ID: 355833
Sample Name: LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe
Cookbook: default.jbs
Time: 07:41:00
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

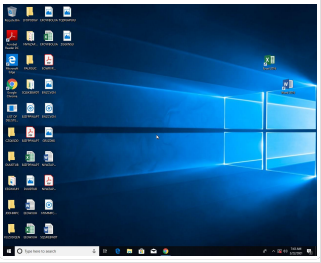
Analysis Report LIST OF DELISTED AGENCIES 22ND FE…

Overview

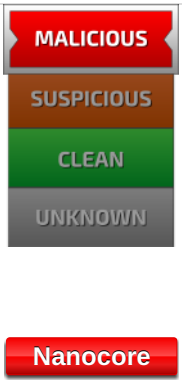
General Information

Sample Name:	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe
Analysis ID:	355833
MD5:	988bbc4bf9b82be.
SHA1:	c4a75851e915e5..
SHA256:	9af6ee7679b5e12.
Tags:	exe NanoCore RAT

Most interesting Screenshot:



Detection



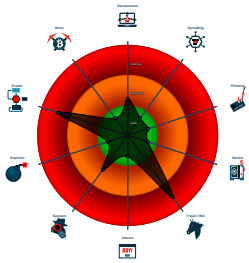
Nanocore

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 dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Sigma detected: Suspicious Double …
- Snort IDS alert for network traffic (e…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Binary contains a suspicious time st…
- C2 URLs / IPs found in malware con…

Classification



Startup

- **System is w10x64**
- LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe (PID: 6336 cmdline: 'C:\Users\user\Desktop\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe' MD5: 988BBC4BF9B82BE5DFA915ECB1B63C49)
  - schtasks.exe (PID: 6864 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\FOvTZkul' /XML 'C:\Users\user\AppData\Local\Temp\tmp9968.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6872 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe (PID: 6908 cmdline: {path} MD5: 988BBC4BF9B82BE5DFA915ECB1B63C49)
    - schtasks.exe (PID: 4552 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp4916.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5460 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe (PID: 3132 cmdline: 'C:\Users\user\Desktop\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe' 0 MD5: 988BBC4BF9B82BE5DFA915ECB1B63C49)
  - schtasks.exe (PID: 2196 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\FOvTZkul' /XML 'C:\Users\user\AppData\Local\Temp\tmpA04.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5928 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe (PID: 1276 cmdline: {path} MD5: 988BBC4BF9B82BE5DFA915ECB1B63C49)
  - LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe (PID: 1236 cmdline: {path} MD5: 988BBC4BF9B82BE5DFA915ECB1B63C49)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "c4cca249-81f6-4232-9f14-01569e09f5f0",
  "Group": "JANUARY",
  "Domain1": "shahzad73.casacam.net",
  "Domain2": "shahzad73.ddns.net",
  "Port": 9036,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "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
00000015.00000002.365342774.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000015.00000002.365342774.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000015.00000002.365342774.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000007.00000002.493487439.0000000002DC1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.280044415.000000000429000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x10cf65:$x1: NanoCore.ClientPluginHost • 0x10cfa2:$x2: IClientNetworkHost • 0x110ad5:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Click to see the 24 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe.4729f40.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe.4729f40.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
21.2.LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe.3e9b7ee.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0x145e3:$x1: NanoCore.ClientPluginHost • 0x2d5d7:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost • 0x14610:$x2: IClientNetworkHost • 0x2d604:$x2: IClientNetworkHost
0.2.LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe.4729f40.3.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe.4729f40.3.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
Click to see the 38 entries				

Sigma Overview

System Summary:

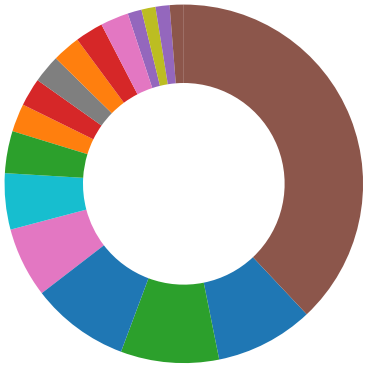
Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Sigma detected: Suspicious Double Extension

Signature Overview

- AV Detection
- Compliance
- Networking
- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality



Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected Nanocore RAT
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Compliance:

- Uses 32bit PE files
- Contains modern PE file flags such as dynamic base (ASLR) or NX

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)
- Initial sample is a PE file and has a suspicious name

Data Obfuscation:

- .NET source code contains potential unpacker
- Binary contains a suspicious time stamp

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)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

