ID: 357315
Sample Name: BILLING INVOICE.pdf.exe
Cookbook: default.jbs
Time: 12:56:18
Date: 24/02/2021
Version: 31.0.0 Emerald

Table of Contents

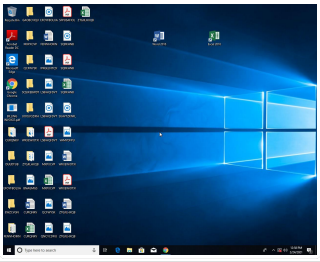
Analysis Report BILLING INVOICE.pdf.exe

Overview

General Information

Sample Name:	BILLING INVOICE.pdf.exe
Analysis ID:	357315
MD5:	2374bb6b267541..
SHA1:	143c5d4ef23ca23..
SHA256:	4c2079f57e1ecb6..
Tags:	Endurance exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

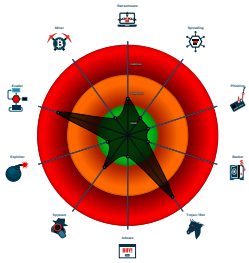
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Sigma detected: Suspicious Double …
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Executable has a suspicious name (…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …

Classification



Startup

- **System is w10x64**
- BILLING INVOICE.pdf.exe (PID: 6836 cmdline: 'C:\Users\user\Desktop\BILLING INVOICE.pdf.exe' MD5: 2374BB6B2675413F13A74466B9325B97)
  - schtasks.exe (PID: 4692 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ihNagUDDVeQ' /XML 'C:\Users\user\AppData\Local\Temp\tmp7646.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6292 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - BILLING INVOICE.pdf.exe (PID: 6552 cmdline: {path} MD5: 2374BB6B2675413F13A74466B9325B97)
    - schtasks.exe (PID: 5556 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp243E.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6556 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- BILLING INVOICE.pdf.exe (PID: 6428 cmdline: 'C:\Users\user\Desktop\BILLING INVOICE.pdf.exe' 0 MD5: 2374BB6B2675413F13A74466B9325B97)
  - schtasks.exe (PID: 7084 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ihNagUDDVeQ' /XML 'C:\Users\user\AppData\Local\Temp\tmpE53C.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7032 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - BILLING INVOICE.pdf.exe (PID: 7132 cmdline: {path} MD5: 2374BB6B2675413F13A74466B9325B97)
- **cleanup**

Malware Configuration

Threatname: NanoCore

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


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000012.00000002.483963807.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000012.00000002.483963807.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000012.00000002.483963807.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
00000012.00000002.485784066.000000000316000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000012.00000002.485784066.000000000316 1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x6942b:$a: NanoCore • 0x69484:$a: NanoCore • 0x694c1:$a: NanoCore • 0x6953a:$a: NanoCore • 0x6948d:$b: ClientPlugin • 0x694ca:$b: ClientPlugin • 0x69dc8:$b: ClientPlugin • 0x69dd5:$b: ClientPlugin • 0x5f5ae:$e: KeepAlive • 0x69915:$g: LogClientMessage • 0x69895:$i: get_Connected • 0x59861:$j: #=q • 0x59891:$j: #=q • 0x598cd:$j: #=q • 0x598f5:$j: #=q • 0x59925:$j: #=q • 0x59955:$j: #=q • 0x59985:$j: #=q • 0x599b5:$j: #=q • 0x599d1:$j: #=q • 0x59a01:$j: #=q
Click to see the 14 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
18.2.BILLING INVOICE.pdf.exe.31c964c.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
18.2.BILLING INVOICE.pdf.exe.31c964c.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
18.2.BILLING INVOICE.pdf.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
18.2.BILLING INVOICE.pdf.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
18.2.BILLING INVOICE.pdf.exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 38 entries				

Sigma Overview

System Summary:

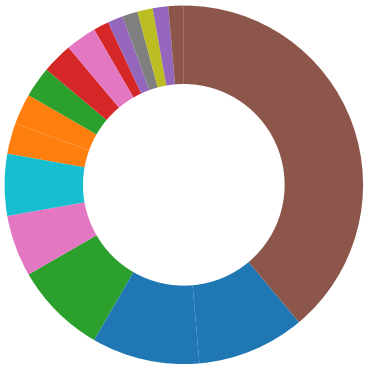
Sigma detected: NanoCore

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:

- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)
- Executable has a suspicious name (potential lure to open the executable)
- Initial sample is a PE file and has a suspicious name

Data Obfuscation:

- .NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

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

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:

