ID: 383708
Sample Name: LIST OF POEA DELISTED AGENCIES.pdf.exe
Cookbook: default.jbs
Time: 07:47:17
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

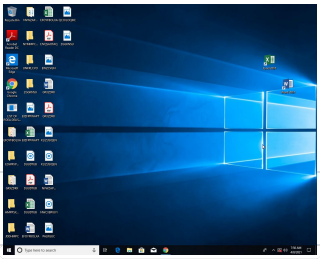
Analysis Report LIST OF POEA DELISTED AGENCIES.p…

Overview

General Information

Sample Name:	LIST OF POEA DELISTED AGENCIES.pdf.exe
Analysis ID:	383708
MD5:	170934b168c75e..
SHA1:	9089f509aae0899.
SHA256:	1b7d2ae0faed1db.
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

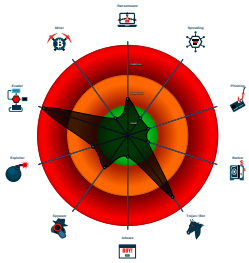
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains method …
- .NET source code contains potentia…
- .NET source code references suspic…

Classification



Startup

- **System is w10x64**
- LIST OF POEA DELISTED AGENCIES.pdf.exe (PID: 204 cmdline: 'C:\Users\user\Desktop\LIST OF POEA DELISTED AGENCIES.pdf.exe' MD5: 170934B168C75ED396332A6AF365A478)
  - schtasks.exe (PID: 804 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\IYcqUUrbhRC' /XML 'C:\Users\user\AppData\Local\Temp\tmp1EF7.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5904 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - LIST OF POEA DELISTED AGENCIES.pdf.exe (PID: 5592 cmdline: {path} MD5: 170934B168C75ED396332A6AF365A478)
    - schtasks.exe (PID: 6240 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpB457.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6248 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- LIST OF POEA DELISTED AGENCIES.pdf.exe (PID: 6380 cmdline: 'C:\Users\user\Desktop\LIST OF POEA DELISTED AGENCIES.pdf.exe' 0 MD5: 170934B168C75ED396332A6AF365A478)
  - schtasks.exe (PID: 6672 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\IYcqUUrbhRC' /XML 'C:\Users\user\AppData\Local\Temp\tmp5375.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6756 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - LIST OF POEA DELISTED AGENCIES.pdf.exe (PID: 6836 cmdline: {path} MD5: 170934B168C75ED396332A6AF365A478)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "a8eeb35c-017d-4116-8f99-efe29258",
  "Group": "uuu",
  "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",
  "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
00000007.00000002.504910894.000000000534 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000007.00000002.504910894.000000000534 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
00000013.00000002.309866896.000000000442 9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000013.00000002.309866896.000000000442 9000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x435b5:$a: NanoCore • 0x4360e:$a: NanoCore • 0x4364b:$a: NanoCore • 0x436c4:$a: NanoCore • 0x56d6f:$a: NanoCore • 0x56d84:$a: NanoCore • 0x56db9:$a: NanoCore • 0x6fd5b:$a: NanoCore • 0x6fd70:$a: NanoCore • 0x6fda5:$a: NanoCore • 0x43617:$b: ClientPlugin • 0x43654:$b: ClientPlugin • 0x43f52:$b: ClientPlugin • 0x43f5f:$b: ClientPlugin • 0x56b2b:$b: ClientPlugin • 0x56b46:$b: ClientPlugin • 0x56b76:$b: ClientPlugin • 0x56d8d:$b: ClientPlugin • 0x56dc2:$b: ClientPlugin • 0x6fb17:$b: ClientPlugin • 0x6fb32:$b: ClientPlugin
00000007.00000002.505287922.000000000578 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
Click to see the 57 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.LIST OF POEA DELISTED AGENCIES.pdf.exe.5780000.22.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
7.2.LIST OF POEA DELISTED AGENCIES.pdf.exe.5780000.22.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
7.2.LIST OF POEA DELISTED AGENCIES.pdf.exe.5780000.22.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
7.2.LIST OF POEA DELISTED AGENCIES.pdf.exe.2eb60d8.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2dbb:$x1: NanoCore.ClientPluginHost • 0x2de5:$x2: IClientNetworkHost
7.2.LIST OF POEA DELISTED AGENCIES.pdf.exe.2eb60d8.3.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2dbb:$x2: NanoCore.ClientPluginHost • 0x4c6b:$s4: PipeCreated
Click to see the 157 entries				

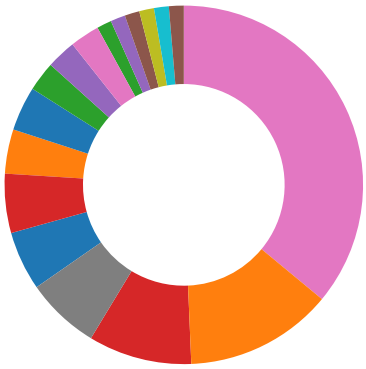
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- 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
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Yara detected Nanocore RAT

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 method to dynamically call methods (often used by packers)

.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)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