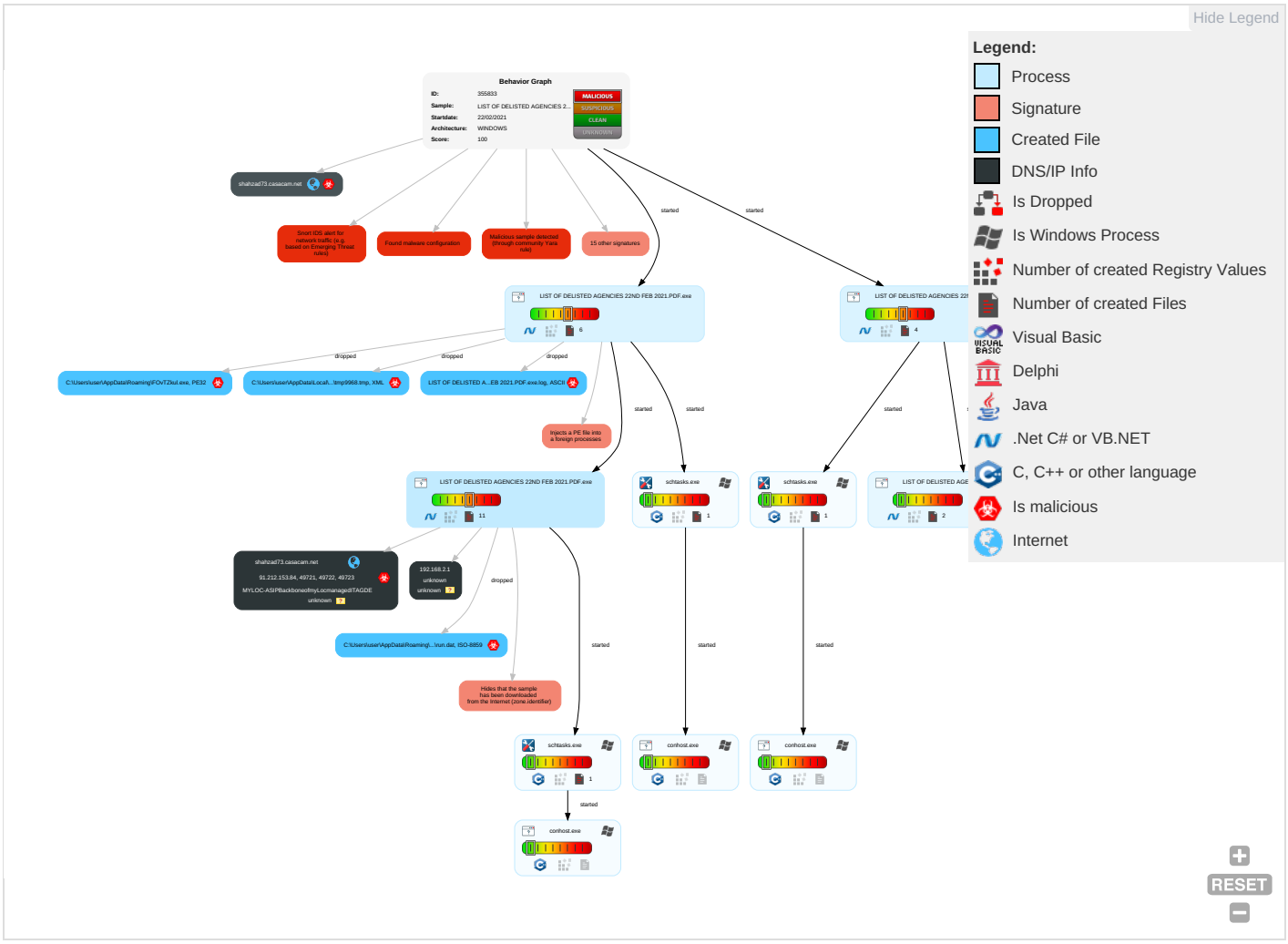
Detected Nanocore Rat

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
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1 1	Input Capture 2 1	Query Registry 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 3	LSASS Memory	Security Software Discovery 1 2 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1 2	DCSync	System Information Discovery 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Timestomp 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe	13%	ReversingLabs	Win32.Trojan.Generic	
LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\FOvTZkul.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\FOvTZkul.exe	13%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
21.2.LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
shahzad73.ddns.net	1%	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.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.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.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
shahzad73.casacam.net	5%	Virustotal		Browse
shahzad73.casacam.net	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

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

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
shahzad73.ddns.net	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
shahzad73.casacam.net	true	• 5%, Virustotal, Browse • Avira URL Cloud: safe	unknown