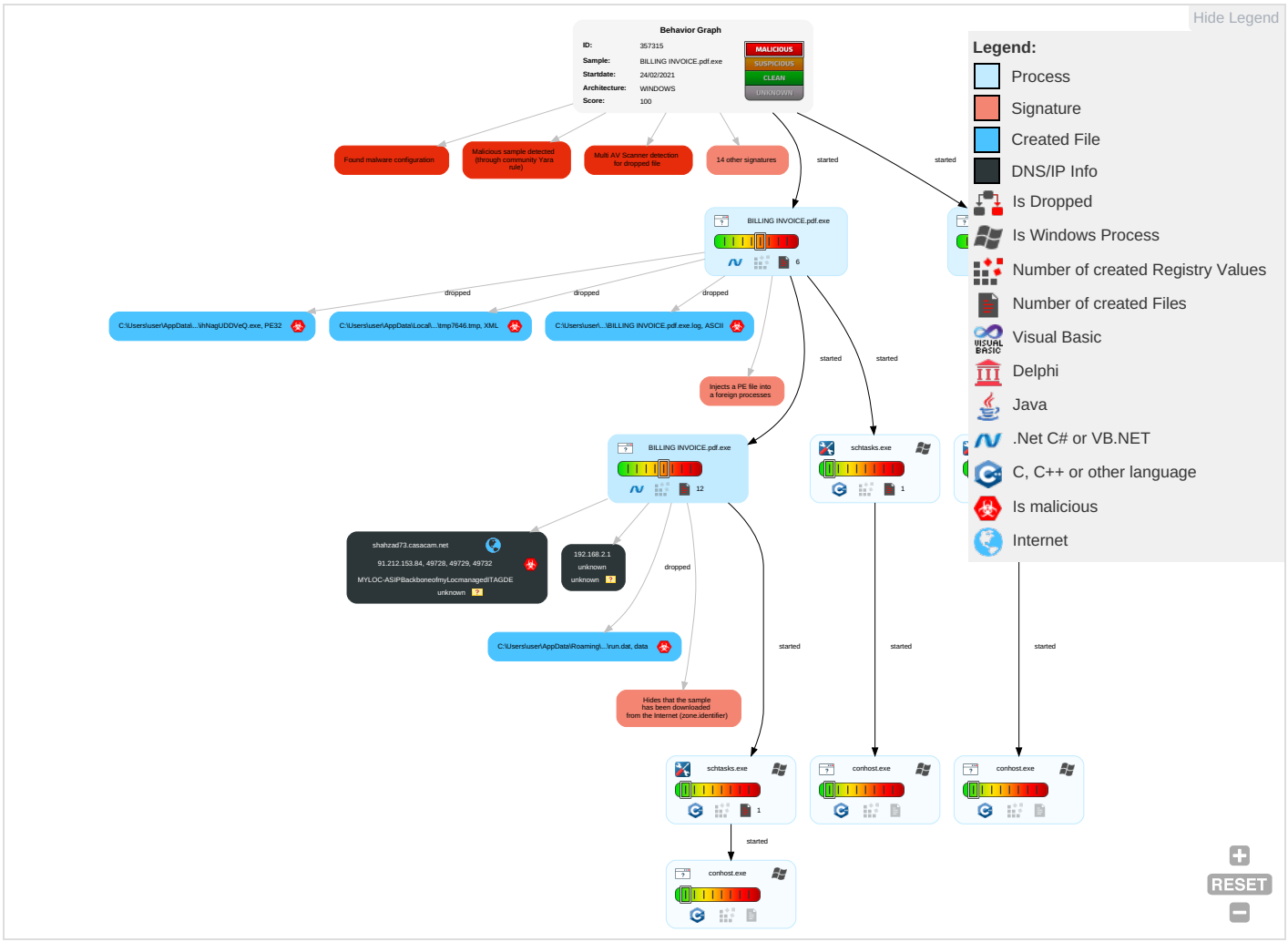
Detected Nanocore Rat

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 1	Masquerading 1 1	Input Capture 1 1	Query Registry 1	Remote Services	Input Capture 1 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 1	NTDS	Process Discovery 1	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

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
BILLING INVOICE.pdf.exe	40%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	
BILLING INVOICE.pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\ihNagUDDVeQ.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\ihNagUDDVeQ.exe	40%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
18.2.BILLING INVOICE.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.coms	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.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.fontbureau.comoitu	0%	URL Reputation	safe	
http://www.fontbureau.comoitu	0%	URL Reputation	safe	
http://www.fontbureau.comoitu	0%	URL Reputation	safe	
http://www.fontbureau.comoitu	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.fontbureau.comm	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	

Source	Detection	Scanner	Label	Link
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	
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