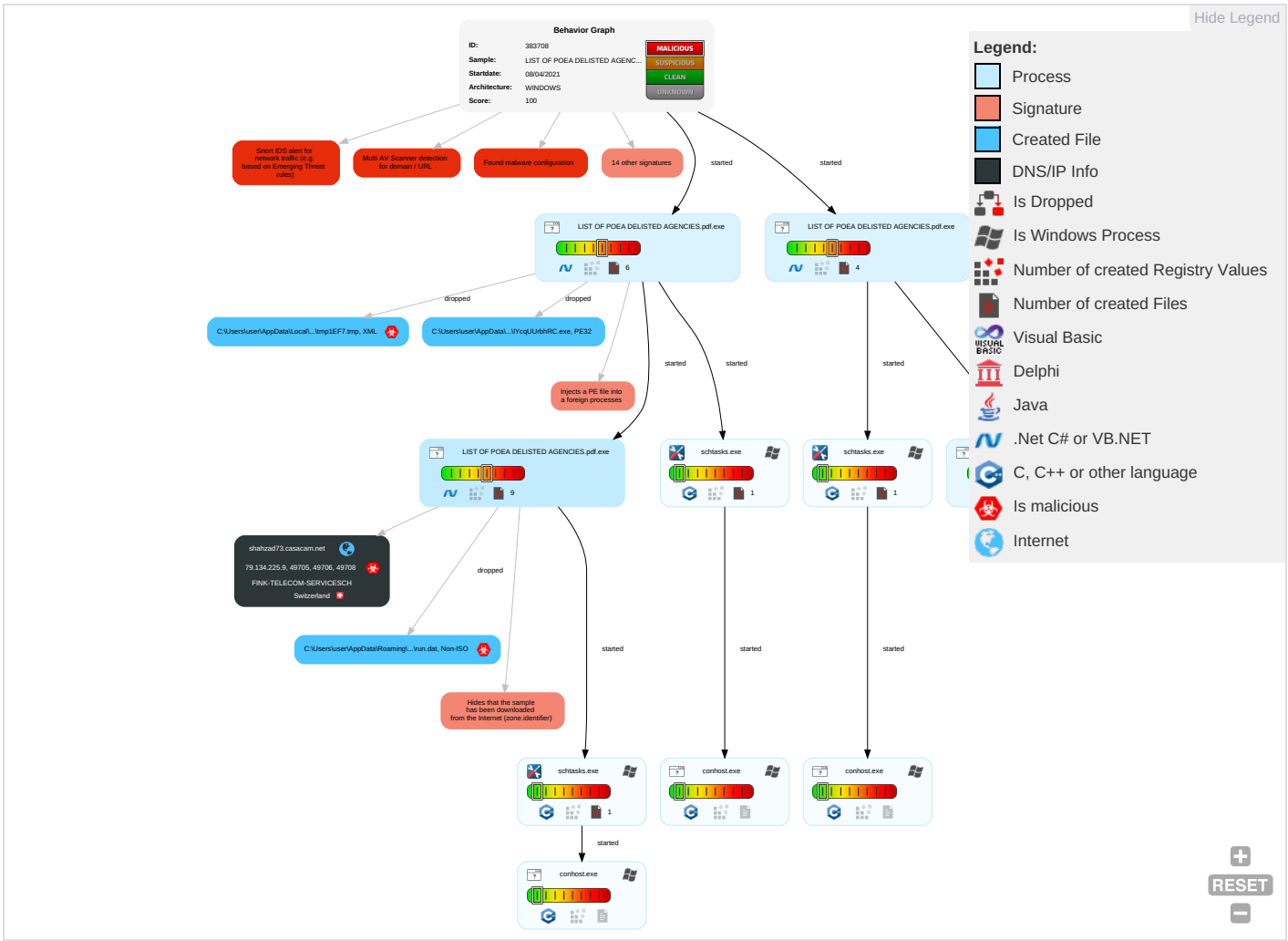
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1 1	Input Capture 1 1	Security Software Discovery 1 1 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM C Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
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	Application Layer Protocol 1 1	Manip Device Comm
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	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc

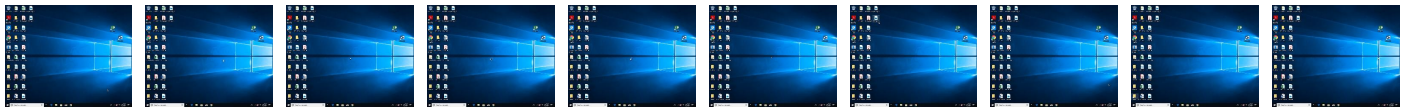
Behavior Graph

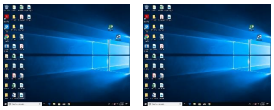


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.LIST OF POEA DELISTED AGENCIES.pdf.exe.5780000.22.unpack	100%	Avira	TR/NanoCore.fadte		Download File
19.2.LIST OF POEA DELISTED AGENCIES.pdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.2.LIST OF POEA DELISTED AGENCIES.pdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
shahzad73.casacam.net	6%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
shahzad73.ddns.net	6%	Virustotal		Browse
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.fontbureau.comueva	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	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.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.carterandcone.coml	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.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.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.founder.com.cn/cn	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/	0%	URL Reputation	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.galapagosdesign.com/DPlease	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.sandoll.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comrY.	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
shahzad73.casacam.net	79.134.225.9	true	true	• 6%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
shahzad73.ddns.net	true	• 6%, Virustotal, Browse • Avira URL Cloud: safe	unknown
shahzad73.casacam.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