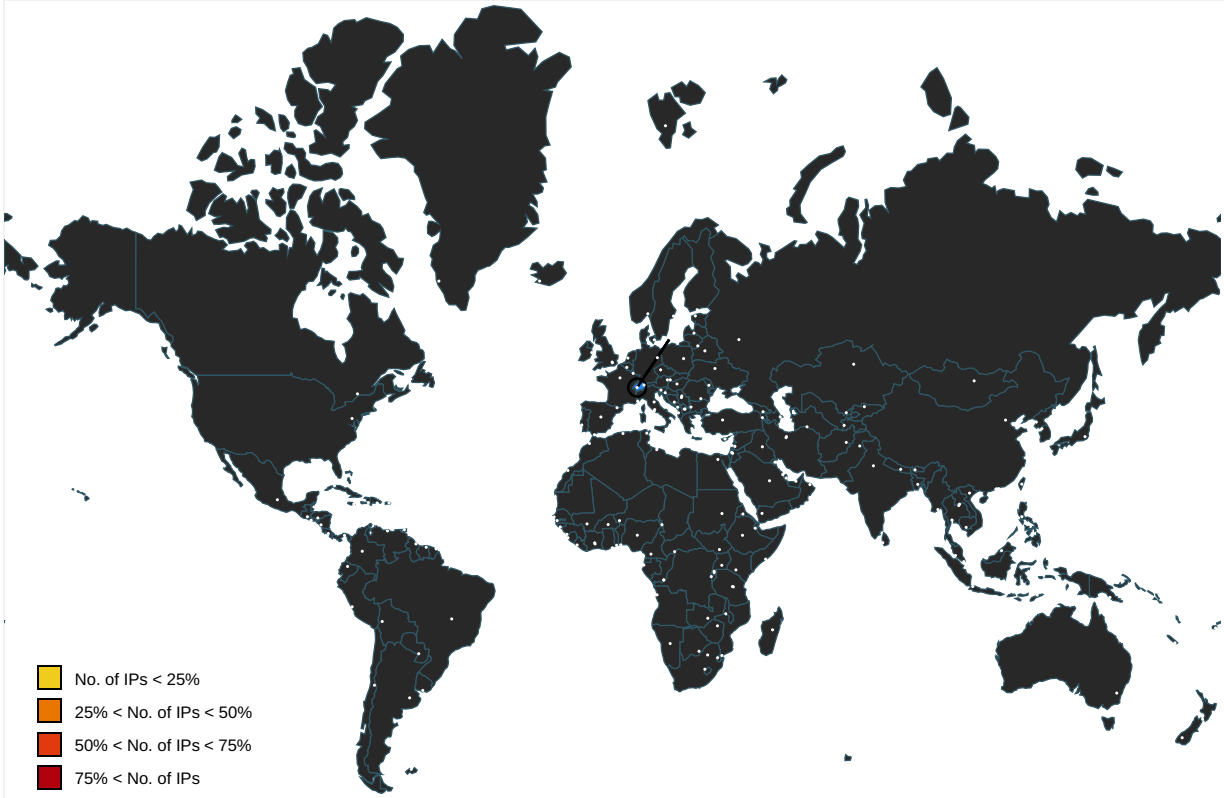
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 00000000.00000002.285862518.00000000072A2000.00000004.00000001.sdmp, LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 0000000F.00000002.354228123.000000000571000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 00000000.00000002.285862518.00000000072A2000.00000004.00000001.sdmp, LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 0000000F.00000002.354228123.000000000571000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 00000000.00000002.285862518.00000000072A2000.00000004.00000001.sdmp, LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 0000000F.00000002.354228123.000000000571000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 00000000.00000002.285862518.00000000072A2000.00000004.00000001.sdmp, LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 0000000F.00000002.354228123.000000000571000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 00000000.00000002.285862518.00000000072A2000.00000004.00000001.sdmp, LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 0000000F.00000002.354228123.000000000571000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 00000000.00000002.285862518.00000000072A2000.00000004.00000001.sdmp, LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 0000000F.00000002.354228123.000000000571000.00000002.00000001.sdmp	false		high
http://www.tiro.com	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 0000000F.00000002.354228123.0000000005710000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 0000000F.00000002.354228123.000000005710000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 00000000.00000002.285862518.00000000072A2000.00000004.00000001.sdmp, LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 0000000F.00000002.354228123.000000000571000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 00000000.00000002.285862518.00000000072A2000.00000004.00000001.sdmp, LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 0000000F.00000002.354228123.000000000571000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 00000000.00000002.285862518.00000000072A2000.00000004.00000001.sdmp, LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 0000000F.00000002.354228123.000000000571000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 00000000.00000002.285862518.00000000072A2000.00000004.00000001.sdmp, LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 0000000F.00000002.354228123.000000000571000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 00000000.00000002.285862518.00000000072A2000.00000004.00000001.sdmp, LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 0000000F.00000002.354228123.000000000571000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 00000000.00000002.285862518.00000000072A2000.00000004.00000001.sdmp, LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 0000000F.00000002.354228123.000000000571000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 00000000.00000002.285862518.00000000072A2000.00000004.00000001.sdmp, LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 0000000F.00000002.354228123.000000000571000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 00000000.00000002.285862518.00000000072A2000.00000004.00000001.sdmp, LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 0000000F.00000002.354228123.000000000571000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 00000000.00000002.285862518.00000000072A2000.00000004.00000001.sdmp, LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 0000000F.00000002.354228123.000000000571000.00000002.00000001.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 DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 00000000.00000002.285862518.00000000072A2000.00000004.00000001.sdmp, LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 0000000F.00000002.354228123.000000000571000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 00000000.00000002.285862518.00000000072A2000.00000004.00000001.sdmp, LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 0000000F.00000002.354228123.000000000571000 0.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 00000000.00000002.285862518.00000000072A2000.00000004.00000001.sdmp, LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 0000000F.00000002.354228123.000000000571000 0.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 00000000.00000002.285862518.00000000072A2000.00000004.00000001.sdmp, LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 0000000F.00000002.354228123.000000000571000 0.00000002.00000001.sdmp	false		high
http://www.fonts.com	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 00000000.00000002.285862518.00000000072A2000.00000004.00000001.sdmp, LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 0000000F.00000002.354228123.000000000571000 0.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 00000000.00000002.285862518.00000000072A2000.00000004.00000001.sdmp, LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 0000000F.00000002.354228123.000000000571000 0.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 00000000.00000002.285862518.00000000072A2000.00000004.00000001.sdmp, LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 0000000F.00000002.354228123.000000000571000 0.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 00000000.00000002.285862518.00000000072A2000.00000004.00000001.sdmp, LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 0000000F.00000002.354228123.000000000571000 0.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 00000000.00000002.279958013.000000000320100000.00000004.00000001.sdmp, LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 0000000F.00000002.349317167.000000000285100 0.00000004.00000001.sdmp	false		high
http://www.sakkal.com	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 00000000.00000002.285862518.00000000072A2000.00000004.00000001.sdmp, LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe, 0000000F.00000002.354228123.000000000571000 0.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	355833
Start date:	22.02.2021
Start time:	07:41:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	LIST OF DELISTED AGENCIES 22ND FEB 2021.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:	32
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@17/10@15/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.7% (good quality ratio 0.6%) • Quality average: 57.4% • Quality standard deviation: 27.8%
HCA Information:	• Successful, ratio: 96% • 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, UsoClient.exe • Excluded IPs from analysis (whitelisted): 51.103.5.186, 104.42.151.234, 204.79.197.200, 13.107.21.200, 104.79.89.181, 93.184.220.29, 51.104.139.180, 13.64.90.137, 92.122.145.220, 104.43.193.48, 104.79.90.110, 104.43.139.144, 93.184.221.240, 92.122.213.194, 92.122.213.247, 20.54.26.129 • Excluded domains from analysis (whitelisted): storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, cs9.wac.phicdn.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, storeedgefd.xbetservices.akadns.net, arc.msn.com, wu.azureedge.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, storeedgefd.dsx.mp.microsoft.com, www.bing.com, client.wns.windows.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, dual-a-0001.a-msedge.net, wu.ec.azureedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, e16646.dscg.akamaiedge.net, skypedataprdcolwus16.cloudapp.net, vip2-par02p.wns.notify.trafficmanager.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:41:54	API Interceptor	803x Sleep call for process: LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe modified
07:42:19	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

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

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
shahzad73.casacam.net	POEA ADVISORY 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
	POEA MEMORANDUM N0 056.exe	Get hash	malicious	Browse	• 91.212.153.84
	Protected.exe	Get hash	malicious	Browse	• 91.212.153.84
	Protected.2.exe	Get hash	malicious	Browse	• 91.212.153.84

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MYLOC-ASIPBackboneofmyLocmanagedITAGDE	POEA ADVISORY 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
	POEA MEMORANDUM N0 056.exe	Get hash	malicious	Browse	• 91.212.153.84
	Swift_Payment_jpeg.exe	Get hash	malicious	Browse	• 62.141.37.17
	Protected.exe	Get hash	malicious	Browse	• 91.212.153.84
	Protected.2.exe	Get hash	malicious	Browse	• 91.212.153.84
	FickerStealer.exe	Get hash	malicious	Browse	• 89.163.225.172
	Documentaci#U00f3n.doc	Get hash	malicious	Browse	• 89.163.210.141
	SecuriteInfo.com.Trojan.DownLoader36.34557.26355.exe	Get hash	malicious	Browse	• 89.163.140.102
	TaskAudio Driver.exe	Get hash	malicious	Browse	• 193.111.198.220
	Z8363664.doc	Get hash	malicious	Browse	• 89.163.210.141
	OhGodAnETHlargementPill2.exe	Get hash	malicious	Browse	• 193.111.198.220
	godflex-r2.exe	Get hash	malicious	Browse	• 193.111.198.220
	PolarisBiosEditor-master.exe	Get hash	malicious	Browse	• 193.111.198.220
	NKsplucdAu.exe	Get hash	malicious	Browse	• 85.114.134.88
	IZVNh1BPxm.exe	Get hash	malicious	Browse	• 85.114.134.88

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	qG5E4q8Cv5.exe	Get hash	malicious	Browse	• 85.114.134.88

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe.log

Process:	C:\Users\user\Desktop\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
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\tmp4916.tmp

