ID: 342227
Sample Name: company profile.scr
Cookbook: default.jbs
Time: 17:09:39
Date: 20/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

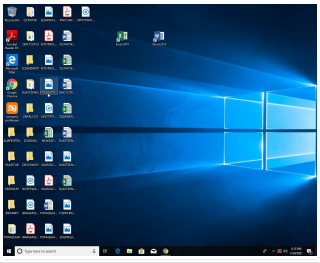
Analysis Report company profile.scr

Overview

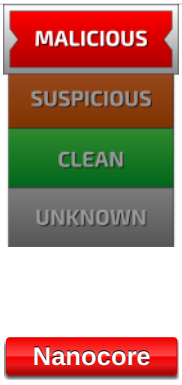
General Information

Sample Name:	company profile.scr (renamed file extension from scr to exe)
Analysis ID:	342227
MD5:	02f3eef9da2ef90…
SHA1:	6bca96158d7228..
SHA256:	76ffd919e86b374..
Tags:	NanoCore RAT scr

Most interesting Screenshot:



Detection



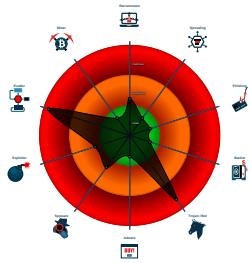
Nanocore

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

Signatures

- Detected Nanocore Rat
- Detected unpacking (changes PE se…
- 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…
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Contains functionality to check if a d…

Classification



Startup

- **System is w10x64**
- company profile.exe (PID: 5960 cmdline: 'C:\Users\user\Desktop\company profile.exe' MD5: 02F3EEF9DA2EF90D0CF59BFACA176886)
  - schtasks.exe (PID: 5976 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\UnShSbgF' /XML 'C:\Users\user\AppData\Local\Temp\tmp75B1.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 2212 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - company profile.exe (PID: 204 cmdline: {path} MD5: 02F3EEF9DA2EF90D0CF59BFACA176886)
  - company profile.exe (PID: 2540 cmdline: {path} MD5: 02F3EEF9DA2EF90D0CF59BFACA176886)
  - company profile.exe (PID: 6080 cmdline: {path} MD5: 02F3EEF9DA2EF90D0CF59BFACA176886)
    - schtasks.exe (PID: 5864 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp132E.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5636 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- company profile.exe (PID: 4920 cmdline: 'C:\Users\user\Desktop\company profile.exe' 0 MD5: 02F3EEF9DA2EF90D0CF59BFACA176886)
  - schtasks.exe (PID: 6368 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\UnShSbgF' /XML 'C:\Users\user\AppData\Local\Temp\tmpCFD7.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6376 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - company profile.exe (PID: 6412 cmdline: {path} MD5: 02F3EEF9DA2EF90D0CF59BFACA176886)
  - company profile.exe (PID: 6420 cmdline: {path} MD5: 02F3EEF9DA2EF90D0CF59BFACA176886)
  - company profile.exe (PID: 6440 cmdline: {path} MD5: 02F3EEF9DA2EF90D0CF59BFACA176886)
  - company profile.exe (PID: 6456 cmdline: {path} MD5: 02F3EEF9DA2EF90D0CF59BFACA176886)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "C2: ": [
    "105.112.102.172"
  ],
  "Version: ": "NanoCore Client, Version=1.2.2.0"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.586154490.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000006.00000002.586154490.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000006.00000002.586154490.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
0000000B.00000002.309768585.0000000002DB3000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0000000B.00000002.312703625.0000000003CE1000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x144bd:$x1: NanoCore.ClientPluginHost • 0x144fa:$x2: IClientNetworkHost • 0x1802d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Click to see the 41 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.company profile.exe.6840000.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
6.2.company profile.exe.6840000.5.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
6.2.company profile.exe.6840000.5.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
25.2.company profile.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
25.2.company profile.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

Click to see the 11 entries

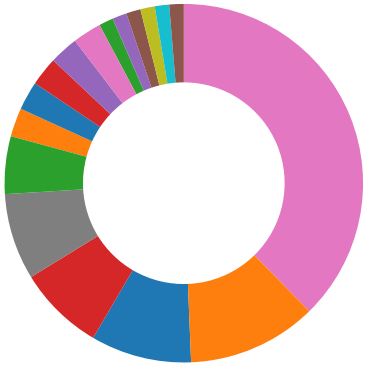
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for 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
- Uses dynamic DNS services

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)
- PE file contains section with special chars
- PE file has nameless sections

Data Obfuscation:

- Detected unpacking (changes PE section rights)
- .NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

Anti Debugging:

Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

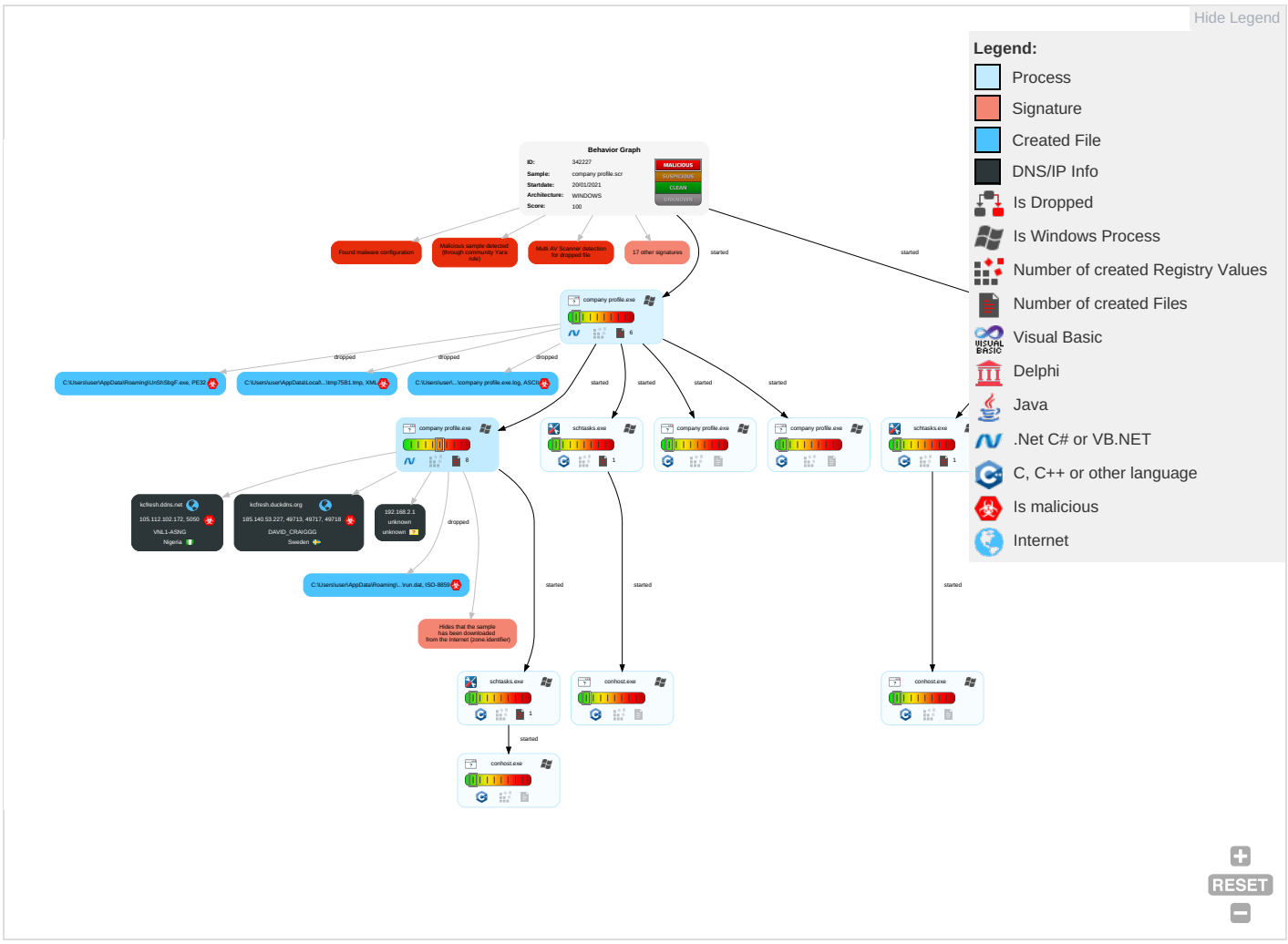
Detected Nanocore Rat

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	Network Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 2	Masquerading 1	Input Capture 1 1	Security Software Discovery 3 2 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdro Insecure Network Commun
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 4	LSASS Memory	Virtualization/Sandbox Evasion 4	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Manipula Device Commun
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocols

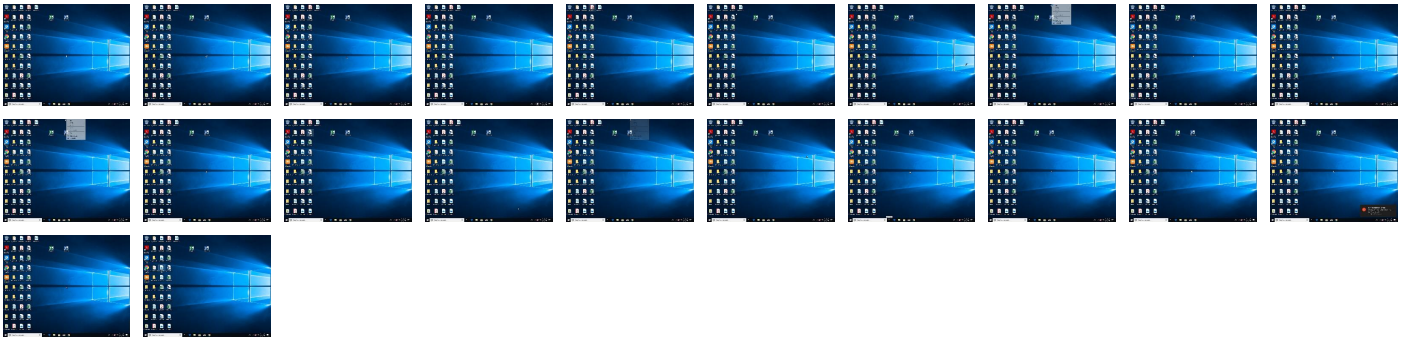
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
company profile.exe	34%	Virustotal		Browse
company profile.exe	38%	ReversingLabs	Win32.Trojan.Wacatac	
company profile.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\UnShSbgF.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\UnShSbgF.exe	34%	Virustotal		Browse
C:\Users\user\AppData\Roaming\UnShSbgF.exe	38%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.company profile.exe.850000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
25.2.company profile.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.2.company profile.exe.6840000.5.unpack	100%	Avira	TR/NanoCore.fadte		Download File
6.2.company profile.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
1.2.company profile.exe.ec0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
kcfresh.duckdns.org	1%	Virustotal		Browse
kcfresh.ddns.net	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kcfresh.duckdns.org	185.140.53.227	true	true	• 1%, Virustotal, Browse	unknown
kcfresh.ddns.net	105.112.102.172	true	true	• 3%, Virustotal, Browse	unknown