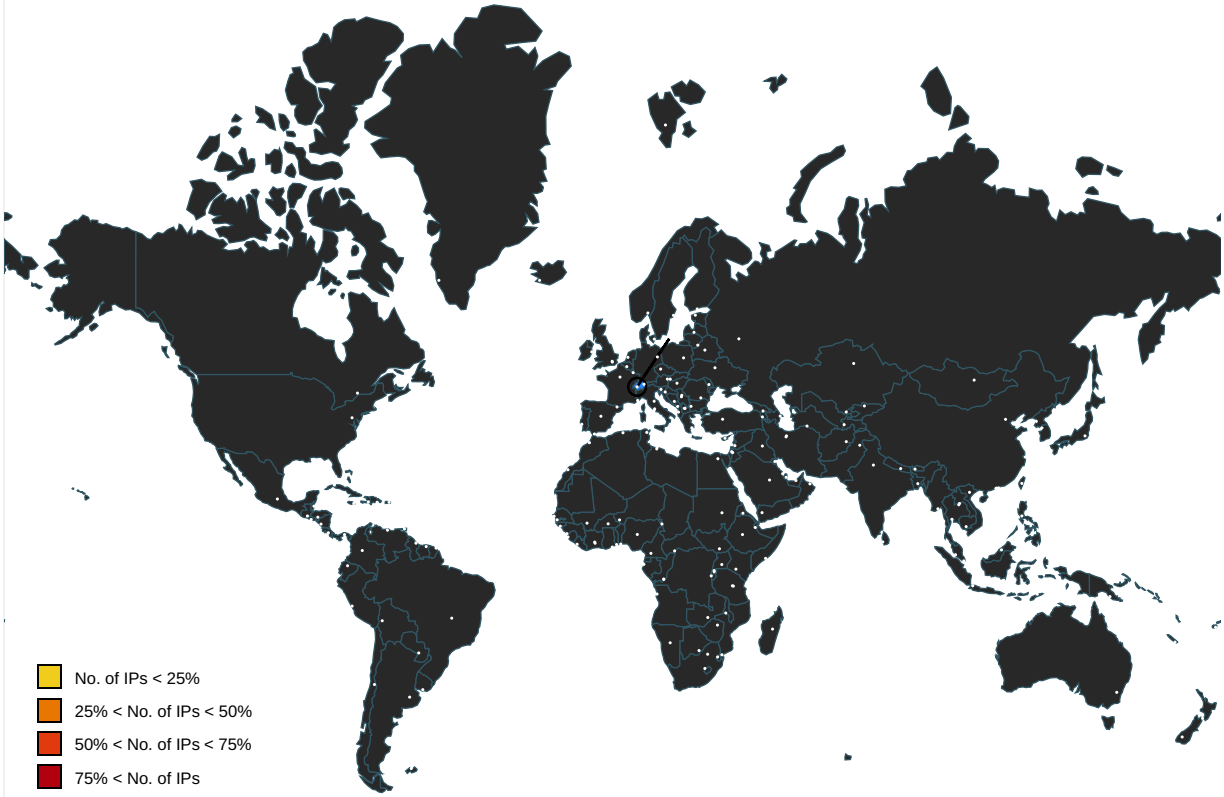
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.26 6816780.00000000068B2000.00000 004.00000001.sdmp, LIST OF POEA DELISTED AGENCIES.pdf.exe, 0 000000B.00000002.299600592.000 0000005790000.00000002.0000000 1.sdmp	false		high
http://www.fontbureau.com	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.26 6816780.00000000068B2000.00000 004.00000001.sdmp, LIST OF POEA DELISTED AGENCIES.pdf.exe, 0 000000B.00000002.299600592.000 0000005790000.00000002.0000000 1.sdmp	false		high
http://www.fontbureau.com/designersG	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.26 6816780.00000000068B2000.00000 004.00000001.sdmp, LIST OF POEA DELISTED AGENCIES.pdf.exe, 0 000000B.00000002.299600592.000 0000005790000.00000002.0000000 1.sdmp	false		high
http://www.fontbureau.com/designers/?	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.26 6816780.00000000068B2000.00000 004.00000001.sdmp, LIST OF POEA DELISTED AGENCIES.pdf.exe, 0 000000B.00000002.299600592.000 0000005790000.00000002.0000000 1.sdmp	false		high
http://www.founder.com.cn/cn/bThe	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.26 6816780.00000000068B2000.00000 004.00000001.sdmp, LIST OF POEA DELISTED AGENCIES.pdf.exe, 0 000000B.00000002.299600592.000 0000005790000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comueva	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.25 8728477.0000000000A17000.00000 004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/michel-pi/EasyBot.Net	LIST OF POEA DELISTED AGENCIES .pdf.exe	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.26 6816780.00000000068B2000.00000 004.00000001.sdmp, LIST OF POEA DELISTED AGENCIES.pdf.exe, 0 000000B.00000002.299600592.000 0000005790000.00000002.0000000 1.sdmp	false		high
http://www.tiro.com	LIST OF POEA DELISTED AGENCIES .pdf.exe, 0000000B.00000002.29 9600592.0000000005790000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	LIST OF POEA DELISTED AGENCIES .pdf.exe, 0000000B.00000002.29 9600592.0000000005790000.00000 002.00000001.sdmp	false		high
http://www.goodfont.co.kr	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.26 6816780.00000000068B2000.00000 004.00000001.sdmp, LIST OF POEA DELISTED AGENCIES.pdf.exe, 0 000000B.00000002.299600592.000 0000005790000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.coma	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.25 8728477.0000000000A17000.00000 004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.26 6816780.00000000068B2000.00000 004.00000001.sdmp, LIST OF POEA DELISTED AGENCIES.pdf.exe, 0 000000B.00000002.299600592.000 0000005790000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.26 6816780.00000000068B2000.00000 004.00000001.sdmp, LIST OF POEA DELISTED AGENCIES.pdf.exe, 0 000000B.00000002.299600592.000 0000005790000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.26 6816780.00000000068B2000.00000 004.00000001.sdmp, LIST OF POEA DELISTED AGENCIES.pdf.exe, 0 000000B.00000002.299600592.000 0000005790000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.26 6816780.00000000068B2000.00000 004.00000001.sdmp, LIST OF POEA DELISTED AGENCIES.pdf.exe, 0 000000B.00000002.299600592.000 0000005790000.00000002.0000000 1.sdmp	false		high
http://www.founder.com.cn/cn/cThe	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.26 6816780.00000000068B2000.00000 004.00000001.sdmp, LIST OF POEA DELISTED AGENCIES.pdf.exe, 0 000000B.00000002.299600592.000 0000005790000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.26 6816780.00000000068B2000.00000 004.00000001.sdmp, LIST OF POEA DELISTED AGENCIES.pdf.exe, 0 000000B.00000002.299600592.000 0000005790000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.26 6816780.00000000068B2000.00000 004.00000001.sdmp, LIST OF POEA DELISTED AGENCIES.pdf.exe, 0 000000B.00000002.299600592.000 0000005790000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.26 6816780.00000000068B2000.00000 004.00000001.sdmp, LIST OF POEA DELISTED AGENCIES.pdf.exe, 0 000000B.00000002.299600592.000 0000005790000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.26 6816780.00000000068B2000.00000 004.00000001.sdmp, LIST OF POEA DELISTED AGENCIES.pdf.exe, 0 000000B.00000002.299600592.000 0000005790000.00000002.0000000 1.sdmp	false		high
http://www.jiyu-kobo.co.jp/	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.26 6816780.00000000068B2000.00000 004.00000001.sdmp, LIST OF POEA DELISTED AGENCIES.pdf.exe, 0 000000B.00000002.299600592.000 0000005790000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.26 6816780.00000000068B2000.00000 004.00000001.sdmp, LIST OF POEA DELISTED AGENCIES.pdf.exe, 0 000000B.00000002.299600592.000 0000005790000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.26 6816780.00000000068B2000.00000 004.00000001.sdmp, LIST OF POEA DELISTED AGENCIES.pdf.exe, 0 000000B.00000002.299600592.000 0000005790000.00000002.0000000 1.sdmp	false		high
http://www.fonts.com	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.26 6816780.00000000068B2000.00000 004.00000001.sdmp, LIST OF POEA DELISTED AGENCIES.pdf.exe, 0 000000B.00000002.299600592.000 0000005790000.00000002.0000000 1.sdmp	false		high
http://www.sandoll.co.kr	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.26 6816780.00000000068B2000.00000 004.00000001.sdmp, LIST OF POEA DELISTED AGENCIES.pdf.exe, 0 000000B.00000002.299600592.000 0000005790000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comrY.	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.25 8728477.0000000000A17000.00000 004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.26 6816780.00000000068B2000.00000 004.00000001.sdmp, LIST OF POEA DELISTED AGENCIES.pdf.exe, 0 000000B.00000002.299600592.000 0000005790000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.26 6816780.00000000068B2000.00000 004.00000001.sdmp, LIST OF POEA DELISTED AGENCIES.pdf.exe, 0 000000B.00000002.299600592.000 0000005790000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.27 0340865.0000000007421000.00000 004.00000001.sdmp, LIST OF POEA DELISTED AGENCIES.pdf.exe, 0 000000B.00000002.300872246.000 0000006FD1000.00000004.0000000 1.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	LIST OF POEA DELISTED AGENCIES .pdf.exe, 00000000.00000002.26 6816780.00000000068B2000.00000 004.00000001.sdmp, LIST OF POEA DELISTED AGENCIES.pdf.exe, 0 000000B.00000002.299600592.000 0000005790000.00000002.0000000 1.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.9	shahzad73.casacam.net	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383708
Start date:	08.04.2021
Start time:	07:47:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	LIST OF POEA 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:	33
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@15/8@15/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0% (good quality ratio 0%) • Quality average: 51% • Quality standard deviation: 0%
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, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 23.54.113.53, 52.147.198.201, 40.88.32.150, 95.100.54.203, 13.88.21.125, 20.82.210.154, 23.10.249.26, 23.10.249.43, 23.0.174.185, 23.0.174.200, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description