Process:	C:\Users\user\Desktop\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1334
Entropy (8bit):	5.144404597944132
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0P1rmxtn:cbk4oL600QydbQxIYODOLedq3S1rmj
MD5:	0A5E79234918A9DC7421157353741D7B
SHA1:	BC266069355067D7392BF79C3D00247E9F087372
SHA-256:	7F9B2BC813F0CA561A2CDFF31637BA263F485678E010B3B826852D84D86DB505
SHA-512:	6202445904E99D2C2F67EBAB1DDB41C406D180DD4713A6A8DE4644639252296F4C96E833BF87BB9A85FE4302334660334ECE2022BA5A28A23CE05863CF7668C
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp9968.tmp

Process:	C:\Users\user\Desktop\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.170732655384553
Encrypted:	false

C:\Users\user\AppData\Local\Temp\tmp9968.tmp

SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjplgUYODOLD9RJh7h8gKBb+Btn:cbhC7ZlNQF/rydbz9I3YODOLNdq3o
MD5:	2D032EADAECDA4DB625CF30C2002F552
SHA1:	3C1EE0FB3F3C69F04EE725902FE767B0690E3BC5
SHA-256:	334E776DB8114F5D9354856A0827C69578508F04895770BF295844EBD3C26DCD
SHA-512:	0B429154D4F5FA3A8F7C67F89D305D85B884A46E58194C98DF0F89F52858B059C1095552015931E28D16E3910EDCC448F1241DFD1096FDB78FB80C81DE3CEEF
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

C:\Users\user\AppData\Local\Temp\tmpA04.tmp

Process:	C:\Users\user\Desktop\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.170732655384553
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjplgUYODOLD9RJh7h8gKBb+Btn:cbhC7ZlNQF/rydbz9I3YODOLNdq3o
MD5:	2D032EADAECDA4DB625CF30C2002F552
SHA1:	3C1EE0FB3F3C69F04EE725902FE767B0690E3BC5
SHA-256:	334E776DB8114F5D9354856A0827C69578508F04895770BF295844EBD3C26DCD
SHA-512:	0B429154D4F5FA3A8F7C67F89D305D85B884A46E58194C98DF0F89F52858B059C1095552015931E28D16E3910EDCC448F1241DFD1096FDB78FB80C81DE3CEEF
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\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat

Process:	C:\Users\user\Desktop\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe
File Type:	data
Category:	dropped
Size (bytes):	1856
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	48:IknjhUknjhUknjhUknjhUknjhUknjhUknjhL:HjhDjhDjhDjhDjhDjhDjhL
MD5:	30D23CC577A89146961915B57F408623
SHA1:	9B5709D6081D8E0A570511E6E0AAE96FA041964F
SHA-256:	E2130A72E55193D402B5F43F7F3584ECF6B423F8EC4B1B1B69AD693C7E0E5A9E
SHA-512:	2D5C5747FD04F8326C2CC1FB313925070BC01D3352AFA6C36C167B72757A15F58B6263D96BD606338DA055812E69DDB628A6E18D64DD59697C2F42D1C58CC6
Malicious:	false
Reputation:	low
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....~f.G0^..;....W2.=...K.~.L..&f...p............:7rH}..../H......L...?...A.K...J.=8x!....+.2e'..E?.G......[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....~f.G0^..;....W2.=...K.~.L..&f...p............:7rH}..../H......L...?...A.K...J.=8x!....+.2e'..E?.G......[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....~f.G0^..;....W2.=...K.~.L..&f...p............:7rH}..../H......L...?...A.K...J.=8x!....+.2e'..E?.G......[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....~f.G0^..;....W2.=...K.~.L..&f...p............:7rH}..../H......L...?...A.K...J.=8x!....+.2e'..E?.G......[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.

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

Process:	C:\Users\user\Desktop\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:0n:0n
MD5:	70B0C2A7A87AC6FFCA5455CE1469ADD8
SHA1:	9C5A4BE670B5898E11ABB80D9722FC69E2B7B331
SHA-256:	E3A50A2FC5598850A582C70D5279C0A9337109C279815754C74C76A559893F05

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
SHA-512:	B0373AA939BAA96D772EDC916C27FCA662D0DD3AA0CBA79798878247D128724A05BC851BADED5C645DA17E082F0E1AFB3BE38ADD0F625EE8F89EAF1FF9C218C4
Malicious:	**true**
Preview:	.4onH..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671BCB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe
File Type:	data
Category:	dropped
Size (bytes):	327768
Entropy (8bit):	**7.999367066417797**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3PlZmqze1d1wI8lkWmtjJ/3Exi:LkjbU7LjGxi
MD5:	2E52F446105FBF828E63CF808B721F9C
SHA1:	5330E54F238F46DC04C1AC62B051DB4FCD7416FB
SHA-256:	2F7479AA2661BD259747BC89106031C11B3A3F79F12190E7F19F5DF65B7C15C8
SHA-512:	C08BA0E3315E2314ECBEF38722DF834C2CB8412446A9A310F41A8F83B4AC5984FCC1B26A1D8B0D58A730FDBDD885714854BDFD04DCDF7F582FC125F552D5C3A
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i..........J.5b7}..fK..HV.,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&.jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<..._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	71
Entropy (8bit):	4.783638408804809
Encrypted:	false
SSDEEP:	3:oNUWJRWpspo7ghog2Zm83kA:oNNJACm7grK0A
MD5:	43AA8380E32959A51180B7AEA3859F9E
SHA1:	203641DD6CCD8889539BF48008CCFDADBC113800
SHA-256:	83A8A0F122EC075D3E7989A32EF07461900ACAB91FCAED30A4F532203229DE96
SHA-512:	30FDBD71FBA99936913807A595BCEAE023D6F182278594E4728B2520F2261EB38C1C47EB13D1DED996E9E2BDA3A0100D8CA096D3FD96013BB13B89E1B2161F5
Malicious:	false
Preview:	C:\Users\user\Desktop\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe

C:\Users\user\AppData\Roaming\FOvTZkul.exe	
Process:	C:\Users\user\Desktop\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	643072
Entropy (8bit):	7.94701935290762
Encrypted:	false