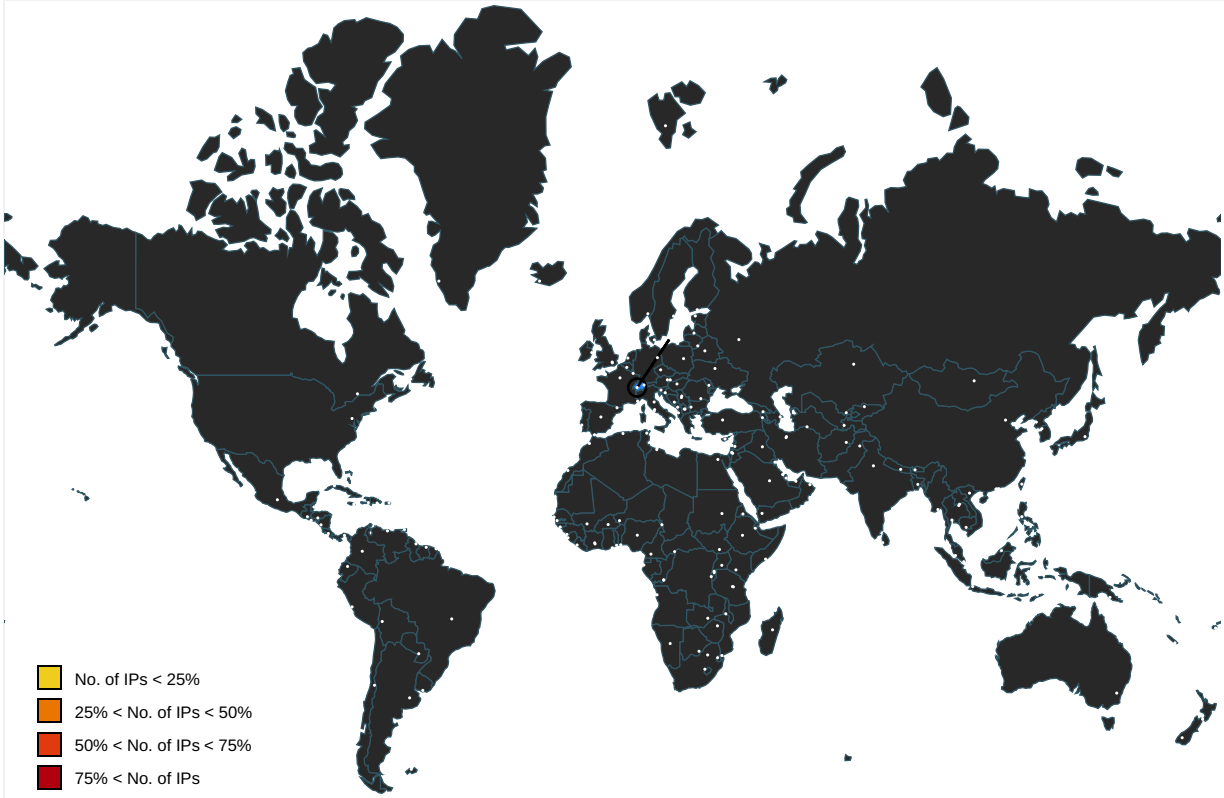
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	BILLING INVOICE.pdf.exe, 00000001.00000002.412476630.0000000006A22000.00000004.00000001.sdmp, BILLING INVOICE.pdf.exe, 0000000B.00000002.479024535.0000000000059F0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	BILLING INVOICE.pdf.exe, 00000001.00000002.412476630.0000000006A22000.00000004.00000001.sdmp, BILLING INVOICE.pdf.exe, 0000000B.00000002.479024535.0000000000059F0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	BILLING INVOICE.pdf.exe, 00000001.00000002.412476630.0000000006A22000.00000004.00000001.sdmp, BILLING INVOICE.pdf.exe, 0000000B.00000002.479024535.0000000000059F0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	BILLING INVOICE.pdf.exe, 00000001.00000002.412476630.0000000006A22000.00000004.00000001.sdmp, BILLING INVOICE.pdf.exe, 0000000B.00000002.479024535.0000000000059F0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	BILLING INVOICE.pdf.exe, 00000001.00000002.412476630.0000000006A22000.00000004.00000001.sdmp, BILLING INVOICE.pdf.exe, 0000000B.00000002.479024535.0000000000059F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.coms	BILLING INVOICE.pdf.exe, 00000001.00000003.348946561.00000000108C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	BILLING INVOICE.pdf.exe, 00000001.00000002.412476630.0000000006A22000.00000004.00000001.sdmp, BILLING INVOICE.pdf.exe, 0000000B.00000002.479024535.00000000059F0000.00000002.00000001.sdmp	false		high
http://www.tiro.com	BILLING INVOICE.pdf.exe, 00000000B.00000002.479024535.00000000059F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	BILLING INVOICE.pdf.exe, 00000000B.00000002.479024535.00000000059F0000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	BILLING INVOICE.pdf.exe, 00000001.00000002.412476630.0000000006A22000.00000004.00000001.sdmp, BILLING INVOICE.pdf.exe, 0000000B.00000002.479024535.00000000059F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	BILLING INVOICE.pdf.exe, 00000001.00000002.412476630.0000000006A22000.00000004.00000001.sdmp, BILLING INVOICE.pdf.exe, 0000000B.00000002.479024535.00000000059F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	BILLING INVOICE.pdf.exe, 00000001.00000002.412476630.0000000006A22000.00000004.00000001.sdmp, BILLING INVOICE.pdf.exe, 0000000B.00000002.479024535.00000000059F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	BILLING INVOICE.pdf.exe, 00000001.00000002.412476630.0000000006A22000.00000004.00000001.sdmp, BILLING INVOICE.pdf.exe, 0000000B.00000002.479024535.00000000059F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	BILLING INVOICE.pdf.exe, 00000001.00000002.412476630.0000000006A22000.00000004.00000001.sdmp, BILLING INVOICE.pdf.exe, 0000000B.00000002.479024535.00000000059F0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	BILLING INVOICE.pdf.exe, 00000001.00000002.412476630.0000000006A22000.00000004.00000001.sdmp, BILLING INVOICE.pdf.exe, 0000000B.00000002.479024535.00000000059F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	BILLING INVOICE.pdf.exe, 00000001.00000002.412476630.0000000006A22000.00000004.00000001.sdmp, BILLING INVOICE.pdf.exe, 0000000B.00000002.479024535.00000000059F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	BILLING INVOICE.pdf.exe, 00000001.00000002.412476630.0000000006A22000.00000004.00000001.sdmp, BILLING INVOICE.pdf.exe, 0000000B.00000002.479024535.00000000059F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	BILLING INVOICE.pdf.exe, 00000001.00000002.412476630.0000000006A22000.00000004.00000001.sdmp, BILLING INVOICE.pdf.exe, 0000000B.00000002.479024535.00000000059F0000.00000002.00000001.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/frere-jones.html	BILLING INVOICE.pdf.exe, 00000001.00000002.412476630.0000000006A22000.00000004.00000001.sdmp, BILLING INVOICE.pdf.exe, 0000000B.00000002.479024535.00000059F0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comoitu	BILLING INVOICE.pdf.exe, 00000001.00000002.400396424.0000000001087000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comm	BILLING INVOICE.pdf.exe, 00000001.00000002.400396424.0000000001087000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	BILLING INVOICE.pdf.exe, 00000001.00000002.412476630.0000000006A22000.00000004.00000001.sdmp, BILLING INVOICE.pdf.exe, 0000000B.00000002.479024535.00000059F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	BILLING INVOICE.pdf.exe, 00000001.00000002.412476630.0000000006A22000.00000004.00000001.sdmp, BILLING INVOICE.pdf.exe, 0000000B.00000002.479024535.00000059F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	BILLING INVOICE.pdf.exe, 00000001.00000002.412476630.0000000006A22000.00000004.00000001.sdmp, BILLING INVOICE.pdf.exe, 0000000B.00000002.479024535.00000059F0000.00000002.00000001.sdmp	false		high
http://www.fonts.com	BILLING INVOICE.pdf.exe, 00000001.00000002.412476630.0000000006A22000.00000004.00000001.sdmp, BILLING INVOICE.pdf.exe, 0000000B.00000002.479024535.00000059F0000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	BILLING INVOICE.pdf.exe, 00000001.00000002.412476630.0000000006A22000.00000004.00000001.sdmp, BILLING INVOICE.pdf.exe, 0000000B.00000002.479024535.00000059F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	BILLING INVOICE.pdf.exe, 00000001.00000002.412476630.0000000006A22000.00000004.00000001.sdmp, BILLING INVOICE.pdf.exe, 0000000B.00000002.479024535.00000059F0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	BILLING INVOICE.pdf.exe, 00000001.00000002.412476630.0000000006A22000.00000004.00000001.sdmp, BILLING INVOICE.pdf.exe, 0000000B.00000002.479024535.00000059F0000.00000002.00000001.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	BILLING INVOICE.pdf.exe, 00000001.00000002.400465122.0000000002841000.00000004.00000001.sdmp, BILLING INVOICE.pdf.exe, 0000000B.00000002.470826846.0000000002A91000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	BILLING INVOICE.pdf.exe, 00000001.00000002.412476630.0000000006A22000.00000004.00000001.sdmp, BILLING INVOICE.pdf.exe, 0000000B.00000002.479024535.00000059F0000.00000002.00000001.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:	357315
Start date:	24.02.2021
Start time:	12:56:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	BILLING INVOICE.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:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@15/11@14/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 89% • 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): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 51.104.139.180, 168.61.161.212, 204.79.197.200, 13.107.21.200, 23.54.113.53, 52.255.188.83, 104.42.151.234, 52.147.198.201, 51.104.144.132, 23.0.174.187, 23.0.174.185, 51.103.5.159, 23.10.249.26, 23.10.249.25, 52.155.217.156, 20.54.26.129, 95.100.54.203 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:57:25	API Interceptor	749x Sleep call for process: BILLING INVOICE.pdf.exe modified
12:57:46	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\BILLING INVOICE.pdf.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
91.212.153.84	JMG Memo-Circular No 018-21.PDF.exe	Get hash	malicious	Browse	
	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe	Get hash	malicious	Browse	
	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	JMG Memo-Circular No 018-21.PDF.exe	Get hash	malicious	Browse	• 91.212.153.84
	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA ADVISORY ON DELISTED AGENCIES.PDF.exe	Get hash	malicious	Browse	• 91.212.153.84
	Swift copy_BILLING INVOICE.pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA ADVISORY NO 450 2021.pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA DELISTED AGENCIES (BATCH A).PDF.exe	Get hash	malicious	Browse	• 91.212.153.84
	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	JMG Memo-Circular No 018-21.PDF.exe	Get hash	malicious	Browse	• 91.212.153.84
	LIST OF DELISTED AGENCIES 22ND FEB 2021.PDF.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA ADVISORY ON DELISTED AGENCIES.PDF.exe	Get hash	malicious	Browse	• 91.212.153.84
	Swift copy_BILLING INVOICE.pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA ADVISORY ON DELISTED AGENCIES.pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA ADVISORY NO 450 2021.pdf.exe	Get hash	malicious	Browse	• 91.212.153.84
	POEA DELISTED AGENCIES (BATCH A).PDF.exe	Get hash	malicious	Browse	• 91.212.153.84
	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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BILLING INVOICE.pdf.exe.log	
Process:	C:\Users\user\Desktop\BILLING INVOICE.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\tmp243E.tmp	
Process:	C:\Users\user\Desktop\BILLING INVOICE.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1312
Entropy (8bit):	5.114327114062219
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0VKZxtn:cbk4oL600QydbQxlYODOLedq3tj
MD5:	5ADF9BAA3F018F7135770CE8913A6CBE
SHA1:	0A15D3279AEC06B1428ED22191656B5704188A3A
SHA-256:	35F2AA041A3F5D5BD661018D40D331D630F2D0D6D104699591F5F41BDF8DC6DC
SHA-512:	8B4CA8D6327A664AC1782A0A401109E81078E7624385130C30F5DAB8CE062D04E0668110867EE868FE8A45DE311C87D08CE3E3B61A6F937BBAA9F84679D042EF
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\tmp7646.tmp	
Process:	C:\Users\user\Desktop\BILLING INVOICE.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1656
Entropy (8bit):	5.162410656291698
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3+qtn:cbha7JlNQV/rydbz9I3YODOLNdq3Mc
MD5:	7D606680B22EE1B5946753B87107DD2F