Time	Type	Description
07:48:17	API Interceptor	941x Sleep call for process: LIST OF POEA DELISTED AGENCIES.pdf.exe modified
07:48:26	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\LIST OF POEA DELISTED AGENCIES.pdf.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.9	Gi#U00e1 FOB t#U00ednh b#U1eb1ng USD..KQ13jvZ9uFZOE8U.exe	Get hash	malicious	Browse	
	#U4ed8#U6b3e#U51ed#U8bc104R927.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.InjectNET.14.25726.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Hosts.48193.7834.exe	Get hash	malicious	Browse	
	MT-10634xls.exe	Get hash	malicious	Browse	
	Scan_202011200113(1)xls.exe	Get hash	malicious	Browse	
	NEW ORDER_8876630.exe	Get hash	malicious	Browse	
	yrIVz5su2U.exe	Get hash	malicious	Browse	
	DHL 2723382830#U6536#U636e,pdf.exe	Get hash	malicious	Browse	
	Huidmwk.exe	Get hash	malicious	Browse	
	Huidmwk.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
shahzad73.casacam.net	Memo-Circular No 018-21.pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA MEMO.pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	RWO-NCR Advisory.pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA MEMO.pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	Memo-Circular No 018-21 MARINA ADVISORY NO 2021-05 .pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	Ircg423Akc.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA MEMORANDUM.PDF.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA Advisory No. 109, 2021 on COVID-19.pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	remittance copy.pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	xbfR1CDx7S.exe	Get hash	malicious	Browse	• 91.212.153.84
	swift_BILLING INVOICE.doc	Get hash	malicious	Browse	• 91.212.153.84
	Bank Transfer Slip.exe	Get hash	malicious	Browse	• 91.212.153.84
	BILLING INVOICE.pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	JMG Memo-Circular No 018-21.PDF.exe	Get hash	malicious	Browse	• 91.212.153.84
	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA ADVISORY ON DELISTED AGENCIES.PDF.exe	Get hash	malicious	Browse	• 91.212.153.84
	Swift copy_BILLING INVOICE.pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	AWB.pdf.exe	Get hash	malicious	Browse	• 79.134.225.102
	AIC7VMxudf.exe	Get hash	malicious	Browse	• 79.134.225.30
	9mm case for ROYAL METAL INDUSTRIES 3milmonth Specification drawings.exe	Get hash	malicious	Browse	• 79.134.225.21
	PO50164.exe	Get hash	malicious	Browse	• 79.134.225.79
	Fast color scan to a PDFfile_1_20210331084231346.pdf.exe	Get hash	malicious	Browse	• 79.134.225.102
	n7dIHuG3v6.exe	Get hash	malicious	Browse	• 79.134.225.92
	F6JT4fXIAQ.exe	Get hash	malicious	Browse	• 79.134.225.92
	order_inquiry2094.xls.exe	Get hash	malicious	Browse	• 79.134.225.102
	5H957qLghX.exe	Get hash	malicious	Browse	• 79.134.225.25
	yBio5dWAOI.exe	Get hash	malicious	Browse	• 79.134.225.7

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	wDIaJji4Vv.exe	Get hash	malicious	Browse	• 79.134.225.7
	DkZY1k3y9F.exe	Get hash	malicious	Browse	• 79.134.225.23
	hbvo9thTAX.exe	Get hash	malicious	Browse	• 79.134.225.7
	SCAN ORDER DOC 040202021.exe	Get hash	malicious	Browse	• 79.134.225.71
	Waybill Doc_pdf.exe	Get hash	malicious	Browse	• 79.134.225.92
	gfcYixSdyD.exe	Get hash	malicious	Browse	• 79.134.225.71
	cJtVGjtNGZ.exe	Get hash	malicious	Browse	• 79.134.225.40
	Transferwise beneficiary detailspdf.exe	Get hash	malicious	Browse	• 79.134.225.22
	NS 001 DOP IPS ORIENTATIONS.doc	Get hash	malicious	Browse	• 79.134.225.73
	cp.msi.exe	Get hash	malicious	Browse	• 79.134.225.109

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\LIST OF POEA DELISTED AGENCIES.pdf.exe.log

Process:	C:\Users\user\Desktop\LIST OF POEA 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:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp1EF7.tmp

Process:	C:\Users\user\Desktop\LIST OF POEA DELISTED AGENCIES.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1648
Entropy (8bit):	5.176749207765345
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBhztn:cbhC7ZlNQF/rydbz9l3YODOLNdq3t
MD5:	21FDD8808218A108E28FCFAB999B711D
SHA1:	8724F1BFA27D5A87431CD380A4E7B92F14745E3A
SHA-256:	87A449C920E2FB74E680B6355F499A8EE116B62F7E841B49BBC48E5BEB9F6105
SHA-512:	DBF4EAFDC5941288BB8091D1665F8140B314D0DDBD6D23E6FB68DF54145CA7EF6585FA1EBA7B9B0CF0258DEF950CD3773A2A120DB306D7DDEABA22060C00348
Malicious:	**true**
Reputation:	low

C:\Users\user\AppData\Local\Temp\tmp1EF7.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>t

C:\Users\user\AppData\Local\Temp\tmp5375.tmp	
Process:	C:\Users\user\Desktop\LIST OF POEA DELISTED AGENCIES.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1648
Entropy (8bit):	5.176749207765345
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBhztn:cbhC7ZlNQF/rydbz9I3YODOLNdq3t
MD5:	21FDD8808218A108E28FCFAB999B711D
SHA1:	8724F1BFA27D5A87431CD380A4E7B92F14745E3A
SHA-256:	87A449C920E2FB74E680B6355F499A8EE116B62F7E841B49BBC48E5BEB9F6105
SHA-512:	DBF4EAFDC5941288BB8091D1665F8140B314D0DDBD6D23E6FB68DF54145CA7EF6585FA1EBA7B9B0CF0258DEF950CD3773A2A120DB306D7DDEABA22060C00348
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>t