C:\Users\user\AppData\Roaming\FOvTZkul.exe	
SSDEEP:	12288:boyEOYO9NojvDqUWCpWf0hWrJMQe/xDvtzgHQ0Hhc7R0yQ:boA4bqmpNhWrmjBFQIR
MD5:	988BBC4BF9B82BE5DFA915ECB1B63C49
SHA1:	C4A75851E915E5072A9EC720139A7693F3819F84
SHA-256:	9AF6EE7679B5E12C34B0530A2B7639C65B1FF8449930ED9A6156338A2EEBBB98
SHA-512:	6BEE253CE21F6A9591418BC09753A19E0F8829A8DB1A51A82AAAC057A2A9CDD311388F7CA2F732ABB6A4914424CC68AA443904108103BA2231863303580297BC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 13%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....P.....0.....2.... .....@.. .....@..... ..@.....O..... ....H.....text...8.... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....i...]....K.....0..S.....r...p(....(....(.....?.....+..r...p(.....(.....X.....-...s.....+`.....,.....Y..o.. ....+;.....(.....,....X.....o.....+.....o.....X.....-..+.....o.....+;..(.....,...+,..(.....,....X....(.....(!...-.....o".....(#.....+.....X.....-.*.....H".....". ($....*....0.....r'..p(.....(...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.94701935290762
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 DELISTED AGENCIES 22ND FEB 2021.PDF.exe
File size:	643072
MD5:	988bbc4bf9b82be5dfa915ecb1b63c49
SHA1:	c4a75851e915e5072a9ec720139a7693f3819f84
SHA256:	9af6ee7679b5e12c34b0530a2b7639c65b1ff8449930ed9a6156338a2eebbb98
SHA512:	6bee253ce21f6a9591418bc09753a19e0f8829a8db1a51a82aaac057a2a9cdd311388f7ca2f732abb6a4914424cc68aa443904108103ba2231863303580297bc
SSDEEP:	12288:boyEOYO9NojvDqUWCpWf0hWrJMQe/xDvtzgHQ0Hhc7R0yQ:boA4bqmpNhWrmjBFQIR
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....P.....0.....2.... .....@.. .....@.....@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x49e432
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:	0xFD105003 [Thu Jul 17 02:25:07 2104 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0

General

File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x9e3e0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa0000	0x5e4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa2000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x9e3c4	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x9c438	0x9c600	False	0.953935289269	data	7.95337285484	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa0000	0x5e4	0x600	False	0.438802083333	data	4.24660402967	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa2000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xa0090	0x354	data		
RT_MANIFEST	0xa03f4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2019 - 2021
Assembly Version	1.0.0.0
InternalName	82kT.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Champen Generator
ProductVersion	1.0.0.0
FileDescription	Champen Generator
OriginalFilename	82kT.exe

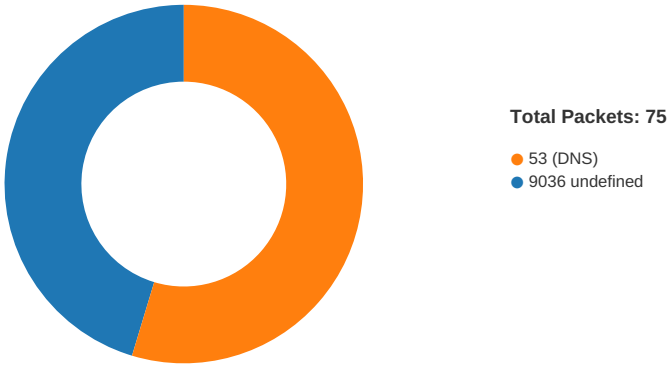
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/22/21-07:42:21.593427	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49721	9036	192.168.2.5	91.212.153.84
02/22/21-07:42:29.881106	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49722	9036	192.168.2.5	91.212.153.84
02/22/21-07:42:36.492972	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49723	9036	192.168.2.5	91.212.153.84
02/22/21-07:42:43.622074	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49730	9036	192.168.2.5	91.212.153.84
02/22/21-07:42:50.684592	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49731	9036	192.168.2.5	91.212.153.84
02/22/21-07:42:55.953198	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49732	9036	192.168.2.5	91.212.153.84
02/22/21-07:43:00.563359	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49738	9036	192.168.2.5	91.212.153.84
02/22/21-07:43:06.741995	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49739	9036	192.168.2.5	91.212.153.84
02/22/21-07:43:12.695848	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49740	9036	192.168.2.5	91.212.153.84
02/22/21-07:43:20.848089	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49741	9036	192.168.2.5	91.212.153.84

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/22/21-07:43:26.935863	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49742	9036	192.168.2.5	91.212.153.84
02/22/21-07:43:34.412469	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49744	9036	192.168.2.5	91.212.153.84
02/22/21-07:43:40.491398	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	9036	192.168.2.5	91.212.153.84
02/22/21-07:43:47.726783	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49746	9036	192.168.2.5	91.212.153.84
02/22/21-07:43:54.481294	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49749	9036	192.168.2.5	91.212.153.84