C:\Users\user\AppData\Local\Temp\tmp7646.tmp

SHA1:	0B0FF271AB0F95CC85B56097BD0F3FE31F5D7D34
SHA-256:	E9DF8AC1EF30AA4DFE4AE252BAA408D81391A8718F47CCFA1DCA634FE30210CE
SHA-512:	7DE94C954F99A130E6D76DE5C626A3431A0FDEB4B08D444DF2A09CF6C28B12FC5FBC4173C500ED094C3B9DA5ABFFB0CEDEF9E8BB772C3792ADED4A8B0753 58F
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

C:\Users\user\AppData\Local\Temp\tmpE53C.tmp

Process:	C:\Users\user\Desktop\BILLING INVOICE.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1656
Entropy (8bit):	5.162410656291698
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3+qtn:cbha7JlNQV/rydbz9I3YODOLNdq3Mc
MD5:	7D606680B22EE1B5946753B87107DD2F
SHA1:	0B0FF271AB0F95CC85B56097BD0F3FE31F5D7D34
SHA-256:	E9DF8AC1EF30AA4DFE4AE252BAA408D81391A8718F47CCFA1DCA634FE30210CE
SHA-512:	7DE94C954F99A130E6D76DE5C626A3431A0FDEB4B08D444DF2A09CF6C28B12FC5FBC4173C500ED094C3B9DA5ABFFB0CEDEF9E8BB772C3792ADED4A8B0753 58F
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>.. <StartWhenAvail

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

Process:	C:\Users\user\Desktop\BILLING INVOICE.pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	1856
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	48:IknjhUknjhUknjhUknjhUknjhUknjhUknjhUknjhL:HjhDjhDjhDjhDjhDjhDjhDjhL
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\BILLING INVOICE.pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:XyAn:iA
MD5:	F5C9CFE85A11961BD3AEB58399B50444
SHA1:	D7E92C41BC0CE6E0AD648E7FF08DCEDB01EAB2AB
SHA-256:	DF1CF9AF49C4A2756ED3A1B4C828C40658C2E59B0F378A4E45FA618DBD59BC87

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
SHA-512:	74C1EA3D84B1AE7812AA0B4E7FCDD86610B858E066D32F2B83A781AE1F8A290D6692C2A99B1E172B974B23B2A2910421A770D19230AB22A19F1E1B91C5B8B6A A
Malicious:	**true**
Preview:	..8....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	
Process:	C:\Users\user\Desktop\BILLING INVOICE.pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	4.501629167387823
Encrypted:	false
SSDEEP:	3:9bzY6oRDIvYk:RzWDI3
MD5:	ACD3FB4310417DC77FE06F15B0E353E6
SHA1:	80E7002E655EB5765FDEB21114295CB96AD9D5EB
SHA-256:	DC3AE604991C9BB8FF8BC4502AE3D0DB8A3317512C0F432490B103B89C1A4368
SHA-512:	DA46A917DB6276CD4528CFE4AD113292D873CA2EBE53414730F442B83502E5FAF3D1AE87BFA295ADF01E3B44FDBCE239E21A318BFB2CCD1F4753846CB21F6F 97
Malicious:	false
Preview:	9iH...}Z.4..f..J".C;"a

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\BILLING INVOICE.pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	5.320159765557392
Encrypted:	false
SSDEEP:	3:9bzY6oRDIvYVsRLY6oRDT6P2bfVn1:RzWDIfRWDT621
MD5:	BB0F9B9992809E733EFFF8B0E562CFD6
SHA1:	F0BAB3CF73A04F5A689E6AFC764FEE9276992742
SHA-256:	C48F04FE7525AA3A3F9540889883F649726233DE021724823720A59B4F37CEAC
SHA-512:	AE4280AA460DC1C0301D458A3A443F6884A0BE37481737B2ADAFD72C33C55F09BED88ED239C91FE6F19CA137AC3CD7C9B8454C21D3F8E759687F701C8B3C7A 6
Malicious:	false
Preview:	9iH...}Z.4..f..J".C;"a9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\BILLING INVOICE.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:	C08BA0E3315E2314ECBEF38722DF834C2CB8412446A9A310F41A8F83B4AC5984FCC1B26A1D8B0D58A730FDBDD885714854BDFD04DCDF7F582FC125F552D5C3 A
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...I.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....l..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\BILLING INVOICE.pdf.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	49
Entropy (8bit):	4.5043757225526235
Encrypted:	false

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
SSDEEP:	3:oNN2+WnU5Smghr:oNN2RAgt
MD5:	93C14289219843A7235690B344ADE36E
SHA1:	FF89BC91614F8ACF36ED4C203D781D6B590B1577
SHA-256:	09998F5BF070501F5208AE0AD6855E1FB7EF44ECC161944F278C634FD3992A77
SHA-512:	7A8C7758B2F130BA48F2DD84337EE951E9985FB04CEC20B4A0E7DE8DAEA9576104B07CEB8AA2F657846BD5523FEA4A6F7EBAE793087DABB763F2EC6764106667
Malicious:	false
Preview:	C:\Users\user\Desktop\BILLING INVOICE.pdf.exe