C:\Users\user\AppData\Local\Temp\tmpB457.tmp	
Process:	C:\Users\user\Desktop\LIST OF POEA DELISTED AGENCIES.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1325
Entropy (8bit):	5.123968322135509
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0ParYxtn:cbk4oL600QydbQxlYODOLedq3SarYj
MD5:	06778E138CFA3F83DB1A10CF4BC36E1C
SHA1:	95880E16C188DFC0601A97E0C9AA9F5F26AA1628
SHA-256:	94CDD87F5330C4C0B7BB6AF3421FD6DE4F009E9F7EEC1EBB3CE74BF30B396CF2
SHA-512:	AB0C359D0E5810AE38D945C8CD488CFCC6FB44ADF1EA8BA5ADFCE6D58693CAB1269ECD197B74CD64247D6C56D925CA051D51E414F87984174F0481F65F69E4B
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\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\LIST OF POEA DELISTED AGENCIES.pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	2784
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	48:IknjhUknjhUknjhUknjhUknjhUknjhUknjhUknjhUknjhUknjhL:HjhDjhDjhDjhDjhDjhDjhDjhDjhDz
MD5:	1D36D3F312F677BFA382C9041352BCDB
SHA1:	760113B8969928B0A7F217EDF96D2F5D7613BF43
SHA-256:	789F505ECA8494C06422B61C4D696512284A0E8F3DA573ED97DBDF3721E2370D
SHA-512:	8736F403BCC40A7C907C28026104B05DA0255EB5B53EF0CF3FAA81DF60927A15CCC5A5E0FE442EB06CE2F1CB6811587339341889DBC8470622FAD7672C7D012
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
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\LIST OF POEA DELISTED AGENCIES.pdf.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:6n:6
MD5:	4BBA759E38EC777A16944C8F97C85C31
SHA1:	1F07F5C461F63EB4F8D0E170115973BD8F2370DD
SHA-256:	09205B6721CE7555EDE9C20FA1BDC52625D90900A1C0D4A41E329AC8FC4F1D2E
SHA-512:	D50DC62E93CAF550171EED2C3C75E7571229644108B648675027FA139DABFE3E0C1B58AF6584620E6F889D64F74A4E69ACC876D89913698430A9457457A6F74E
Malicious:	**true**
Reputation:	low
Preview:	.=i\...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\LIST OF POEA DELISTED AGENCIES.pdf.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	62
Entropy (8bit):	4.73041723004934
Encrypted:	false
SSDEEP:	3:oNUWJRWpsp+g9ghog2TJ:oNNJACwg9grOJ
MD5:	9AE7E0FF2AF6D9EB4CE4796CEC5B4818
SHA1:	F28D47C4F13A78B75078275459021506B42EE14F
SHA-256:	44FF48647A1E176BF1ED2ADF9FAA479C082D878431FB917B44EE84A8E0D2A4AA
SHA-512:	629E099713D43EAFE5E64590E1CD0168658FF458F07230B11A159DD2265D4149A6A800B7D80AB619DBFA1C2FBB7DDADFB9BA84120AD1560E32360EC5D049955
Malicious:	false
Reputation:	low
Preview:	C:\Users\user\Desktop\LIST OF POEA DELISTED AGENCIES.pdf.exe

C:\Users\user\AppData\Roaming\lYcqUUrbhRC.exe	
Process:	C:\Users\user\Desktop\LIST OF POEA DELISTED AGENCIES.pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	756736
Entropy (8bit):	7.894509991682861
Encrypted:	false
SSDEEP:	12288:Yf0Plu2iNSbc3TKa00gTBz4CJOqW2WZrpyszp3AKlOALeCmxaMdGkq0yTOI:hdu1xTKacuCIqW2WNpyszpQKlreCmzGr
MD5:	170934B168C75ED396332A6AF365A478
SHA1:	9089F509AAE08997E6C8DA1A33F3C5156A6F06BC
SHA-256:	1B7D2AE0FAED1DB793CFCF75E11CC0308C69AF37540D27B9DBD104D0F850A658
SHA-512:	938C117C81509373F841970EA06AFF42A3E9C455712AD8DD27851D0580C1C9D08AD16A00DA4E334CA10F9A58867A00530B5027E39F0D99D907F00C79AB8E97BD
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....n`.....0..... .....@.. ..... ..@.....`...O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....d.....hZ...F.....^..}.....(.....(.....*..*..0..+.....,.{.....+...,...{....o.....(....*..0.....(....s.....s...}.....s...}.....s...}.....s...}.....s ...}.....s!...}.....s"...}.....{....o#.....{....o$.....(#.....{.....o%.....{....o&....".Bs'...o(...&.{....o&....".Bs'...o(...&.{....o)....{.....o*.....{....o)....{.....o*.....{....o)....{.....o*.....{....o)....{.....o*.....{....o

Static File Info

General

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.894509991682861
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	LIST OF POEA DELISTED AGENCIES.pdf.exe
File size:	756736
MD5:	170934b168c75ed396332a6af365a478
SHA1:	9089f509aae08997e6c8da1a33f3c5156a6f06bc
SHA256:	1b7d2ae0faed1db793cfcf75e11cc0308c69af37540d27b9dbd104d0f850a658
SHA512:	938c117c81509373f841970ea06aff42a3e9c455712ad8dd27851d0580c1c9d08ad16a00da4e334ca10f9a58867a00530b5027e39f0d99d907f00c79ab8e97bd
SSDEEP:	12288:Yf0Plu2iNSbc3TKa00gTBz4CJOqW2WZrpyszp3AKlOALeCmxaMdGkq0yTOI:hdu1xTKacuCIqW2WNpyszpQKlreCmzGr
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....n`.....0..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4ba1b2
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:	0x606E938B [Thu Apr 8 05:24:27 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]
mov dword ptr [eax+4Eh], edx
inc edi
or eax, 000A1A0Ah
add byte ptr [eax], al
add byte ptr [ecx+45h], cl
dec esi
inc esp
scasb
inc edx

Instruction
pushad
add byte ptr [eax], 00000000h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xba160	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbc000	0x5bc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xbe000	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	0xb81d0	0xb8200	False	0.907598491599	data	7.90065645819	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xbc000	0x5bc	0x600	False	0.428385416667	data	4.16709322798	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xbe000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xbc090	0x32c	data		
RT_MANIFEST	0xbc3cc	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018 - 2021
Assembly Version	3.1.0.5
InternalName	JGg.exe
FileVersion	3.1.0.5
CompanyName	
LegalTrademarks	
Comments	
ProductName	Image Manager
ProductVersion	3.1.0.5
FileDescription	Image Manager
OriginalFilename	JGg.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-07:48:27.180566	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49705	9036	192.168.2.5	79.134.225.9
04/08/21-07:48:34.865853	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49706	9036	192.168.2.5	79.134.225.9
04/08/21-07:48:41.371122	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49708	9036	192.168.2.5	79.134.225.9
04/08/21-07:48:51.473538	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49712	9036	192.168.2.5	79.134.225.9
04/08/21-07:48:58.549058	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49718	9036	192.168.2.5	79.134.225.9
04/08/21-07:49:05.479859	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49720	9036	192.168.2.5	79.134.225.9
04/08/21-07:49:12.586754	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49721	9036	192.168.2.5	79.134.225.9
04/08/21-07:49:19.709242	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49724	9036	192.168.2.5	79.134.225.9
04/08/21-07:49:26.263194	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49730	9036	192.168.2.5	79.134.225.9
04/08/21-07:49:33.336462	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49731	9036	192.168.2.5	79.134.225.9
04/08/21-07:49:43.348194	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49732	9036	192.168.2.5	79.134.225.9
04/08/21-07:49:49.428114	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49733	9036	192.168.2.5	79.134.225.9
04/08/21-07:49:56.532596	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49736	9036	192.168.2.5	79.134.225.9
04/08/21-07:50:03.559289	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49737	9036	192.168.2.5	79.134.225.9
04/08/21-07:50:10.669991	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49738	9036	192.168.2.5	79.134.225.9

