.0000000004429000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\gVFZdFg.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CEF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpF515.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CEF7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3BC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF515.tmp	success or wait	1	6CEF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\gVFZdFg.exe	unknown	737280	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 52 5d 2f 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 32 08 00 00 0c 03 00 00 00 00 00 4e 51 08 00 00 20 00 00 00 60 08 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 a0 0b 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...R]/`.......... ....0..2..........NQ... ...`.. ..@.. ....@................	success or wait	1	6CEF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF515.tmp	unknown	1640	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 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	6CEF1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E3BC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Users\user\Desktop\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe	unknown	737280	success or wait	1	6CEF1B4F	ReadFile

Analysis Process: schtasks.exe PID: 5592 Parent PID: 2412

General

Start time:	08:28:55
Start date:	19/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\gVFZdFg' /XML 'C:\Users\ user\AppData\Local\Temp\tmpF515.tmp'
Imagebase:	0xba0000
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\tmpF515.tmp	unknown	2	success or wait	1	BAAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpF515.tmp	unknown	1641	success or wait	1	BAABD9	ReadFile

Analysis Process: conhost.exe PID: 5596 Parent PID: 5592

General

Start time:	08:28:55
Start date:	19/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: POEA ADVISORY ON DELISTED AGENCIES.pdf.exe PID: 3492
Parent PID: 2412

General

Start time:	08:28:56
Start date:	19/02/2021
Path:	C:\Users\user\Desktop\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x7f0000
File size:	737280 bytes
MD5 hash:	AFCC0C7F6FADF41949E66C9325B9F843
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: NanoCore, Description: unknown, Source: 00000004.00000003.300424422.0000000004893000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CEFBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CEF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpA223.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CEF7038	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CEF1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CEFBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CEFBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	14	6CEF1E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CEF1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	2	6CEF1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CEFDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA223.tmp	success or wait	1	6CEF6A95	DeleteFileW
C:\Users\user\Desktop\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe:Zone.Identifier	success or wait	1	5247E96	DeleteFileA
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	success or wait	1	6CEF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	be c1 a0 75 f3 d4 d8 48	...u...H	success or wait	1	6CEF1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmpA223.tmp	unknown	1328	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 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	6CEF1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	65	43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 44 65 73 6b 74 6f 70 5c 50 4f 45 41 20 41 44 56 49 53 4f 52 59 20 4f 4e 20 44 45 4c 49 53 54 45 44 20 41 47 45 4e 43 49 45 53 2e 70 64 66 2e 65 78 65	C:\Users\user\Desktop\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe	success or wait	1	6CEF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc bb 8e f9 04 20 53 f0 bc 12 1c d2 7d 46 46 d4 32 d7 fe a4 68 e2 b4 4d 2b cf cc b9 c1 ec 4c bb 23 8c 58 cb ee 2b 8b b7 cd 01 a9 c0 2a c7 f9 1e d1 7e 66 1e 47 30 5e c3 a9 dd 96 3b b4 2e 95 a2 57 32 c2 3d 10 b3 ce 4b ca 7e c7 4c cc 9f 15 26 66 8d bb 2e 70 c8 04 1b f8 b7 c2 0f e9 ff e7 0b 10 3a 37 72 48 7d bd be f1 88 0d 2f 48 16 b2 87 06 17 96 4c 8c b6 04 3f b5 f3 04 41 08 4b 07 d1 e5 84 4a 17 3d 38 78 21 19 a1 e1 e4 2b fa 32 65 27 d7 1f 45 3f d9 47 11 9e a7 e7 a8 01 f0 5b 00 26	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i..... S.....}FF.2.. .h..M+.....L.#.X..+.....*.... ~f.G0^....;....W2.=...K.~.L... &f...p.....:7rH}...../H .....L...?...A.K....J.=8x!... .+.2e'..E?.G.....[.&	success or wait	8	6CEF1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	327768	70 54 c7 ab ad 21 b0 08 57 f6 fa 47 14 4a ba aa 61 dd a0 29 17 40 c6 8b 69 8b df 77 70 4b 98 73 6f 40 e2 06 e5 35 e7 b7 3d e9 b8 90 5e ab 1d 51 82 6f 79 f9 3d 65 40 39 c3 42 8d f7 95 46 bc cb 30 39 75 22 33 8b f5 20 30 74 c0 19 52 44 6e 5f 34 64 fb b8 17 02 df 45 c0 90 06 69 f4 08 9f ae bb 8a 7e 0c 89 85 7c 87 eb 66 58 5f 0e c2 ed 58 66 88 70 5e e2 f5 ff 94 03 e5 3e 61 db 8b 91 24 8d 8a 8f 65 05 36 3a 37 64 b6 28 61 05 41 e4 fe e0 3d be 29 2a 0d 96 a8 90 8e 7b 42 1c 5b ab 87 cb 79 25 b3 2a e4 b8 b1 9f 69 a7 51 84 3c f3 94 a2 90 78 74 c4 a9 58 13 11 48 09 d7 20 ad cc a4 48 46 37 67 0f e0 c5 49 96 2a 33 03 7b 0c 6e 92 bf 90 be 4c d1 9b 79 3b 69 87 bc 73 2d 1e b6 f9 b8 28 35 69 c2 8b 92 d6 10 ac a7 02 93 ee 89 08 17 4a 09 35 62 37 7d fe 86 66 4b af ab 48 56	pT...!..W..G.J..a..).@..i..wp K .so@...5..=...^..Q.oy.=e@9 .B...F..09u"3.. 0t..RDn_4d.....E.. .i.....~...|..fX_...Xf.p^.... ..>a...$...e.6:7d.(a.A...=.)*. ....{B.[...y%.*....i.Q.<....xt ..X..H.. ...HF7g...I.*3.{.n... .L..y;i..s-....(5i..... .J.5b7}..fK..HV	success or wait	1	6CEF1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	24	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d f0 4a 22 83 43 3b 22 61	9iH....}Z..4..f..J".C;"a	success or wait	2	6CEF1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	0	24	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d f0 4a 22 83 43 3b 22 61	9iH....}Z..4..f..J".C;"a	success or wait	1	6CEFDD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Users\user\Desktop\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe	unknown	4096	success or wait	1	6E06D72F	unknown
C:\Users\user\Desktop\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe	unknown	512	success or wait	1	6E06D72F	unknown