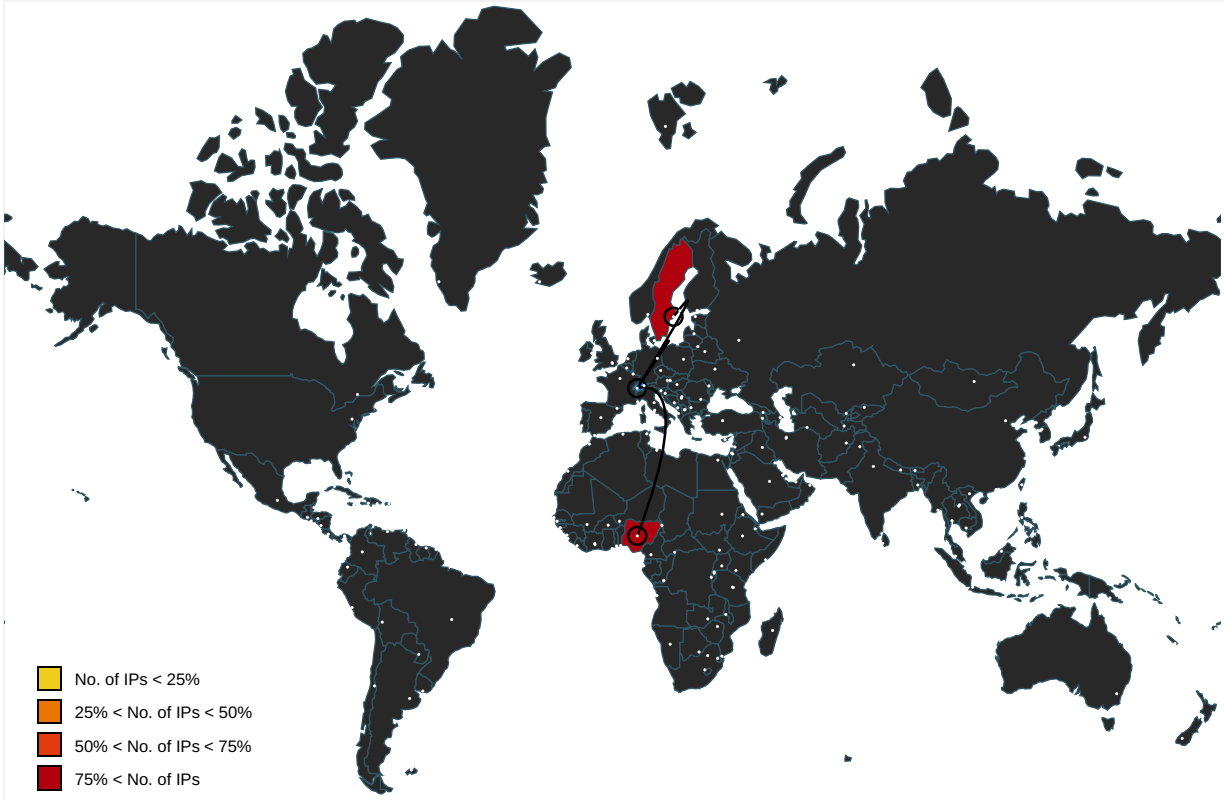
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	company profile.exe, 00000001.00000002.261375523.000000000CE02000.00000004.00000001.sdmp, company profile.exe, 0000000B.00000002.317231994.000000000B520000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	company profile.exe, 00000001.00000002.261375523.000000000CE02000.00000004.00000001.sdmp, company profile.exe, 0000000B.00000002.317231994.000000000B520000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	company profile.exe, 00000001.00000002.261375523.000000000CE02000.00000004.00000001.sdmp, company profile.exe, 0000000B.00000002.317231994.000000000B520000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	company profile.exe, 00000001.00000002.261375523.000000000CE02000.00000004.00000001.sdmp, company profile.exe, 0000000B.00000002.317231994.000000000B520000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	company profile.exe, 00000001.00000002.261375523.000000000CE02000.00000004.00000001.sdmp, company profile.exe, 0000000B.00000002.317231994.000000000B520000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	company profile.exe, 00000001.00000002.261375523.000000000CE02000.00000004.00000001.sdmp, company profile.exe, 0000000B.00000002.317231994.000000000B520000.00000002.00000001.sdmp	false		high
http://www.tiro.com	company profile.exe, 0000000B.00000002.317231994.000000000B520000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	company profile.exe, 0000000B.00000002.317231994.000000000B520000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	company profile.exe, 00000001.00000002.261375523.000000000CE02000.00000004.00000001.sdmp, company profile.exe, 0000000B.00000002.317231994.000000000B520000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	company profile.exe, 00000001.00000002.261375523.000000000CE02000.00000004.00000001.sdmp, company profile.exe, 0000000B.00000002.317231994.000000000B520000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	company profile.exe, 00000001.00000002.261375523.000000000CE02000.00000004.00000001.sdmp, company profile.exe, 0000000B.00000002.317231994.000000000B520000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	company profile.exe, 00000001.00000002.261375523.000000000CE02000.00000004.00000001.sdmp, company profile.exe, 0000000B.00000002.317231994.000000000B520000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	company profile.exe, 00000001.00000002.261375523.000000000CE02000.00000004.00000001.sdmp, company profile.exe, 0000000B.00000002.317231994.000000000B520000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	company profile.exe, 00000001.00000002.261375523.000000000CE02000.00000004.00000001.sdmp, company profile.exe, 0000000B.00000002.317231994.000000000B520000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	company profile.exe, 00000001.00000002.261375523.000000000CE02000.00000004.00000001.sdmp, company profile.exe, 0000000B.00000002.317231994.000000000B520000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	company profile.exe, 00000001.00000002.261375523.000000000CE02000.00000004.00000001.sdmp, company profile.exe, 0000000B.00000002.317231994.000000000B520000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	company profile.exe, 00000001.00000002.261375523.000000000CE02000.00000004.00000001.sdmp, company profile.exe, 0000000B.00000002.317231994.000000000B520000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	company profile.exe, 00000001.00000002.261375523.000000000CE02000.00000004.00000001.sdmp, company profile.exe, 0000000B.00000002.317231994.000000000B520000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	company profile.exe, 00000001.00000002.261375523.000000000CE02000.00000004.00000001.sdmp, company profile.exe, 0000000B.00000002.317231994.000000000B520000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	company profile.exe, 00000001.00000002.261375523.000000000CE02000.00000004.00000001.sdmp, company profile.exe, 0000000B.00000002.317231994.000000000B520000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	company profile.exe, 00000001.00000002.261375523.000000000CE02000.00000004.00000001.sdmp, company profile.exe, 0000000B.00000002.317231994.000000000B520000.00000002.00000001.sdmp	false		high
http://www.fonts.com	company profile.exe, 00000001.00000002.261375523.000000000CE02000.00000004.00000001.sdmp, company profile.exe, 0000000B.00000002.317231994.000000000B520000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	company profile.exe, 00000001.00000002.261375523.000000000CE02000.00000004.00000001.sdmp, company profile.exe, 0000000B.00000002.317231994.000000000B520000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	company profile.exe, 00000001.00000002.261375523.000000000CE02000.00000004.00000001.sdmp, company profile.exe, 0000000B.00000002.317231994.000000000B520000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cn	company profile.exe, 00000001.00000002.261375523.000000000CE02000.00000004.00000001.sdmp, company profile.exe, 0000000B.00000002.317231994.000000000B520000.00000002.00000001.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	company profile.exe, 00000001.00000002.252392608.0000000003407000.00000004.00000001.sdmp, company profile.exe, 0000000B.00000002.309406249.0000000002D27000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	company profile.exe, 00000001.00000002.261375523.000000000CE02000.00000004.00000001.sdmp, company profile.exe, 0000000B.00000002.317231994.000000000B520000.00000002.00000001.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
185.140.53.227	unknown	Sweden		209623	DAVID_CRAIGGG	true
105.112.102.172	unknown	Nigeria		36873	VNL1-ASNG	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	342227
Start date:	20.01.2021