Network Port Distribution

Total Packets: 74

- 53 (DNS)
- 9036 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 07:48:26.866081953 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:27.123334885 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:27.123454094 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:27.180566072 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:27.464819908 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:27.522058964 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:27.550477028 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:27.773880005 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:27.810262918 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.079947948 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.102189064 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.107131958 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.109965086 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.112442970 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.117477894 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.119174004 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.220895052 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.334566116 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.334588051 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.334700108 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.339201927 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.342142105 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.345869064 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.345936060 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.351286888 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.351397991 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.356271982 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.356365919 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.362250090 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.362319946 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.368325949 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.368392944 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.489358902 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.559335947 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.563226938 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.563474894 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.567389011 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.573513985 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.575066090 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.579336882 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.586924076 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.588799000 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.591115952 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.596718073 CEST	9036	49705	79.134.225.9	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 07:48:28.596848011 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.601644039 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.605289936 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.608308077 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.611953974 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.617472887 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.617559910 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.624857903 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.629694939 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.629854918 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.635412931 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.640856981 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.640968084 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.783225060 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.788338900 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.788439035 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.795783997 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.801173925 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.801253080 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.806395054 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.816768885 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.816859007 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.824079037 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.827111006 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.827250004 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.831958055 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.836673021 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.836730003 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.844211102 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.851360083 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.851458073 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.854172945 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.857846022 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.857894897 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.862154961 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.866118908 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.866183043 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.871197939 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.874090910 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.875751019 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.878529072 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.883141041 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.883202076 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.886209011 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.888813019 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.888860941 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.891371965 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.893531084 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.893589020 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.899333954 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.903410912 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.903456926 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.905775070 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.911732912 CEST	9036	49705	79.134.225.9	192.168.2.5
Apr 8, 2021 07:48:28.911789894 CEST	49705	9036	192.168.2.5	79.134.225.9
Apr 8, 2021 07:48:28.912324905 CEST	9036	49705	79.134.225.9	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 07:48:00.896857023 CEST	53784	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:48:00.923322916 CEST	53	53784	8.8.8.8	192.168.2.5
Apr 8, 2021 07:48:02.408575058 CEST	65307	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:48:02.427350044 CEST	53	65307	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 07:48:06.749180079 CEST	64344	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:48:06.762243986 CEST	53	64344	8.8.8.8	192.168.2.5
Apr 8, 2021 07:48:11.783354998 CEST	62060	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:48:11.796008110 CEST	53	62060	8.8.8.8	192.168.2.5
Apr 8, 2021 07:48:12.681210995 CEST	61805	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:48:12.695575953 CEST	53	61805	8.8.8.8	192.168.2.5
Apr 8, 2021 07:48:13.369292974 CEST	54795	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:48:13.381272078 CEST	53	54795	8.8.8.8	192.168.2.5
Apr 8, 2021 07:48:18.824450970 CEST	49557	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:48:18.840527058 CEST	53	49557	8.8.8.8	192.168.2.5
Apr 8, 2021 07:48:24.758177996 CEST	61733	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:48:24.773238897 CEST	53	61733	8.8.8.8	192.168.2.5
Apr 8, 2021 07:48:26.554634094 CEST	65447	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:48:26.574033976 CEST	53	65447	8.8.8.8	192.168.2.5
Apr 8, 2021 07:48:26.831653118 CEST	52441	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:48:26.844439983 CEST	53	52441	8.8.8.8	192.168.2.5
Apr 8, 2021 07:48:34.417330980 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:48:34.596225023 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 8, 2021 07:48:40.197369099 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:48:40.212357998 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 8, 2021 07:48:41.047751904 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:48:41.060312033 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 8, 2021 07:48:41.099203110 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:48:41.115523100 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 8, 2021 07:48:41.416022062 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:48:41.428499937 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 8, 2021 07:48:48.194073915 CEST	56969	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:48:48.207519054 CEST	53	56969	8.8.8.8	192.168.2.5
Apr 8, 2021 07:48:48.250762939 CEST	55161	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:48:48.268780947 CEST	53	55161	8.8.8.8	192.168.2.5
Apr 8, 2021 07:48:52.499470949 CEST	54757	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:48:52.512556076 CEST	53	54757	8.8.8.8	192.168.2.5
Apr 8, 2021 07:48:53.715282917 CEST	49992	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:48:53.729660034 CEST	53	49992	8.8.8.8	192.168.2.5
Apr 8, 2021 07:48:54.344264030 CEST	60075	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:48:54.357188940 CEST	53	60075	8.8.8.8	192.168.2.5
Apr 8, 2021 07:48:56.016964912 CEST	55016	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:48:56.037491083 CEST	53	55016	8.8.8.8	192.168.2.5
Apr 8, 2021 07:48:58.308763027 CEST	64345	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:48:58.324584007 CEST	53	64345	8.8.8.8	192.168.2.5
Apr 8, 2021 07:49:01.351356983 CEST	57128	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:49:01.390177011 CEST	53	57128	8.8.8.8	192.168.2.5
Apr 8, 2021 07:49:05.247042894 CEST	54791	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:49:05.262593985 CEST	53	54791	8.8.8.8	192.168.2.5
Apr 8, 2021 07:49:12.299179077 CEST	50463	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:49:12.311767101 CEST	53	50463	8.8.8.8	192.168.2.5
Apr 8, 2021 07:49:18.401609898 CEST	50394	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:49:18.415184975 CEST	53	50394	8.8.8.8	192.168.2.5
Apr 8, 2021 07:49:19.285248995 CEST	58530	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:49:19.463937044 CEST	53	58530	8.8.8.8	192.168.2.5
Apr 8, 2021 07:49:21.707190037 CEST	53813	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:49:21.728830099 CEST	53	53813	8.8.8.8	192.168.2.5
Apr 8, 2021 07:49:26.016213894 CEST	63732	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:49:26.028558016 CEST	53	63732	8.8.8.8	192.168.2.5
Apr 8, 2021 07:49:33.096348047 CEST	57344	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:49:33.109216928 CEST	53	57344	8.8.8.8	192.168.2.5
Apr 8, 2021 07:49:40.105407000 CEST	54450	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:49:40.118659973 CEST	53	54450	8.8.8.8	192.168.2.5
Apr 8, 2021 07:49:49.194911957 CEST	59261	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:49:49.208095074 CEST	53	59261	8.8.8.8	192.168.2.5
Apr 8, 2021 07:49:52.491797924 CEST	57151	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:49:52.504312038 CEST	53	57151	8.8.8.8	192.168.2.5
Apr 8, 2021 07:49:54.534698963 CEST	59413	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:49:54.563549042 CEST	53	59413	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 07:49:56.283787966 CEST	60516	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:49:56.298697948 CEST	53	60516	8.8.8.8	192.168.2.5
Apr 8, 2021 07:50:03.256059885 CEST	51649	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:50:03.268548965 CEST	53	51649	8.8.8.8	192.168.2.5
Apr 8, 2021 07:50:10.280827045 CEST	65086	53	192.168.2.5	8.8.8.8
Apr 8, 2021 07:50:10.417323112 CEST	53	65086	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 07:48:26.831653118 CEST	192.168.2.5	8.8.8.8	0x117a	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Apr 8, 2021 07:48:34.417330980 CEST	192.168.2.5	8.8.8.8	0x5fb4	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Apr 8, 2021 07:48:41.099203110 CEST	192.168.2.5	8.8.8.8	0xdddf	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Apr 8, 2021 07:48:48.194073915 CEST	192.168.2.5	8.8.8.8	0x9a64	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Apr 8, 2021 07:48:58.308763027 CEST	192.168.2.5	8.8.8.8	0x6c03	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Apr 8, 2021 07:49:05.247042894 CEST	192.168.2.5	8.8.8.8	0xe4c	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Apr 8, 2021 07:49:12.299179077 CEST	192.168.2.5	8.8.8.8	0xc737	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Apr 8, 2021 07:49:19.285248995 CEST	192.168.2.5	8.8.8.8	0xbb26	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Apr 8, 2021 07:49:26.016213894 CEST	192.168.2.5	8.8.8.8	0xc029	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Apr 8, 2021 07:49:33.096348047 CEST	192.168.2.5	8.8.8.8	0xb015	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Apr 8, 2021 07:49:40.105407000 CEST	192.168.2.5	8.8.8.8	0x279d	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Apr 8, 2021 07:49:49.194911957 CEST	192.168.2.5	8.8.8.8	0x24da	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Apr 8, 2021 07:49:56.283787966 CEST	192.168.2.5	8.8.8.8	0xe4d0	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Apr 8, 2021 07:50:03.256059885 CEST	192.168.2.5	8.8.8.8	0x9dc1	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Apr 8, 2021 07:50:10.280827045 CEST	192.168.2.5	8.8.8.8	0x8a2a	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)