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 07:42:21.346079111 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:21.400332928 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:21.400435925 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:21.593426943 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:21.658158064 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:21.783725023 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:21.838402987 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:21.838526964 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:21.931456089 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:21.931559086 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.025207996 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.043894053 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.043924093 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.043936968 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.043948889 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.044037104 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.098258018 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.098294020 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.098309040 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.098325968 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.098341942 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.098352909 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.098357916 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.098373890 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.098388910 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.098390102 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.098411083 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.098442078 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.152570963 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.152600050 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.152615070 CET	9036	49721	91.212.153.84	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 07:42:22.152632952 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.152647972 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.152661085 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.152667999 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.152693987 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.152693987 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.152704000 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.152709007 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.152712107 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.152721882 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.152739048 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.152755022 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.152757883 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.152774096 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.152791023 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.152803898 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.152827024 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.153772116 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.153791904 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.153839111 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.208830118 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.208859921 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.208875895 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.208890915 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.208909035 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.208920002 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.208925009 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.208945036 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.208954096 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.208962917 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.208971024 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.208977938 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.208995104 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.209007025 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.209011078 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.209027052 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.209039927 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.209043980 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.209059954 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.209063053 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.209079027 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.209095955 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.209104061 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.209111929 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.209127903 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.209136009 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.209144115 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.209158897 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.209166050 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.209175110 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.209192038 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.209206104 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.209212065 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.209228992 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.209244013 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.209247112 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.209259987 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.209269047 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.209275007 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.209290981 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.209292889 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.209306955 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.209321976 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.209341049 CET	9036	49721	91.212.153.84	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 07:42:22.209343910 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.209358931 CET	9036	49721	91.212.153.84	192.168.2.5
Feb 22, 2021 07:42:22.209373951 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.209398985 CET	49721	9036	192.168.2.5	91.212.153.84
Feb 22, 2021 07:42:22.263416052 CET	9036	49721	91.212.153.84	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 07:41:40.746920109 CET	52704	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:41:40.798894882 CET	53	52704	8.8.8.8	192.168.2.5
Feb 22, 2021 07:41:40.999994040 CET	52212	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:41:41.051974058 CET	53	52212	8.8.8.8	192.168.2.5
Feb 22, 2021 07:41:41.061655045 CET	54302	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:41:41.110433102 CET	53	54302	8.8.8.8	192.168.2.5
Feb 22, 2021 07:41:41.183825016 CET	53784	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:41:41.239687920 CET	65307	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:41:41.243401051 CET	53	53784	8.8.8.8	192.168.2.5
Feb 22, 2021 07:41:41.291181087 CET	53	65307	8.8.8.8	192.168.2.5
Feb 22, 2021 07:41:42.013196945 CET	64344	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:41:42.057163000 CET	62060	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:41:42.070410967 CET	53	64344	8.8.8.8	192.168.2.5
Feb 22, 2021 07:41:42.106024981 CET	53	62060	8.8.8.8	192.168.2.5
Feb 22, 2021 07:41:42.292028904 CET	61805	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:41:42.341510057 CET	53	61805	8.8.8.8	192.168.2.5
Feb 22, 2021 07:41:44.636951923 CET	54795	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:41:44.695111036 CET	53	54795	8.8.8.8	192.168.2.5
Feb 22, 2021 07:42:07.032399893 CET	49557	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:42:07.081406116 CET	53	49557	8.8.8.8	192.168.2.5
Feb 22, 2021 07:42:08.875176907 CET	61733	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:42:08.935323954 CET	53	61733	8.8.8.8	192.168.2.5
Feb 22, 2021 07:42:09.026894093 CET	65447	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:42:09.078555107 CET	53	65447	8.8.8.8	192.168.2.5
Feb 22, 2021 07:42:10.430279970 CET	52441	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:42:10.479943991 CET	53	52441	8.8.8.8	192.168.2.5
Feb 22, 2021 07:42:11.501677990 CET	62176	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:42:11.550242901 CET	53	62176	8.8.8.8	192.168.2.5
Feb 22, 2021 07:42:12.912683964 CET	59596	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:42:12.964369059 CET	53	59596	8.8.8.8	192.168.2.5
Feb 22, 2021 07:42:13.984936953 CET	65296	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:42:14.038144112 CET	53	65296	8.8.8.8	192.168.2.5
Feb 22, 2021 07:42:15.270951033 CET	63183	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:42:15.320935011 CET	53	63183	8.8.8.8	192.168.2.5
Feb 22, 2021 07:42:16.584808111 CET	60151	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:42:16.636240959 CET	53	60151	8.8.8.8	192.168.2.5
Feb 22, 2021 07:42:17.960716009 CET	56969	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:42:18.013379097 CET	53	56969	8.8.8.8	192.168.2.5
Feb 22, 2021 07:42:19.170850992 CET	55161	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:42:19.233702898 CET	53	55161	8.8.8.8	192.168.2.5
Feb 22, 2021 07:42:20.671390057 CET	54757	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:42:20.886221886 CET	53	54757	8.8.8.8	192.168.2.5
Feb 22, 2021 07:42:29.532972097 CET	49992	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:42:29.733645916 CET	53	49992	8.8.8.8	192.168.2.5
Feb 22, 2021 07:42:36.199965954 CET	60075	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:42:36.378938913 CET	53	60075	8.8.8.8	192.168.2.5
Feb 22, 2021 07:42:37.266455889 CET	55016	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:42:37.327311993 CET	53	55016	8.8.8.8	192.168.2.5
Feb 22, 2021 07:42:38.906033039 CET	64345	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:42:38.954696894 CET	53	64345	8.8.8.8	192.168.2.5
Feb 22, 2021 07:42:41.304291964 CET	57128	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:42:41.353187084 CET	53	57128	8.8.8.8	192.168.2.5
Feb 22, 2021 07:42:43.312575102 CET	54791	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:42:43.519887924 CET	53	54791	8.8.8.8	192.168.2.5
Feb 22, 2021 07:42:50.568192005 CET	50463	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 07:42:50.628134012 CET	53	50463	8.8.8.8	192.168.2.5
Feb 22, 2021 07:42:55.344563007 CET	50394	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:42:55.401375055 CET	53	50394	8.8.8.8	192.168.2.5
Feb 22, 2021 07:42:59.249066114 CET	58530	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:42:59.307461023 CET	53	58530	8.8.8.8	192.168.2.5
Feb 22, 2021 07:43:00.449156046 CET	53813	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:43:00.506299019 CET	53	53813	8.8.8.8	192.168.2.5
Feb 22, 2021 07:43:06.597510099 CET	63732	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:43:06.655592918 CET	53	63732	8.8.8.8	192.168.2.5
Feb 22, 2021 07:43:12.588944912 CET	57344	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:43:12.637726068 CET	53	57344	8.8.8.8	192.168.2.5
Feb 22, 2021 07:43:20.708695889 CET	54450	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:43:20.768855095 CET	53	54450	8.8.8.8	192.168.2.5
Feb 22, 2021 07:43:26.781378031 CET	59261	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:43:26.829952002 CET	53	59261	8.8.8.8	192.168.2.5
Feb 22, 2021 07:43:26.895569086 CET	57151	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:43:26.944562912 CET	53	57151	8.8.8.8	192.168.2.5
Feb 22, 2021 07:43:34.210283041 CET	59413	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:43:34.273186922 CET	53	59413	8.8.8.8	192.168.2.5
Feb 22, 2021 07:43:40.341476917 CET	60516	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:43:40.398835897 CET	53	60516	8.8.8.8	192.168.2.5
Feb 22, 2021 07:43:47.446223974 CET	51649	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:43:47.662240982 CET	53	51649	8.8.8.8	192.168.2.5
Feb 22, 2021 07:43:49.746726036 CET	65086	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:43:49.814780951 CET	53	65086	8.8.8.8	192.168.2.5
Feb 22, 2021 07:43:54.371562004 CET	56432	53	192.168.2.5	8.8.8.8
Feb 22, 2021 07:43:54.423114061 CET	53	56432	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 07:42:20.671390057 CET	192.168.2.5	8.8.8.8	0x127c	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 22, 2021 07:42:29.532972097 CET	192.168.2.5	8.8.8.8	0x7f3b	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 22, 2021 07:42:36.199965954 CET	192.168.2.5	8.8.8.8	0x3447	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 22, 2021 07:42:43.312575102 CET	192.168.2.5	8.8.8.8	0x68b5	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 22, 2021 07:42:50.568192005 CET	192.168.2.5	8.8.8.8	0xa58a	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 22, 2021 07:42:55.344563007 CET	192.168.2.5	8.8.8.8	0xfe4d	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 22, 2021 07:43:00.449156046 CET	192.168.2.5	8.8.8.8	0xe5d8	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 22, 2021 07:43:06.597510099 CET	192.168.2.5	8.8.8.8	0xf36e	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 22, 2021 07:43:12.588944912 CET	192.168.2.5	8.8.8.8	0xcc62	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 22, 2021 07:43:20.708695889 CET	192.168.2.5	8.8.8.8	0x2b7c	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 22, 2021 07:43:26.781378031 CET	192.168.2.5	8.8.8.8	0xab87	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 22, 2021 07:43:34.210283041 CET	192.168.2.5	8.8.8.8	0x1908	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 22, 2021 07:43:40.341476917 CET	192.168.2.5	8.8.8.8	0x23cd	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 22, 2021 07:43:47.446223974 CET	192.168.2.5	8.8.8.8	0xa681	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)
Feb 22, 2021 07:43:54.371562004 CET	192.168.2.5	8.8.8.8	0x4993	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)