Start time:	17:09:39
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	company profile.scr (renamed file extension from scr to 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:	40
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@25/7@16/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.1% (good quality ratio 1.1%) • Quality average: 30.7% • Quality standard deviation: 34.6%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 13.88.21.125, 104.42.151.234, 23.210.248.85, 51.104.144.132, 8.248.147.254, 8.248.115.254, 8.253.204.121, 67.27.157.126, 67.27.159.126, 20.54.26.129, 92.122.213.194, 92.122.213.247, 51.104.139.180, 52.155.217.156 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, arc.msn.com.nsatc.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, ris.api.iris.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, au-bg-shim.trafficmanager.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:12:42	API Interceptor	1305x Sleep call for process: company profile.exe modified
17:12:54	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\company profile.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.140.53.227	New Order.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	NEWORDERrefno0992883jpg.exe	Get hash	malicious	Browse	• 185.140.53.253
	richiealvin.exe	Get hash	malicious	Browse	• 91.193.75.185
	Quotation.exe	Get hash	malicious	Browse	• 185.140.53.154
	DHL Delivery Shipping Cargo. Pdf.exe	Get hash	malicious	Browse	• 185.244.30.18
	CompanyLicense.exe	Get hash	malicious	Browse	• 185.140.53.253
	Purchase Order 2094742424.exe	Get hash	malicious	Browse	• 185.244.30.132
	PURCHASE OREDER. PRINT. pdf.exe	Get hash	malicious	Browse	• 91.193.75.45
	PO.exe	Get hash	malicious	Browse	• 185.140.53.234
	SWIFT.exe	Get hash	malicious	Browse	• 185.140.53.154
	SecuriteInfo.com.BScope.Trojan-Dropper.Injector.exe	Get hash	malicious	Browse	• 185.140.53.234
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 185.140.53.131
	Orden n.#U00ba STL21119, pdf.exe	Get hash	malicious	Browse	• 185.140.53.129
	Proof of Payment.exe	Get hash	malicious	Browse	• 185.244.30.51
	DxCHoDnNLn.exe	Get hash	malicious	Browse	• 185.140.53.202
	T7gzTHDZ7g.rtf	Get hash	malicious	Browse	• 185.140.53.202
	PO - 2021-000511.exe	Get hash	malicious	Browse	• 185.244.30.69
	PO AR483-1590436 _ J-3000 PROJT.xlsx	Get hash	malicious	Browse	• 185.140.53.202
	Qotation.exe	Get hash	malicious	Browse	• 185.140.53.154
	PO - 2021-000511.exe	Get hash	malicious	Browse	• 185.244.30.69
	file.exe	Get hash	malicious	Browse	• 91.193.75.155
VNL1-ASNG	Order_List_PO# 081929.exe	Get hash	malicious	Browse	• 105.112.102.160
	Doc#6620200947535257653.exe	Get hash	malicious	Browse	• 105.112.102.162
	Doc#6620200947535257653.exe	Get hash	malicious	Browse	• 105.112.106.128
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 105.112.113.90
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 105.112.113.90
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 105.112.113.90
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 105.112.113.90
	Confirmation Copy RefNo-MT102.exe	Get hash	malicious	Browse	• 105.112.102.57
	FedExs AWB#5305323204643.exe	Get hash	malicious	Browse	• 105.112.113.90
	PAYMENT COPY.exe	Get hash	malicious	Browse	• 105.112.109.37
	PO456789.exe	Get hash	malicious	Browse	• 105.112.96.12
	DHL_10177_R293_DOCUMENT.exe	Get hash	malicious	Browse	• 105.112.101.201
	ibgcrnNmhB.exe	Get hash	malicious	Browse	• 105.112.25.130
	purchase order.exe	Get hash	malicious	Browse	• 105.112.25.74
	packing list.xlsx.exe	Get hash	malicious	Browse	• 105.112.69.142
	9087654.exe	Get hash	malicious	Browse	• 105.112.101.151
	RFQ.exe	Get hash	malicious	Browse	• 105.112.100.239
	LOI.exe	Get hash	malicious	Browse	• 105.112.100.239
	corporate-tax.exe	Get hash	malicious	Browse	• 105.112.101.84
	QUOTATION - COVID 19 PROTECTION SOLUTIONS - final.exe	Get hash	malicious	Browse	• 105.112.124.8