DNS Answers

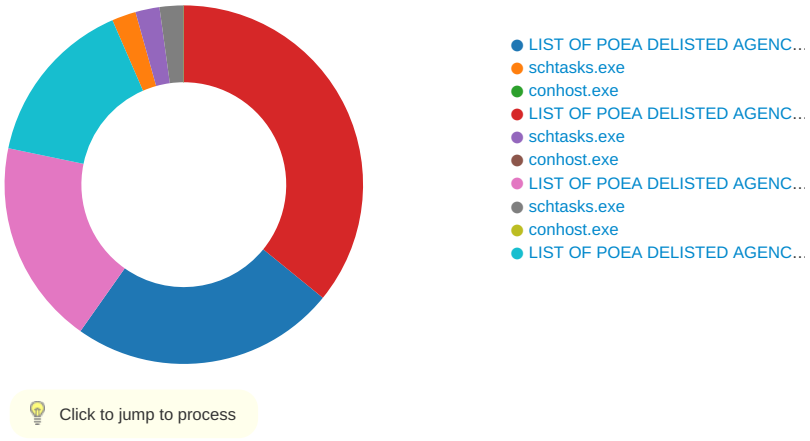
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 07:48:26.844439983 CEST	8.8.8.8	192.168.2.5	0x117a	No error (0)	shahzad73.casacam.net		79.134.225.9	A (IP address)	IN (0x0001)
Apr 8, 2021 07:48:34.596225023 CEST	8.8.8.8	192.168.2.5	0x5fb4	No error (0)	shahzad73.casacam.net		79.134.225.9	A (IP address)	IN (0x0001)
Apr 8, 2021 07:48:41.115523100 CEST	8.8.8.8	192.168.2.5	0xdddf	No error (0)	shahzad73.casacam.net		79.134.225.9	A (IP address)	IN (0x0001)
Apr 8, 2021 07:48:48.207519054 CEST	8.8.8.8	192.168.2.5	0x9a64	No error (0)	shahzad73.casacam.net		79.134.225.9	A (IP address)	IN (0x0001)
Apr 8, 2021 07:48:58.324584007 CEST	8.8.8.8	192.168.2.5	0x6c03	No error (0)	shahzad73.casacam.net		79.134.225.9	A (IP address)	IN (0x0001)
Apr 8, 2021 07:49:05.262593985 CEST	8.8.8.8	192.168.2.5	0xe4c	No error (0)	shahzad73.casacam.net		79.134.225.9	A (IP address)	IN (0x0001)
Apr 8, 2021 07:49:12.311767101 CEST	8.8.8.8	192.168.2.5	0xc737	No error (0)	shahzad73.casacam.net		79.134.225.9	A (IP address)	IN (0x0001)
Apr 8, 2021 07:49:19.463937044 CEST	8.8.8.8	192.168.2.5	0xbb26	No error (0)	shahzad73.casacam.net		79.134.225.9	A (IP address)	IN (0x0001)
Apr 8, 2021 07:49:26.028558016 CEST	8.8.8.8	192.168.2.5	0xc029	No error (0)	shahzad73.casacam.net		79.134.225.9	A (IP address)	IN (0x0001)
Apr 8, 2021 07:49:33.109216928 CEST	8.8.8.8	192.168.2.5	0xb015	No error (0)	shahzad73.casacam.net		79.134.225.9	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 07:49:40.118659973 CEST	8.8.8.8	192.168.2.5	0x279d	No error (0)	shahzad73.casacam.net		79.134.225.9	A (IP address)	IN (0x0001)
Apr 8, 2021 07:49:49.208095074 CEST	8.8.8.8	192.168.2.5	0x24da	No error (0)	shahzad73.casacam.net		79.134.225.9	A (IP address)	IN (0x0001)
Apr 8, 2021 07:49:56.298697948 CEST	8.8.8.8	192.168.2.5	0xe4d0	No error (0)	shahzad73.casacam.net		79.134.225.9	A (IP address)	IN (0x0001)
Apr 8, 2021 07:50:03.268548965 CEST	8.8.8.8	192.168.2.5	0x9dc1	No error (0)	shahzad73.casacam.net		79.134.225.9	A (IP address)	IN (0x0001)
Apr 8, 2021 07:50:10.417323112 CEST	8.8.8.8	192.168.2.5	0x8a2a	No error (0)	shahzad73.casacam.net		79.134.225.9	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: LIST OF POEA DELISTED AGENCIES.pdf.exe PID: 204 Parent PID: 5632