C:\Users\user\AppData\Roaming\ihNagUDDVeQ.exe	
Process:	C:\Users\user\Desktop\BILLING INVOICE.pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	381440
Entropy (8bit):	7.912703799735133
Encrypted:	false
SSDEEP:	6144:IdLOyWI+/pOD6wzzMLDOsFnWTU607u94jQBGQgwQ+6kLhokTpQmqSvtyvu:JEL6wEfOsFWTU5SmjQBG1P+d3pZX
MD5:	2374BB6B2675413F13A74466B9325B97
SHA1:	143C5D4EF23CA231614A625971788275D9DAEE44
SHA-256:	4C2079F57E1ECB6DD303D37CBE6B7E84E44D987A3FC29EF1E351EBBA9FD5CC35
SHA-512:	819782C178CD37D0668EA40CC1B8EBD7EE6154D00388D86FBA4FA608A87C633C06093AB9F9E15A3C7C947B9B4FD79116CFA260A10812789C9987D1ECFA125C8
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 40%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....5`..... .....@.. .....@..... ..@.....O..... ..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....@...\[.....g..h$.....r.(8.....r...p(7.....o;....*....0.....{.....+..*.0..*.....#.....,...}....+..#.....}....*...0.... .....{.....+..*.0..*.....#.....}....+..#.....}....*...0.....{.....+..*.0..*.....#.....,..}....+..#.....}....*...0..M.....#.....@.{.....{....ZZ#.....@.{.....{....ZZX#.....@.{..... {....ZZX.+..*....0.....{.....{....Z.{....Z.+..*...0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.912703799735133
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.98% • Win32 Executable (generic) a (10002005/4) 49.93% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	BILLING INVOICE.pdf.exe
File size:	381440
MD5:	2374bb6b2675413f13a74466b9325b97
SHA1:	143c5d4ef23ca231614a625971788275d9daee44
SHA256:	4c2079f57e1ecb6dd303d37cbe6b7e84e44d987a3fc29ef1e351ebba9fd5cc35
SHA512:	819782c178cd37d0668ea40cc1b8ebd7ee6154d00388d86fba4fa608a87c633c06093ab9f9e15a3c7c947b9b4fd79116cfa260a10812789c9987d1ecfa125cc8
SSDEEP:	6144:IdLOyWI+/pOD6wzzMLDOsFnWTU607u94jQBGQgwQ+6kLhokTpQmqSvtyvu:JEL6wEfOsFWTU5SmjQBG1P+d3pZX
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....5`..... .....@.. .....@..... ..@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x45e7ee
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:	0x60359F02 [Wed Feb 24 00:34:10 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IMPORT	0x5e79c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x60000	0x600	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x62000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x5c7f4	0x5c800	False	0.931579919764	data	7.92505185821	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x60000	0x600	0x600	False	0.442057291667	data	4.29994504602	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x62000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x60090	0x36c	data		
RT_MANIFEST	0x6040c	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

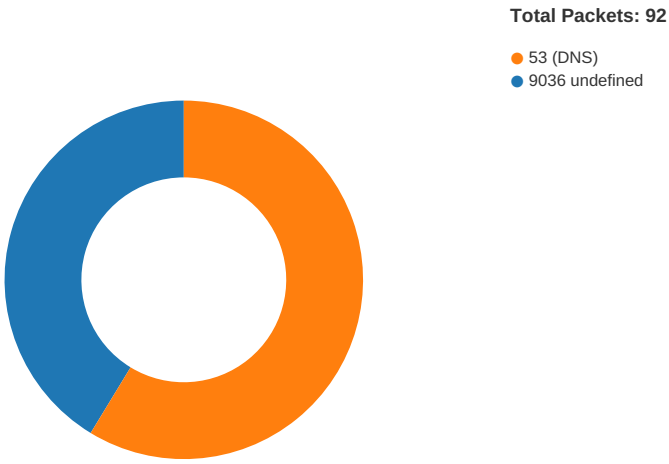
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Neudesic 2017
Assembly Version	1.0.0.0
InternalName	GH5EC.exe
FileVersion	1.0.0.0
CompanyName	Neudesic
LegalTrademarks	
Comments	
ProductName	VectorBasedDrawing
ProductVersion	1.0.0.0
FileDescription	VectorBasedDrawing
OriginalFilename	GH5EC.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 12:57:47.697957993 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:47.719449997 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:47.719549894 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:47.796598911 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:47.823239088 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:47.845339060 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:47.866569042 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:47.889058113 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:47.963701963 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:47.975496054 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:47.975543976 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:47.975574970 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:47.975583076 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:47.975621939 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:47.975651979 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:47.996611118 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:47.996642113 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:47.996665001 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:47.996686935 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:47.996707916 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:47.996723890 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:47.996745110 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:47.996756077 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:47.996777058 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:47.996787071 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:47.996808052 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:47.996869087 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:48.017303944 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.017426968 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.017452002 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.017478943 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.017505884 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.017539978 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:48.017566919 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.017590046 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.017601013 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:48.017623901 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.017636061 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:48.017653942 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.017668009 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:48.017744064 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.017767906 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.017786026 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:48.017802000 CET	9036	49728	91.212.153.84	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 12:57:48.017827988 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.017844915 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:48.018040895 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.018064976 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.018090010 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.018096924 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:48.018143892 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:48.029783010 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:48.038485050 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.038511038 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.038527966 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.038551092 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.038568020 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.038584948 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.038599968 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:48.038618088 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.038635015 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.038645029 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:48.038660049 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.038671017 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:48.038708925 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:48.038954973 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.038980007 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.038996935 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.039011955 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.039028883 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:48.039042950 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.039062977 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.039079905 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.039098024 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.039108992 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:48.039114952 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:48.039134979 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.039151907 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:48.039171934 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.039180994 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:48.039201975 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.039215088 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:48.039237022 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:48.039982080 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.040050983 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.040079117 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.040082932 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:48.040102959 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.040127039 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.040127039 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:48.040149927 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.040153980 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:48.040174961 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.040188074 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:48.040201902 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.040220022 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:48.040225029 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.040249109 CET	49728	9036	192.168.2.6	91.212.153.84
Feb 24, 2021 12:57:48.040249109 CET	9036	49728	91.212.153.84	192.168.2.6
Feb 24, 2021 12:57:48.040271044 CET	49728	9036	192.168.2.6	91.212.153.84