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\company profile.exe.log

Process:	C:\Users\user\Desktop\company profile.exe
File Type:	ASCII text, with CRLF line terminators

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\company profile.exe.log	
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:ML9E4Ks29E4Kx1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MxHKX9HKx1qHiYHKhQnoPtHoxHhAHKzr
MD5:	B666A4404B132B2BF6C04FBF848EB948
SHA1:	D2EFB3D43F8B8806544D3A47F7DAEE8534981739
SHA-256:	7870616D981C8C0DE9A54E7383CD035470DB20CBF75ACDF729C32889D4B6ED96
SHA-512:	00E955EE9F14CEAE07E571A8EF2E103200CF421BAE83A66ED9F9E1AA6A9F449B653EDF1BFDB662A364D58ECF9B5FE4BB69D590DB2653F2F46A09F4D47719A862
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",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\tmp132E.tmp	
Process:	C:\Users\user\Desktop\company profile.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1305
Entropy (8bit):	5.095160776157076
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK00lxtn:cbk4oL600QydbQxIYODOLedq37j
MD5:	4F99D40B064D2DF7C7D4C116C77F3D4A
SHA1:	7A3169F99997B406FEA127C0B9A7E8D6ACE00CA1
SHA-256:	13EA833AE6E2760DE9D70F0B3AB442CCA6DF2240206120DAE783F66147778B30
SHA-512:	E7064B43AF7C38D18CAF462524D2A8A2DC3CF93DD4CBE5495AD5762D81365EE26C4CB54AAAA387A6C25D3151F264183926AF46C9684CC07F039AF780F571488
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\tmp75B1.tmp	
Process:	C:\Users\user\Desktop\company profile.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1641
Entropy (8bit):	5.186538159731165
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBEItn:cbh47TlNQ//rydbz9I3YODOLNdq3j
MD5:	5D4EB8C36D9B89226BDC5ADB52FDDFC0
SHA1:	AF597C7A4A7C686AFFAF2482DB75417D5F92315D
SHA-256:	93466395E1FD944F5ED9AFD1063E0B46CE6CA6F8CF5CE0E89BD2CE049862175F
SHA-512:	7C7B7AFD07D5444A373CE4113F200C1BBCA840399D473EC144562B51174D404B1442A660E63CA47BA6C83492BC676839852C80157F2503B2FAD9A1C92B81D95A
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmpCFD7.tmp	
Process:	C:\Users\user\Desktop\company profile.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Temp\tmpCFD7.tmp	
Size (bytes):	1641
Entropy (8bit):	5.186538159731165
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBEItn:cbh47TlNQ//rydbz9I3YODOLNdq3j
MD5:	5D4EB8C36D9B89226BDC5ADB52FDDFC0
SHA1:	AF597C7A4A7C686AFFAF2482DB75417D5F92315D
SHA-256:	93466395E1FD944F5ED9AFD1063E0B46CE6CA6F8CF5CE0E89BD2CE049862175F
SHA-512:	7C7B7AFD07D5444A373CE4113F200C1BBCA840399D473EC144562B51174D404B1442A660E63CA47BA6C83492BC676839852C80157F2503B2FAD9A1C92B81D95A
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\company profile.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:reCYP:KCYP
MD5:	8B9C7557FD06FFDB6AB44F46DC5604D4
SHA1:	D1E1B759695E4473A8241ED6FD686B085DE6AC9B
SHA-256:	B7BB0299B1B8D42CABBA97A91C9AB732DEBDE40B8D5CA84904C938AB443F3ABC
SHA-512:	A9BDE3F3F6DE9608AE9FA5BC4422BB4735BC6540482DC8D74DD87DCB2F400D52BBCDE5F685A11D21758CCDC0266C08C4F6CECCCF7CE96D570A4E81DA6BCC2E3
Malicious:	**true**
Preview:	d.{....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\company profile.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	42
Entropy (8bit):	4.424955744609936
Encrypted:	false
SSDEEP:	3:oNWXp5vGKIVE4XoJ:oNWXpFGTiJ
MD5:	97913E49D175BDD85E9DF3F71519605F
SHA1:	B6D8C0E8D4888A71AE16529A5332A745D2F6E6FB
SHA-256:	C46B23847096F56A5952D29B05027728B48DB4B1B98A804CBEF9B88659CD5D2B
SHA-512:	77916F0BF82170A6398C251FF77A578741039D9D03915EE83BA374F6E0FD09BF550AAAE0B91277FBF21F5B91709AF5D987C0D566960488E93E2A64E46AAA5833
Malicious:	false
Preview:	C:\Users\user\Desktop\company profile.exe