General

Start time:	07:48:07
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\LIST OF POEA DELISTED AGENCIES.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\LIST OF POEA DELISTED AGENCIES.pdf.exe'
Imagebase:	0x400000
File size:	756736 bytes
MD5 hash:	170934B168C75ED396332A6AF365A478
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: 00000000.00000002.259633262.00000000038F9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.259633262.00000000038F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.259633262.00000000038F9000.00000004.00000001.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	6DABCF06	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	6DABCF06	unknown
C:\Users\user\AppData\Roaming\IYcqUUrbhRC.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C901E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp1EF7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C907038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\LIST OF POEA DELISTED AGENCIES.pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DDCC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1EF7.tmp	success or wait	1	6C906A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\lYcqUUrbhRC.exe	unknown	756736	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 8b 93 6e 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 82 0b 00 00 08 00 00 00 00 00 00 b2 a1 0b 00 00 20 00 00 00 c0 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 0c 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L.....n`.......... ....0................. ....@.. ....@.................	success or wait	1	6C901B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp1EF7.tmp	unknown	1648	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 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo>.. <Date>2014-10- 25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </RegistrationI	success or wait	1	6C901B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\LIST OF POEA 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	6DDCC907	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	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C901B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C901B4F	ReadFile
C:\Users\user\Desktop\LIST OF POEA DELISTED AGENCIES.pdf.exe	unknown	756736	success or wait	1	6C901B4F	ReadFile

Analysis Process: schtasks.exe PID: 804 Parent PID: 204

General

Start time:	07:48:20
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\lYcqUUrbhRC' /XML 'C:\Users\user\AppData\Local\Temp\tmp1EF7.tmp'
Imagebase:	0xd90000
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\tmp1EF7.tmp	unknown	2	success or wait	1	D9AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp1EF7.tmp	unknown	1649	success or wait	1	D9ABD9	ReadFile

Analysis Process: conhost.exe PID: 5904 Parent PID: 804

General

Start time:	07:48:21
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: LIST OF POEA DELISTED AGENCIES.pdf.exe PID: 5592 Parent PID: 204

General

Start time:	07:48:21
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\LIST OF POEA DELISTED AGENCIES.pdf.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x920000
File size:	756736 bytes
MD5 hash:	170934B168C75ED396332A6AF365A478
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: 00000007.00000002.504910894.0000000005340000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.504910894.0000000005340000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.505287922.0000000005780000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.505287922.0000000005780000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.505287922.0000000005780000.00000004.00000001.sdmp, Author:

Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.505774970.0000000006620000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.505774970.0000000006620000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.505788129.0000000006630000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.505788129.0000000006630000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.505834895.0000000006670000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.505834895.0000000006670000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.505731790.00000000065F0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.505731790.00000000065F0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.505705551.00000000065D0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.505705551.00000000065D0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.505744453.0000000006600000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.505744453.0000000006600000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.505679942.00000000065B0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.505679942.00000000065B0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: NanoCore, Description: unknown, Source: 00000007.00000002.502325933.00000000040DD000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.505693803.00000000065C0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.505693803.00000000065C0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.505618683.0000000006560000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.505618683.0000000006560000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.497876017.0000000002DE1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.505717572.00000000065E0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.505717572.00000000065E0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.501649897.0000000003DE1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000007.00000002.501649897.0000000003DE1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.493270074.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.493270074.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000007.00000002.493270074.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.505218094.0000000005550000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.505218094.0000000005550000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.501964198.0000000003F3F000.00000004.00000001.sdmp, Author: Joe Security

	• Rule: NanoCore, Description: unknown, Source: 00000007.00000002.501964198.0000000003F3F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.505667640.00000000065A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.505667640.00000000065A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.502093667.0000000003FEF000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.502093667.0000000003FEF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.498112941.0000000002E4C000.00000004.00000001.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	6DABCF06	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	6DABCF06	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	6C90BEFF	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	6C901E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpB457.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C907038	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	6C901E60	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	6C90BEFF	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	6C90BEFF	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	10	6C901E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpB457.tmp	success or wait	1	6C906A95	DeleteFileW
C:\Users\user\Desktop\LIST OF POEA DELISTED AGENCIES.pdf.exe:Zone.Identifier	success or wait	1	6C882935	unknown

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	f2 3d 69 5c 9d fa d8 48	.=i\...H	success or wait	1	6C901B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmpB457.tmp	unknown	1325	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	6C901B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	62	43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 44 65 73 6b 74 6f 70 5c 4c 49 53 54 20 4f 46 20 50 4f 45 41 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\LIST OF POEA DELISTED AGENCIES.pdf.exe	success or wait	1	6C901B4F	WriteFile
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	12	6C901B4F	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	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C901B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C901B4F	ReadFile
C:\Users\user\Desktop\LIST OF POEA DELISTED AGENCIES.pdf.exe	unknown	4096	success or wait	1	6DA7D72F	unknown
C:\Users\user\Desktop\LIST OF POEA DELISTED AGENCIES.pdf.exe	unknown	512	success or wait	1	6DA7D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	6DA7D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6DA7D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6DA7D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6DA7D72F	unknown

Analysis Process: schtasks.exe PID: 6240 Parent PID: 5592

General

Start time:	07:48:24
Start date:	08/04/2021
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\tmpB457.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\tmpB457.tmp	unknown	2	success or wait	1	BAAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpB457.tmp	unknown	1326	success or wait	1	BAABD9	ReadFile

Analysis Process: conhost.exe PID: 6248 Parent PID: 6240

General

Start time:	07:48:24
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: LIST OF POEA DELISTED AGENCIES.pdf.exe PID: 6380 Parent PID: 904

General

Start time:	07:48:27
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\LIST OF POEA DELISTED AGENCIES.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\LIST OF POEA DELISTED AGENCIES.pdf.exe' 0
Imagebase:	0x430000
File size:	756736 bytes
MD5 hash:	170934B168C75ED396332A6AF365A478
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: 0000000B.00000002.294311257.0000000003869000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.294311257.0000000003869000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.294311257.0000000003869000.00000004.00000001.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	6DABCF06	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	6DABCF06	unknown
C:\Users\user\AppData\Local\Temp\tmp5375.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C907038	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp5375.tmp	success or wait	1	6C906A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp5375.tmp	unknown	1648	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 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49	<?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>.. </RegistrationI	success or wait	1	6C901B4F	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	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C901B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C901B4F	ReadFile

Analysis Process: schtasks.exe PID: 6672 Parent PID: 6380

General

Start time:	07:48:34
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\lYcqUUrbhRC' /XML 'C:\Users\user\AppData\Local\Temp\tmp5375.tmp'
Imagebase:	0xd50000
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\tmp5375.tmp	unknown	2	success or wait	1	D5AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp5375.tmp	unknown	1649	success or wait	1	D5ABD9	ReadFile

Analysis Process: conhost.exe PID: 6756 Parent PID: 6672

General

Start time:	07:48:34
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: LIST OF POEA DELISTED AGENCIES.pdf.exe PID: 6836 Parent PID: 6380

General

Start time:	07:48:35
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\LIST OF POEA DELISTED AGENCIES.pdf.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xfc0000
File size:	756736 bytes
MD5 hash:	170934B168C75ED396332A6AF365A478
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.309866896.0000000004429000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.309866896.0000000004429000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.308929356.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.308929356.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.308929356.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.309746032.0000000003421000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.309746032.0000000003421000.00000004.00000001.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	6DABCF06	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	6DABCF06	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	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C901B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C901B4F	ReadFile

Disassembly

Code Analysis