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 12:57:05.205404043 CET	49283	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:57:05.217932940 CET	53	49283	8.8.8.8	192.168.2.6
Feb 24, 2021 12:57:05.250516891 CET	58377	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:57:05.651149988 CET	55074	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 12:57:05.664232016 CET	53	55074	8.8.8.8	192.168.2.6
Feb 24, 2021 12:57:06.256783009 CET	58377	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:57:06.270220995 CET	53	58377	8.8.8.8	192.168.2.6
Feb 24, 2021 12:57:06.847357035 CET	54513	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:57:06.860454082 CET	53	54513	8.8.8.8	192.168.2.6
Feb 24, 2021 12:57:07.685013056 CET	62044	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:57:07.697124958 CET	53	62044	8.8.8.8	192.168.2.6
Feb 24, 2021 12:57:08.170537949 CET	63791	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:57:08.188425064 CET	53	63791	8.8.8.8	192.168.2.6
Feb 24, 2021 12:57:08.495271921 CET	64267	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:57:08.508690119 CET	53	64267	8.8.8.8	192.168.2.6
Feb 24, 2021 12:57:10.466887951 CET	49448	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:57:10.479806900 CET	53	49448	8.8.8.8	192.168.2.6
Feb 24, 2021 12:57:11.250217915 CET	60342	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:57:11.263050079 CET	53	60342	8.8.8.8	192.168.2.6
Feb 24, 2021 12:57:12.459167004 CET	61346	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:57:12.471975088 CET	53	61346	8.8.8.8	192.168.2.6
Feb 24, 2021 12:57:13.403403044 CET	51774	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:57:13.415361881 CET	53	51774	8.8.8.8	192.168.2.6
Feb 24, 2021 12:57:14.188536882 CET	56023	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:57:14.203088999 CET	53	56023	8.8.8.8	192.168.2.6
Feb 24, 2021 12:57:15.222028971 CET	58384	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:57:15.234819889 CET	53	58384	8.8.8.8	192.168.2.6
Feb 24, 2021 12:57:15.916160107 CET	60261	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:57:15.928978920 CET	53	60261	8.8.8.8	192.168.2.6
Feb 24, 2021 12:57:17.134922028 CET	56061	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:57:17.147279024 CET	53	56061	8.8.8.8	192.168.2.6
Feb 24, 2021 12:57:18.041114092 CET	58336	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:57:18.053656101 CET	53	58336	8.8.8.8	192.168.2.6
Feb 24, 2021 12:57:21.272644997 CET	53781	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:57:21.284456968 CET	53	53781	8.8.8.8	192.168.2.6
Feb 24, 2021 12:57:22.324059963 CET	54064	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:57:22.336911917 CET	53	54064	8.8.8.8	192.168.2.6
Feb 24, 2021 12:57:23.433034897 CET	52811	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:57:23.446010113 CET	53	52811	8.8.8.8	192.168.2.6
Feb 24, 2021 12:57:24.150922060 CET	55299	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:57:24.163077116 CET	53	55299	8.8.8.8	192.168.2.6
Feb 24, 2021 12:57:25.186011076 CET	63745	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:57:25.198486090 CET	53	63745	8.8.8.8	192.168.2.6
Feb 24, 2021 12:57:27.536396980 CET	50055	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:57:27.550003052 CET	53	50055	8.8.8.8	192.168.2.6
Feb 24, 2021 12:57:41.728310108 CET	61374	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:57:41.742105007 CET	53	61374	8.8.8.8	192.168.2.6
Feb 24, 2021 12:57:47.524568081 CET	50339	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:57:47.687066078 CET	53	50339	8.8.8.8	192.168.2.6
Feb 24, 2021 12:57:57.713361979 CET	63307	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:57:57.891199112 CET	53	63307	8.8.8.8	192.168.2.6
Feb 24, 2021 12:58:01.390185118 CET	49694	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:58:01.408746958 CET	53	49694	8.8.8.8	192.168.2.6
Feb 24, 2021 12:58:02.596286058 CET	54982	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:58:03.609375000 CET	54982	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:58:03.621659994 CET	53	54982	8.8.8.8	192.168.2.6
Feb 24, 2021 12:58:04.647655964 CET	50010	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:58:04.662698030 CET	53	50010	8.8.8.8	192.168.2.6
Feb 24, 2021 12:58:11.736670971 CET	63718	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:58:11.750356913 CET	53	63718	8.8.8.8	192.168.2.6
Feb 24, 2021 12:58:17.943790913 CET	62116	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:58:17.956743002 CET	53	62116	8.8.8.8	192.168.2.6
Feb 24, 2021 12:58:20.021786928 CET	63816	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:58:20.039413929 CET	53	63816	8.8.8.8	192.168.2.6
Feb 24, 2021 12:58:24.259593964 CET	55014	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:58:24.272880077 CET	53	55014	8.8.8.8	192.168.2.6
Feb 24, 2021 12:58:26.774240017 CET	62208	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:58:26.787739038 CET	53	62208	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 12:58:27.379511118 CET	57574	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:58:27.400059938 CET	53	57574	8.8.8.8	192.168.2.6
Feb 24, 2021 12:58:27.940001011 CET	51818	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:58:27.951958895 CET	53	51818	8.8.8.8	192.168.2.6
Feb 24, 2021 12:58:28.613869905 CET	56628	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:58:28.626753092 CET	53	56628	8.8.8.8	192.168.2.6
Feb 24, 2021 12:58:29.067420959 CET	60778	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:58:29.080293894 CET	53	60778	8.8.8.8	192.168.2.6
Feb 24, 2021 12:58:29.509764910 CET	53799	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:58:29.522228003 CET	53	53799	8.8.8.8	192.168.2.6
Feb 24, 2021 12:58:30.487044096 CET	54683	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:58:30.499699116 CET	53	54683	8.8.8.8	192.168.2.6
Feb 24, 2021 12:58:30.681929111 CET	59329	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:58:30.715142965 CET	53	59329	8.8.8.8	192.168.2.6
Feb 24, 2021 12:58:31.432158947 CET	64021	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:58:31.446798086 CET	53	64021	8.8.8.8	192.168.2.6
Feb 24, 2021 12:58:32.100343943 CET	56129	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:58:32.266587019 CET	53	56129	8.8.8.8	192.168.2.6
Feb 24, 2021 12:58:32.503792048 CET	58177	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:58:32.516326904 CET	53	58177	8.8.8.8	192.168.2.6
Feb 24, 2021 12:58:32.979120970 CET	50700	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:58:32.992527008 CET	53	50700	8.8.8.8	192.168.2.6
Feb 24, 2021 12:58:39.167280912 CET	54069	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:58:39.337960005 CET	53	54069	8.8.8.8	192.168.2.6
Feb 24, 2021 12:58:40.697551966 CET	61178	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:58:40.716012955 CET	53	61178	8.8.8.8	192.168.2.6
Feb 24, 2021 12:58:46.362746000 CET	57017	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:58:46.375458002 CET	53	57017	8.8.8.8	192.168.2.6
Feb 24, 2021 12:58:53.114048958 CET	56327	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:58:53.126672029 CET	53	56327	8.8.8.8	192.168.2.6
Feb 24, 2021 12:59:00.165194035 CET	50243	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:59:00.178086996 CET	53	50243	8.8.8.8	192.168.2.6
Feb 24, 2021 12:59:05.285968065 CET	62055	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:59:05.299699068 CET	53	62055	8.8.8.8	192.168.2.6
Feb 24, 2021 12:59:11.865730047 CET	61249	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:59:11.879116058 CET	53	61249	8.8.8.8	192.168.2.6
Feb 24, 2021 12:59:16.899044991 CET	65252	53	192.168.2.6	8.8.8.8
Feb 24, 2021 12:59:16.913017035 CET	53	65252	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 24, 2021 12:57:47.524568081 CET	192.168.2.6	8.8.8.8	0x11e7	Standard query (0)	shahzad73. casacam.net	A (IP address)	IN (0x0001)
Feb 24, 2021 12:57:57.713361979 CET	192.168.2.6	8.8.8.8	0x552a	Standard query (0)	shahzad73. casacam.net	A (IP address)	IN (0x0001)
Feb 24, 2021 12:58:04.647655964 CET	192.168.2.6	8.8.8.8	0xf647	Standard query (0)	shahzad73. casacam.net	A (IP address)	IN (0x0001)
Feb 24, 2021 12:58:11.736670971 CET	192.168.2.6	8.8.8.8	0xe229	Standard query (0)	shahzad73. casacam.net	A (IP address)	IN (0x0001)
Feb 24, 2021 12:58:17.943790913 CET	192.168.2.6	8.8.8.8	0xb1bb	Standard query (0)	shahzad73. casacam.net	A (IP address)	IN (0x0001)
Feb 24, 2021 12:58:24.259593964 CET	192.168.2.6	8.8.8.8	0x2f7f	Standard query (0)	shahzad73. casacam.net	A (IP address)	IN (0x0001)
Feb 24, 2021 12:58:32.100343943 CET	192.168.2.6	8.8.8.8	0x8851	Standard query (0)	shahzad73. casacam.net	A (IP address)	IN (0x0001)
Feb 24, 2021 12:58:39.167280912 CET	192.168.2.6	8.8.8.8	0x1196	Standard query (0)	shahzad73. casacam.net	A (IP address)	IN (0x0001)
Feb 24, 2021 12:58:46.362746000 CET	192.168.2.6	8.8.8.8	0x59db	Standard query (0)	shahzad73. casacam.net	A (IP address)	IN (0x0001)
Feb 24, 2021 12:58:53.114048958 CET	192.168.2.6	8.8.8.8	0x7c93	Standard query (0)	shahzad73. casacam.net	A (IP address)	IN (0x0001)
Feb 24, 2021 12:59:00.165194035 CET	192.168.2.6	8.8.8.8	0x5875	Standard query (0)	shahzad73. casacam.net	A (IP address)	IN (0x0001)
Feb 24, 2021 12:59:05.285968065 CET	192.168.2.6	8.8.8.8	0x6886	Standard query (0)	shahzad73. casacam.net	A (IP address)	IN (0x0001)
Feb 24, 2021 12:59:11.865730047 CET	192.168.2.6	8.8.8.8	0xf877	Standard query (0)	shahzad73. casacam.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 24, 2021 12:59:16.899044991 CET	192.168.2.6	8.8.8.8	0xcaa8	Standard query (0)	shahzad73.casacam.net	A (IP address)	IN (0x0001)