C:\Users\user\AppData\Roaming\UnShSbgF.exe	
Process:	C:\Users\user\Desktop\company profile.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1499648
Entropy (8bit):	7.424594248821242
Encrypted:	false
SSDEEP:	24576:Wb8xxR5pV+4Xd8LO6TVz7uxgHf8JnHkDasy:E8f7jWdTVei/OHkDq
MD5:	02F3EEF9DA2EF90D0CF59BFACA176886
SHA1:	6BCA96158D72284A8B5A9E1FE01EB8504A1A05FF
SHA-256:	76FFD919E86B374004BCBC276CB6E18BE4B63287D0CE6F7D9B1B756BFD79D47E
SHA-512:	CE64211FA30C6C1F8541D8889E0E373A829ABD4E786B1EF6B473E851E9E7CF7C5109D0B2F85936494D4D3125CF63FFC6A282C75E1A34CDCF052111753AC3574
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 34%, Browse • Antivirus: ReversingLabs, Detection: 38%

C:\Users\user\AppData\Roaming\UnShSbgF.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....0.....@..... ....@.. .....`..... ..@.....K....`..... .....@.....H.....EMP;.s.bPD... ...F.....@....text.....J..... ..`.rsr c.....`.....&.....@..@.reloc..... .....@..B.....@..... ..`..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.424594248821242
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.96% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	company profile.exe
File size:	1499648
MD5:	02f3eef9da2ef90d0cf59bfaca176886
SHA1:	6bca96158d72284a8b5a9e1fe01eb8504a1a05ff
SHA256:	76ffd919e86b374004bcbc276cb6e18be4b63287d0ce6f7d9b1b756bfd79d47e
SHA512:	ce64211fa30c6c1f8541d8889e0e373a829abd4e786b1ef6b473e851e9e7cf7c5109d0b2f85936494d4d3125cf63ffc6a282c75e1a34cdcf052111753ac35747
SSDEEP:	24576:Wb8xxR5pV+4Xd8LO6TVz7uxgHf8JnHkDasy:E8f7jWdTVei/OHkDq
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....0.....@..... ....@.. .....`.....@.....

File Icon

Icon Hash:	926cd8b0b4d24f92

Static PE Info

General

Entrypoint:	0x57400a
Entrypoint Section:	
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:	0x6007DFD9 [Wed Jan 20 07:46:33 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 [00574000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xf8890	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x156000	0x1b788	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x172000	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	0x174000	0x8	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0xf8000	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
EMP;sb	0x2000	0xf4450	0xf4600	False	1.00031569693	data	7.99980466465	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.text	0xf8000	0x5dae8	0x5dc00	False	0.2996171875	data	4.37913403496	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x156000	0x1b788	0x1b800	False	0.186780894886	data	3.43599224394	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x172000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
	0x174000	0x10	0x200	False	0.044921875	data	0.142635768149	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x156220	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x156688	0x2ad0	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x159158	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 3892081920, next used block 3187504384		
RT_ICON	0x15b700	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4294866176, next used block 4294866176		
RT_ICON	0x15c7a8	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x16cfd0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 670987520, next used block 0		
RT_GROUP_ICON	0x1711f8	0x5a	data		
RT_VERSION	0x171254	0x342	data		
RT_MANIFEST	0x171598	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 Hewlett-Packard 2016
Assembly Version	46.3.0.0
InternalName	8v.exe
FileVersion	46.3.0.0
CompanyName	Hewlett-Packard
LegalTrademarks	
Comments	
ProductName	
ProductVersion	46.3.0.0
FileDescription	
OriginalFilename	8v.exe