DNS Answers

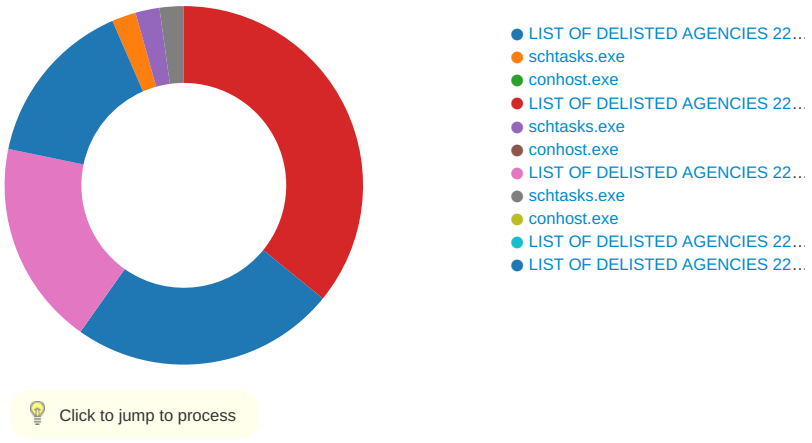
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 07:42:20.886221886 CET	8.8.8.8	192.168.2.5	0x127c	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 07:42:29.733645916 CET	8.8.8.8	192.168.2.5	0x7f3b	No error (0)	shahzad73. casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 22, 2021 07:42:36.378938913 CET	8.8.8.8	192.168.2.5	0x3447	No error (0)	shahzad73. casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 22, 2021 07:42:43.519887924 CET	8.8.8.8	192.168.2.5	0x68b5	No error (0)	shahzad73. casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 22, 2021 07:42:50.628134012 CET	8.8.8.8	192.168.2.5	0xa58a	No error (0)	shahzad73. casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 22, 2021 07:42:55.401375055 CET	8.8.8.8	192.168.2.5	0xfe4d	No error (0)	shahzad73. casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 22, 2021 07:43:00.506299019 CET	8.8.8.8	192.168.2.5	0xe5d8	No error (0)	shahzad73. casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 22, 2021 07:43:06.655592918 CET	8.8.8.8	192.168.2.5	0xf36e	No error (0)	shahzad73. casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 22, 2021 07:43:12.637726068 CET	8.8.8.8	192.168.2.5	0xcc62	No error (0)	shahzad73. casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 22, 2021 07:43:20.768855095 CET	8.8.8.8	192.168.2.5	0x2b7c	No error (0)	shahzad73. casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 22, 2021 07:43:26.829952002 CET	8.8.8.8	192.168.2.5	0xab87	No error (0)	shahzad73. casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 22, 2021 07:43:34.273186922 CET	8.8.8.8	192.168.2.5	0x1908	No error (0)	shahzad73. casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 22, 2021 07:43:40.398835897 CET	8.8.8.8	192.168.2.5	0x23cd	No error (0)	shahzad73. casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 22, 2021 07:43:47.662240982 CET	8.8.8.8	192.168.2.5	0xa681	No error (0)	shahzad73. casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 22, 2021 07:43:54.423114061 CET	8.8.8.8	192.168.2.5	0x4993	No error (0)	shahzad73. casacam.net		91.212.153.84	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe PID: 6336
Parent PID: 5760

General

Start time:	07:41:47
Start date:	22/02/2021
Path:	C:\Users\user\Desktop\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe'
Imagebase:	0xca0000
File size:	643072 bytes
MD5 hash:	988BBC4BF9B82BE5DFA915ECB1B63C49
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: 00000000.00000002.280044415.0000000004209000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.280044415.0000000004209000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.280044415.0000000004209000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.281405044.00000000046F7000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.281405044.00000000046F7000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.281405044.00000000046F7000.00000004.00000001.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	6DA5CF06	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	6DA5CF06	unknown
C:\Users\user\AppData\Roaming\FOvTZkuI.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C8A1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp9968.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C8A7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DD6C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp9968.tmp	success or wait	1	6C8A6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\FOvTZkul.exe	unknown	643072	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 03 50 10 fd 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 c6 09 00 00 08 00 00 00 00 00 00 32 e4 09 00 00 20 00 00 00 00 0a 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 0a 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....P........... ....0............2.... ....@.. ....@ ....@................	success or wait	1	6C8A1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp9968.tmp	unknown	1645	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	6C8A1B4F	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 DELISTED AGENCIES 22ND FEB 2021.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	6DD6C907	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	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA35705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA3CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8A1B4F	ReadFile
C:\Users\user\Desktop\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe	unknown	643072	success or wait	1	6C8A1B4F	ReadFile

Analysis Process: schtasks.exe PID: 6864 Parent PID: 6336

General

Start time:	07:42:12
Start date:	22/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\FOvTZkul' /XML 'C:\Users\user\AppData\Local\Temp\tmp9968.tmp'
Imagebase:	0x11a0000
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\tmp9968.tmp	unknown	2	success or wait	1	11AAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp9968.tmp	unknown	1646	success or wait	1	11AABD9	ReadFile

Analysis Process: conhost.exe PID: 6872 Parent PID: 6864

General

Start time:	07:42:12
Start date:	22/02/2021
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 DELISTED AGENCIES 22ND FEB 2021.PDF.exe PID: 6908 Parent PID: 6336