DNS Answers

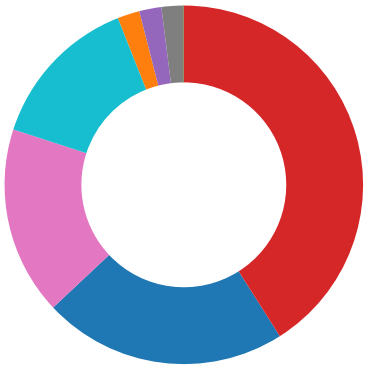
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 24, 2021 12:57:47.687066078 CET	8.8.8.8	192.168.2.6	0x11e7	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 24, 2021 12:57:57.891199112 CET	8.8.8.8	192.168.2.6	0x552a	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 24, 2021 12:58:04.662698030 CET	8.8.8.8	192.168.2.6	0xf647	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 24, 2021 12:58:11.750356913 CET	8.8.8.8	192.168.2.6	0xe229	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 24, 2021 12:58:17.956743002 CET	8.8.8.8	192.168.2.6	0xb1bb	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 24, 2021 12:58:24.272880077 CET	8.8.8.8	192.168.2.6	0x2f7f	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 24, 2021 12:58:32.266587019 CET	8.8.8.8	192.168.2.6	0x8851	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 24, 2021 12:58:39.337960005 CET	8.8.8.8	192.168.2.6	0x1196	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 24, 2021 12:58:46.375458002 CET	8.8.8.8	192.168.2.6	0x59db	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 24, 2021 12:58:53.126672029 CET	8.8.8.8	192.168.2.6	0x7c93	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 24, 2021 12:59:00.178086996 CET	8.8.8.8	192.168.2.6	0x5875	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 24, 2021 12:59:05.299699068 CET	8.8.8.8	192.168.2.6	0x6886	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 24, 2021 12:59:11.879116058 CET	8.8.8.8	192.168.2.6	0xf877	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)
Feb 24, 2021 12:59:16.913017035 CET	8.8.8.8	192.168.2.6	0xcaa8	No error (0)	shahzad73.casacam.net		91.212.153.84	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

- BILLING INVOICE.pdf.exe
- schtasks.exe
- conhost.exe
- BILLING INVOICE.pdf.exe
- schtasks.exe
- conhost.exe
- BILLING INVOICE.pdf.exe
- schtasks.exe
- conhost.exe
- BILLING INVOICE.pdf.exe



Click to jump to process

System Behavior

Analysis Process: BILLING INVOICE.pdf.exe PID: 6836 Parent PID: 5856

General

Start time:	12:57:13
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\BILLING INVOICE.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\BILLING INVOICE.pdf.exe'
Imagebase:	0x550000
File size:	381440 bytes
MD5 hash:	2374BB6B2675413F13A74466B9325B97
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: 00000001.00000002.403279843.0000000003849000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.403279843.0000000003849000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.403279843.0000000003849000.00000004.00000001.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	6DEACF06	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	6DEACF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ihNagUDDVeQ.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CCF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp7646.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CCF7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BILLING INVOICE.pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1BC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7646.tmp	success or wait	1	6CCF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ihNagUDDVeQ.exe	unknown	381440	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 02 9f 35 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 c8 05 00 00 08 00 00 00 00 00 00 ee e7 05 00 00 20 00 00 00 00 00 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 06 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.....5`.......... ....@.. ....@ ....@................	success or wait	1	6CCF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7646.tmp	unknown	1656	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </Registratio	success or wait	1	6CCF1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\BILLING INVOICE.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	6E1BC907	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	6DE85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE8CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Users\user\Desktop\BILLING INVOICE.pdf.exe	unknown	381440	success or wait	1	6CCF1B4F	ReadFile

Analysis Process: schtasks.exe PID: 4692 Parent PID: 6836

General

Start time:	12:57:40
Start date:	24/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ihNagUDDVeQ' /XML 'C:\Us ers\user\AppData\Local\Temp\tmp7646.tmp'
Imagebase:	0x1290000
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\tmp7646.tmp	unknown	2	success or wait	1	129AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7646.tmp	unknown	1657	success or wait	1	129ABD9	ReadFile

Analysis Process: conhost.exe PID: 6292 Parent PID: 4692

General

Start time:	12:57:41
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: BILLING INVOICE.pdf.exe PID: 6552 Parent PID: 6836