Network Behavior

Network Port Distribution

Total Packets: 100

- 53 (DNS)
- 5050 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 17:12:53.951412916 CET	49713	5050	192.168.2.3	185.140.53.227
Jan 20, 2021 17:12:54.000073910 CET	5050	49713	185.140.53.227	192.168.2.3
Jan 20, 2021 17:12:54.504492998 CET	49713	5050	192.168.2.3	185.140.53.227
Jan 20, 2021 17:12:54.553361893 CET	5050	49713	185.140.53.227	192.168.2.3
Jan 20, 2021 17:12:55.064599037 CET	49713	5050	192.168.2.3	185.140.53.227
Jan 20, 2021 17:12:55.113152027 CET	5050	49713	185.140.53.227	192.168.2.3
Jan 20, 2021 17:12:59.254609108 CET	49717	5050	192.168.2.3	185.140.53.227
Jan 20, 2021 17:12:59.303097963 CET	5050	49717	185.140.53.227	192.168.2.3
Jan 20, 2021 17:12:59.830631971 CET	49717	5050	192.168.2.3	185.140.53.227
Jan 20, 2021 17:12:59.879139900 CET	5050	49717	185.140.53.227	192.168.2.3
Jan 20, 2021 17:13:00.493585110 CET	49717	5050	192.168.2.3	185.140.53.227
Jan 20, 2021 17:13:00.542746067 CET	5050	49717	185.140.53.227	192.168.2.3
Jan 20, 2021 17:13:04.674650908 CET	49718	5050	192.168.2.3	185.140.53.227
Jan 20, 2021 17:13:04.723083019 CET	5050	49718	185.140.53.227	192.168.2.3
Jan 20, 2021 17:13:05.331134081 CET	49718	5050	192.168.2.3	185.140.53.227
Jan 20, 2021 17:13:05.379919052 CET	5050	49718	185.140.53.227	192.168.2.3
Jan 20, 2021 17:13:06.034282923 CET	49718	5050	192.168.2.3	185.140.53.227
Jan 20, 2021 17:13:06.083101034 CET	5050	49718	185.140.53.227	192.168.2.3
Jan 20, 2021 17:13:10.632256985 CET	49721	5050	192.168.2.3	105.112.102.172
Jan 20, 2021 17:13:13.659883976 CET	49721	5050	192.168.2.3	105.112.102.172
Jan 20, 2021 17:13:19.676093102 CET	49721	5050	192.168.2.3	105.112.102.172
Jan 20, 2021 17:13:27.459836960 CET	49725	5050	192.168.2.3	105.112.102.172
Jan 20, 2021 17:13:30.473774910 CET	49725	5050	192.168.2.3	105.112.102.172
Jan 20, 2021 17:13:36.489917994 CET	49725	5050	192.168.2.3	105.112.102.172
Jan 20, 2021 17:13:44.849807978 CET	49733	5050	192.168.2.3	105.112.102.172
Jan 20, 2021 17:13:47.850276947 CET	49733	5050	192.168.2.3	105.112.102.172
Jan 20, 2021 17:13:53.850784063 CET	49733	5050	192.168.2.3	105.112.102.172
Jan 20, 2021 17:14:01.686594963 CET	49742	5050	192.168.2.3	185.140.53.227
Jan 20, 2021 17:14:01.735313892 CET	5050	49742	185.140.53.227	192.168.2.3
Jan 20, 2021 17:14:02.242161989 CET	49742	5050	192.168.2.3	185.140.53.227
Jan 20, 2021 17:14:02.291104078 CET	5050	49742	185.140.53.227	192.168.2.3
Jan 20, 2021 17:14:02.804785967 CET	49742	5050	192.168.2.3	185.140.53.227
Jan 20, 2021 17:14:02.853647947 CET	5050	49742	185.140.53.227	192.168.2.3
Jan 20, 2021 17:14:06.974219084 CET	49743	5050	192.168.2.3	185.140.53.227
Jan 20, 2021 17:14:07.023099899 CET	5050	49743	185.140.53.227	192.168.2.3
Jan 20, 2021 17:14:07.523895979 CET	49743	5050	192.168.2.3	185.140.53.227
Jan 20, 2021 17:14:07.572540045 CET	5050	49743	185.140.53.227	192.168.2.3
Jan 20, 2021 17:14:08.086697102 CET	49743	5050	192.168.2.3	185.140.53.227
Jan 20, 2021 17:14:08.135360956 CET	5050	49743	185.140.53.227	192.168.2.3
Jan 20, 2021 17:14:12.538840055 CET	49744	5050	192.168.2.3	185.140.53.227
Jan 20, 2021 17:14:12.587572098 CET	5050	49744	185.140.53.227	192.168.2.3
Jan 20, 2021 17:14:13.102432966 CET	49744	5050	192.168.2.3	185.140.53.227
Jan 20, 2021 17:14:13.151457071 CET	5050	49744	185.140.53.227	192.168.2.3
Jan 20, 2021 17:14:13.665100098 CET	49744	5050	192.168.2.3	185.140.53.227

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 17:14:13.713771105 CET	5050	49744	185.140.53.227	192.168.2.3
Jan 20, 2021 17:14:17.888115883 CET	49745	5050	192.168.2.3	105.112.102.172
Jan 20, 2021 17:14:20.884325981 CET	49745	5050	192.168.2.3	105.112.102.172
Jan 20, 2021 17:14:26.900515079 CET	49745	5050	192.168.2.3	105.112.102.172
Jan 20, 2021 17:14:34.720561028 CET	49748	5050	192.168.2.3	105.112.102.172
Jan 20, 2021 17:14:37.729413986 CET	49748	5050	192.168.2.3	105.112.102.172
Jan 20, 2021 17:14:43.729974031 CET	49748	5050	192.168.2.3	105.112.102.172
Jan 20, 2021 17:14:51.353595972 CET	49749	5050	192.168.2.3	105.112.102.172
Jan 20, 2021 17:14:54.355807066 CET	49749	5050	192.168.2.3	105.112.102.172
Jan 20, 2021 17:15:00.356338024 CET	49749	5050	192.168.2.3	105.112.102.172
Jan 20, 2021 17:15:08.322185040 CET	49750	5050	192.168.2.3	185.140.53.227
Jan 20, 2021 17:15:08.370486021 CET	5050	49750	185.140.53.227	192.168.2.3
Jan 20, 2021 17:15:08.872690916 CET	49750	5050	192.168.2.3	185.140.53.227
Jan 20, 2021 17:15:08.921380043 CET	5050	49750	185.140.53.227	192.168.2.3
Jan 20, 2021 17:15:09.435206890 CET	49750	5050	192.168.2.3	185.140.53.227
Jan 20, 2021 17:15:09.483859062 CET	5050	49750	185.140.53.227	192.168.2.3
Jan 20, 2021 17:15:13.769426107 CET	49751	5050	192.168.2.3	185.140.53.227
Jan 20, 2021 17:15:13.818001032 CET	5050	49751	185.140.53.227	192.168.2.3
Jan 20, 2021 17:15:14.326442003 CET	49751	5050	192.168.2.3	185.140.53.227
Jan 20, 2021 17:15:14.374986887 CET	5050	49751	185.140.53.227	192.168.2.3
Jan 20, 2021 17:15:14.893300056 CET	49751	5050	192.168.2.3	185.140.53.227
Jan 20, 2021 17:15:14.942029953 CET	5050	49751	185.140.53.227	192.168.2.3
Jan 20, 2021 17:15:19.113058090 CET	49757	5050	192.168.2.3	185.140.53.227
Jan 20, 2021 17:15:19.161782980 CET	5050	49757	185.140.53.227	192.168.2.3
Jan 20, 2021 17:15:19.686198950 CET	49757	5050	192.168.2.3	185.140.53.227
Jan 20, 2021 17:15:19.734893084 CET	5050	49757	185.140.53.227	192.168.2.3
Jan 20, 2021 17:15:20.288041115 CET	49757	5050	192.168.2.3	185.140.53.227
Jan 20, 2021 17:15:20.336539984 CET	5050	49757	185.140.53.227	192.168.2.3
Jan 20, 2021 17:15:24.561131954 CET	49763	5050	192.168.2.3	105.112.102.172
Jan 20, 2021 17:15:27.711155891 CET	49763	5050	192.168.2.3	105.112.102.172
Jan 20, 2021 17:15:33.727176905 CET	49763	5050	192.168.2.3	105.112.102.172