General

Start time:	07:42:13
Start date:	22/02/2021
Path:	C:\Users\user\Desktop\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x9d0000
File size:	643072 bytes
MD5 hash:	988BBC4BF9B82BE5DFA915ECB1B63C49
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: 00000007.00000002.493487439.0000000002DC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.488637501.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.488637501.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.488637501.0000000000402000.00000040.00000001.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	6DA5CF06	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	6DA5CF06	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	6C8ABEFF	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	6C8A1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp4916.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C8A7038	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	6C8A1E60	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	6C8ABEFF	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	6C8ABEFF	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	11	6C8A1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C8A1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C8A1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4916.tmp	success or wait	1	6C8A6A95	DeleteFileW
C:\Users\user\Desktop\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe:Zone.Identifier	success or wait	1	6C822935	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	a5 34 6f 6e 48 d7 d8 48	.4onH..H	success or wait	1	6C8A1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4916.tmp	unknown	1334	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	6C8A1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	71	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 44 45 4c 49 53 54 45 44 20 41 47 45 4e 43 49 45 53 20 32 32 4e 44 20 46 45 42 20 32 30 32 31 2e 50 44 46 2e 65 78 65	C:\Users\user\Desktop\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe	success or wait	1	6C8A1B4F	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	8	6C8A1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	327768	70 54 c7 ab ad 21 b0 08 57 f6 fa 47 14 4a ba aa 61 dd a0 29 17 40 c6 8b 69 8b df 77 70 4b 98 73 6f 40 e2 06 e5 35 e7 b7 3d e9 b8 90 5e ab 1d 51 82 6f 79 f9 3d 65 40 39 c3 42 8d f7 95 46 bc cb 30 39 75 22 33 8b f5 20 30 74 c0 19 52 44 6e 5f 34 64 fb b8 17 02 df 45 c0 90 06 69 f4 08 9f ae bb 8a 7e 0c 89 85 7c 87 eb 66 58 5f 0e c2 ed 58 66 88 70 5e e2 f5 ff 94 03 e5 3e 61 db 8b 91 24 8d 8a 8f 65 05 36 3a 37 64 b6 28 61 05 41 e4 fe e0 3d be 29 2a 0d 96 a8 90 8e 7b 42 1c 5b ab 87 cb 79 25 b3 2a e4 b8 b1 9f 69 a7 51 84 3c f3 94 a2 90 78 74 c4 a9 58 13 11 48 09 d7 20 ad cc a4 48 46 37 67 0f e0 c5 49 96 2a 33 03 7b 0c 6e 92 bf 90 be 4c d1 9b 79 3b 69 87 bc 73 2d 1e b6 f9 b8 28 35 69 c2 8b 92 d6 10 ac a7 02 93 ee 89 08 17 4a 09 35 62 37 7d fe 86 66 4b af ab 48 56	pT...!..W..G.J..a..).@..i..wpK .so@...5..=...^..Q.oy.=e@9 .B...F..09u"3.. 0t..RDn_4d.....E.. .i.....~...|..fX_....Xf.p^.... ..>a...$...e.6:7d.(a.A...=.)*. ....{B.[...y%.*....i.Q.<....xt ..X..H.. ...HF7g...I.*3.{.n... .L..y;i..s-....(5i..... .J.5b7}..fK..HV	success or wait	1	6C8A1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 7e 61 d3 f8 a3 01 06 96 0c a9 7e ba 7e 86 90 d9 e5 05 8d ca 33 e7 55 0b	9iH....}Z..4..f.~a.....~.~. .....3.U.	success or wait	1	6C8A1B4F	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	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA35705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA3CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8A1B4F	ReadFile
C:\Users\user\Desktop\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe	unknown	4096	success or wait	1	6DA1D72F	unknown
C:\Users\user\Desktop\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe	unknown	512	success or wait	1	6DA1D72F	unknown

Analysis Process: schtasks.exe PID: 4552 Parent PID: 6908

General

Start time:	07:42:16
Start date:	22/02/2021

Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp4916.tmp'
Imagebase:	0x11a0000
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\tmp4916.tmp	unknown	2	success or wait	1	11AAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp4916.tmp	unknown	1335	success or wait	1	11AABD9	ReadFile

Analysis Process: conhost.exe PID: 5460 Parent PID: 4552

General

Start time:	07:42:16
Start date:	22/02/2021
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 DELISTED AGENCIES 22ND FEB 2021.PDF.exe PID: 3132 Parent PID: 904

General

Start time:	07:42:19
Start date:	22/02/2021
Path:	C:\Users\user\Desktop\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe' 0
Imagebase:	0x3e0000
File size:	643072 bytes
MD5 hash:	988BBC4BF9B82BE5DFA915ECB1B63C49
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: 0000000F.00000002.352145184.0000000003859000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.352145184.0000000003859000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.352145184.0000000003859000.00000004.00000001.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	6DA5CF06	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	6DA5CF06	unknown
C:\Users\user\AppData\Local\Temp\tmpA04.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C8A7038	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA04.tmp	success or wait	1	6C8A6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA04.tmp	unknown	1645	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	6C8A1B4F	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	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA35705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA3CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8A1B4F	ReadFile

Analysis Process: schtasks.exe PID: 2196 Parent PID: 3132

General

Start time:	07:42:43
Start date:	22/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\FOvTZkul' /XML 'C:\Users\user\AppData\Local\Temp\tmpA04.tmp'
Imagebase:	0x1180000
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\tmpA04.tmp	unknown	2	success or wait	1	118AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA04.tmp	unknown	1646	success or wait	1	118ABD9	ReadFile

Analysis Process: conhost.exe PID: 5928 Parent PID: 2196

General

Start time:	07:42:44
Start date:	22/02/2021
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 DELISTED AGENCIES 22ND FEB 2021.PDF.exe PID: 1276 Parent PID: 3132

General

Start time:	07:42:44
Start date:	22/02/2021
Path:	C:\Users\user\Desktop\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x20000
File size:	643072 bytes
MD5 hash:	988BBC4BF9B82BE5DFA915ECB1B63C49
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe PID: 1236 Parent PID: 3132

General

Start time:	07:42:45
Start date:	22/02/2021
Path:	C:\Users\user\Desktop\LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x7ff797770000
File size:	643072 bytes
MD5 hash:	988BBC4BF9B82BE5DFA915ECB1B63C49
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: 00000015.00000002.365342774.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.365342774.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.365342774.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.370926802.0000000003E59000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.370926802.0000000003E59000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.370366843.0000000002E51000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.370366843.0000000002E51000.00000004.00000001.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	6DA5CF06	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	6DA5CF06	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	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA35705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA3CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9903DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9903DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA35705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8A1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8A1B4F	ReadFile

Disassembly

Code Analysis