General

Start time:	12:57:41
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\BILLING INVOICE.pdf.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xfd0000
File size:	381440 bytes
MD5 hash:	2374BB6B2675413F13A74466B9325B97
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.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	6DEACF06	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	6DEACF06	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	6CCFBEFF	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	6CCF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp243E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CCF7038	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	6CCF1E60	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	6CCFBEFF	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	6CCFBEFF	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	13	6CCF1E60	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	6CCF1E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	2	6CCF1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CCFDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp243E.tmp	success or wait	1	6CCF6A95	DeleteFileW
C:\Users\user\Desktop\BILLING INVOICE.pdf.exe:Zone.Identifier	success or wait	1	6CC72935	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	success or wait	1	6CCF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	0c 9c 38 d5 06 d9 d8 48	..8....H	success or wait	1	6CCF1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp243E.tmp	unknown	1312	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 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 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	6CCF1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	49	43 3a 5c 55 73 65 72 73 5c 65 6e 67 69 6e 65 65 72 5c 44 65 73 6b 74 6f 70 5c 42 49 4c 4c 49 4e 47 20 49 4e 56 4f 49 43 45 2e 70 64 66 2e 65 78 65	C:\Users\user\Desktop\BILLING INVOICE.pdf.exe	success or wait	1	6CCF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc bb 8e f9 04 20 53 f0 bc 12 1c d2 7d 46 46 d4 32 d7 fe a4 68 e2 b4 4d 2b cf cc b9 c1 ec 4c bb 23 8c 58 cb ee 2b 8b b7 cd 01 a9 c0 2a c7 f9 1e d1 7e 66 1e 47 30 5e c3 a9 dd 96 3b b4 2e 95 a2 57 32 c2 3d 10 b3 ce 4b ca 7e c7 4c cc 9f 15 26 66 8d bb 2e 70 c8 04 1b f8 b7 c2 0f e9 ff e7 0b 10 3a 37 72 48 7d bd be f1 88 0d 2f 48 16 b2 87 06 17 96 4c 8c b6 04 3f b5 f3 04 41 08 4b 07 d1 e5 84 4a 17 3d 38 78 21 19 a1 e1 e4 2b fa 32 65 27 d7 1f 45 3f d9 47 11 9e a7 e7 a8 01 f0 5b 00 26	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i..... S.....}FF.2.. .h..M+.....L.#.X..+.....*.... ~f.G0^....;....W2.=...K.~.L... &f...p.....:7rH}...../H .....L...?...A.K....J.=8x!... .+.2e'..E?.G.....[.&	success or wait	8	6CCF1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	327768	70 54 c7 ab ad 21 b0 08 57 f6 fa 47 14 4a ba aa 61 dd a0 29 17 40 c6 8b 69 8b df 77 70 4b 98 73 6f 40 e2 06 e5 35 e7 b7 3d e9 b8 90 5e ab 1d 51 82 6f 79 f9 3d 65 40 39 c3 42 8d f7 95 46 bc cb 30 39 75 22 33 8b f5 20 30 74 c0 19 52 44 6e 5f 34 64 fb b8 17 02 df 45 c0 90 06 69 f4 08 9f ae bb 8a 7e 0c 89 85 7c 87 eb 66 58 5f 0e c2 ed 58 66 88 70 5e e2 f5 ff 94 03 e5 3e 61 db 8b 91 24 8d 8a 8f 65 05 36 3a 37 64 b6 28 61 05 41 e4 fe e0 3d be 29 2a 0d 96 a8 90 8e 7b 42 1c 5b ab 87 cb 79 25 b3 2a e4 b8 b1 9f 69 a7 51 84 3c f3 94 a2 90 78 74 c4 a9 58 13 11 48 09 d7 20 ad cc a4 48 46 37 67 0f e0 c5 49 96 2a 33 03 7b 0c 6e 92 bf 90 be 4c d1 9b 79 3b 69 87 bc 73 2d 1e b6 f9 b8 28 35 69 c2 8b 92 d6 10 ac a7 02 93 ee 89 08 17 4a 09 35 62 37 7d fe 86 66 4b af ab 48 56	pT...!..W..G.J..a..).@..i..wp K .so@...5..=...^..Q.oy.=e@9 .B...F..09u"3.. 0t..RDn_4d.....E.. .i.....~...|..fX_...Xf.p^.... ..>a...$...e.6:7d.(a.A...=.)*. ....{B.[...y%.*....i.Q.<....xt ..X..H.. ...HF7g...I.*3.{.n... .L..y;i..s-....(5i..... .J.5b7}..fK..HV	success or wait	1	6CCF1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	24	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d f0 4a 22 83 43 3b 22 61	9iH....}Z..4..f..J".C;"a	success or wait	2	6CCF1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	0	24	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d f0 4a 22 83 43 3b 22 61	9iH....}Z..4..f..J".C;"a	success or wait	1	6CCFDD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE85705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE8CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCF1B4F	ReadFile
C:\Users\user\Desktop\BILLING INVOICE.pdf.exe	unknown	4096	success or wait	1	6DE6D72F	unknown
C:\Users\user\Desktop\BILLING INVOICE.pdf.exe	unknown	512	success or wait	1	6DE6D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6DE6D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6DE6D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6DE6D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6DE6D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6DE6D72F	unknown

Analysis Process: schtasks.exe PID: 5556 Parent PID: 6552

General

Start time:	12:57:44
Start date:	24/02/2021
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\tmp243E.tmp'
Imagebase:	0x1290000
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\tmp243E.tmp	unknown	2	success or wait	1	129AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp243E.tmp	unknown	1313	success or wait	1	129ABD9	ReadFile

Analysis Process: conhost.exe PID: 6556 Parent PID: 5556

General

Start time:	12:57:44
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: BILLING INVOICE.pdf.exe PID: 6428 Parent PID: 936

General

Start time:	12:57:46
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\BILLING INVOICE.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\BILLING INVOICE.pdf.exe' 0
Imagebase:	0x680000
File size:	381440 bytes
MD5 hash:	2374BB6B2675413F13A74466B9325B97
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.474284915.0000000003A99000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.474284915.0000000003A99000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.474284915.0000000003A99000.00000004.00000001.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	6DEACF06	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	6DEACF06	unknown
C:\Users\user\AppData\Local\Temp\tmpE53C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CCF7038	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE53C.tmp	success or wait	1	6CCF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE53C.tmp	unknown	1656	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </Registratio	success or wait	1	6CCF1B4F	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	6DE85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE8CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCF1B4F	ReadFile

Analysis Process: schtasks.exe PID: 7084 Parent PID: 6428

General

Start time:	12:58:09
Start date:	24/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ihNagUDDVeQ' /XML 'C:\Users\user\AppData\Local\Temp\tmpE53C.tmp'
Imagebase:	0x1290000
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\tmpE53C.tmp	unknown	2	success or wait	1	129AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE53C.tmp	unknown	1657	success or wait	1	129ABD9	ReadFile

Analysis Process: conhost.exe PID: 7032 Parent PID: 7084

General

Start time:	12:58:11
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: BILLING INVOICE.pdf.exe PID: 7132 Parent PID: 6428

General

Start time:	12:58:12
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\BILLING INVOICE.pdf.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xdd0000
File size:	381440 bytes
MD5 hash:	2374BB6B2675413F13A74466B9325B97
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: 00000012.00000002.483963807.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.483963807.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.483963807.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.485784066.0000000003161000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.485784066.0000000003161000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.485969919.0000000004169000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.485969919.0000000004169000.00000004.00000001.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	6DEACF06	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	6DEACF06	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	6DE85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE85705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE8CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE85705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCF1B4F	ReadFile

Disassembly

Code Analysis