Analysis Process: schtasks.exe PID: 5580 Parent PID: 3492

General

Start time:	08:28:59
Start date:	19/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpA223.tmp'
Imagebase:	0xf00000
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\tmpA223.tmp	unknown	2	success or wait	1	F0AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA223.tmp	unknown	1329	success or wait	1	F0ABD9	ReadFile

Analysis Process: conhost.exe PID: 1380 Parent PID: 5580

General

Start time:	08:28:59
Start date:	19/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: POEA ADVISORY ON DELISTED AGENCIES.pdf.exe PID: 5904
Parent PID: 528

General

Start time:	08:29:00
Start date:	19/02/2021
Path:	C:\Users\user\Desktop\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe' 0
Imagebase:	0x7ff7ca4e0000
File size:	737280 bytes
MD5 hash:	AFCC0C7F6FADF41949E66C9325B9F843
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.311283460.00000000042D9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.311283460.00000000042D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.311283460.00000000042D9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.311591988.0000000004376000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.311591988.0000000004376000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.311591988.0000000004376000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	unknown
C:\Users\user\AppData\Local\Temp\tmp5650.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CEF7038	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp5650.tmp	success or wait	1	6CEF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp5650.tmp	unknown	1640	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 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	6CEF1B4F	WriteFile

File Read

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

Analysis Process: schtasks.exe PID: 5704 Parent PID: 5904

General

Start time:	08:29:20
Start date:	19/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\gVFZdFg' /XML 'C:\Users\user\AppData\Local\Temp\tmp5650.tmp'
Imagebase:	0x8f0000
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\tmp5650.tmp	unknown	2	success or wait	1	8FAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp5650.tmp	unknown	1641	success or wait	1	8FABD9	ReadFile

Analysis Process: conhost.exe PID: 5528 Parent PID: 5704

General

Start time:	08:29:20
Start date:	19/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: POEA ADVISORY ON DELISTED AGENCIES.pdf.exe PID: 2592 Parent PID: 5904

General

Start time:	08:29:21
Start date:	19/02/2021
Path:	C:\Users\user\Desktop\POEA ADVISORY ON DELISTED AGENCIES.pdf.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x8d0000
File size:	737280 bytes
MD5 hash:	AFCC0C7F6FADF41949E66C9325B9F843
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: NanoCore, Description: unknown, Source: 00000012.00000002.327116738.0000000002E09000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.325925653.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.325925653.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.325925653.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.327064470.0000000002DD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.327179644.0000000003DD9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.327179644.0000000003DD9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	unknown

File Read

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

Disassembly

Code Analysis