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 17:12:30.115456104 CET	60152	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:12:30.171864986 CET	53	60152	8.8.8.8	192.168.2.3
Jan 20, 2021 17:12:31.108071089 CET	57544	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:12:31.164551973 CET	53	57544	8.8.8.8	192.168.2.3
Jan 20, 2021 17:12:33.920929909 CET	55984	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:12:33.971705914 CET	53	55984	8.8.8.8	192.168.2.3
Jan 20, 2021 17:12:36.327366114 CET	64185	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:12:36.375221014 CET	53	64185	8.8.8.8	192.168.2.3
Jan 20, 2021 17:12:37.282816887 CET	65110	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:12:37.330900908 CET	53	65110	8.8.8.8	192.168.2.3
Jan 20, 2021 17:12:47.214193106 CET	58361	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:12:47.262096882 CET	53	58361	8.8.8.8	192.168.2.3
Jan 20, 2021 17:12:48.410496950 CET	63492	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:12:48.461219072 CET	53	63492	8.8.8.8	192.168.2.3
Jan 20, 2021 17:12:50.876347065 CET	60831	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:12:50.926973104 CET	53	60831	8.8.8.8	192.168.2.3
Jan 20, 2021 17:12:52.303313971 CET	60100	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:12:52.362260103 CET	53	60100	8.8.8.8	192.168.2.3
Jan 20, 2021 17:12:53.715147018 CET	53195	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:12:53.936311007 CET	53	53195	8.8.8.8	192.168.2.3
Jan 20, 2021 17:12:57.024483919 CET	50141	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:12:57.085048914 CET	53	50141	8.8.8.8	192.168.2.3
Jan 20, 2021 17:12:59.203219891 CET	53023	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:12:59.251117945 CET	53	53023	8.8.8.8	192.168.2.3
Jan 20, 2021 17:13:04.612528086 CET	49563	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:13:04.668864012 CET	53	49563	8.8.8.8	192.168.2.3
Jan 20, 2021 17:13:06.832524061 CET	51352	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:13:06.880430937 CET	53	51352	8.8.8.8	192.168.2.3
Jan 20, 2021 17:13:10.573229074 CET	59349	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 17:13:10.630872011 CET	53	59349	8.8.8.8	192.168.2.3
Jan 20, 2021 17:13:15.194449902 CET	57084	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:13:16.192384958 CET	57084	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:13:16.240313053 CET	53	57084	8.8.8.8	192.168.2.3
Jan 20, 2021 17:13:24.219270945 CET	58823	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:13:24.267188072 CET	53	58823	8.8.8.8	192.168.2.3
Jan 20, 2021 17:13:26.721561909 CET	57568	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:13:26.769531012 CET	53	57568	8.8.8.8	192.168.2.3
Jan 20, 2021 17:13:27.398511887 CET	50540	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:13:27.457781076 CET	53	50540	8.8.8.8	192.168.2.3
Jan 20, 2021 17:13:27.945595026 CET	54366	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:13:27.993823051 CET	53	54366	8.8.8.8	192.168.2.3
Jan 20, 2021 17:13:30.246763945 CET	53034	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:13:30.294702053 CET	53	53034	8.8.8.8	192.168.2.3
Jan 20, 2021 17:13:31.382765055 CET	57762	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:13:31.430870056 CET	53	57762	8.8.8.8	192.168.2.3
Jan 20, 2021 17:13:32.011482954 CET	55435	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:13:32.082386971 CET	53	55435	8.8.8.8	192.168.2.3
Jan 20, 2021 17:13:32.660548925 CET	50713	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:13:32.711457014 CET	53	50713	8.8.8.8	192.168.2.3
Jan 20, 2021 17:13:35.258546114 CET	56132	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:13:35.309422970 CET	53	56132	8.8.8.8	192.168.2.3
Jan 20, 2021 17:13:36.446857929 CET	58987	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:13:36.494741917 CET	53	58987	8.8.8.8	192.168.2.3
Jan 20, 2021 17:13:44.700119019 CET	56579	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:13:44.757843018 CET	53	56579	8.8.8.8	192.168.2.3
Jan 20, 2021 17:13:45.841614962 CET	60633	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:13:45.889656067 CET	53	60633	8.8.8.8	192.168.2.3
Jan 20, 2021 17:13:51.571892023 CET	61292	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:13:51.629636049 CET	53	61292	8.8.8.8	192.168.2.3
Jan 20, 2021 17:14:01.463038921 CET	63619	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:14:01.684941053 CET	53	63619	8.8.8.8	192.168.2.3
Jan 20, 2021 17:14:06.915060997 CET	64938	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:14:06.971584082 CET	53	64938	8.8.8.8	192.168.2.3
Jan 20, 2021 17:14:12.313934088 CET	61946	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:14:12.535736084 CET	53	61946	8.8.8.8	192.168.2.3
Jan 20, 2021 17:14:17.765189886 CET	64910	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:14:17.825486898 CET	53	64910	8.8.8.8	192.168.2.3
Jan 20, 2021 17:14:21.005423069 CET	52123	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:14:21.056504965 CET	53	52123	8.8.8.8	192.168.2.3
Jan 20, 2021 17:14:23.060621977 CET	56130	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:14:23.119894981 CET	53	56130	8.8.8.8	192.168.2.3
Jan 20, 2021 17:14:34.662410975 CET	56338	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:14:34.718652010 CET	53	56338	8.8.8.8	192.168.2.3
Jan 20, 2021 17:14:51.294055939 CET	59420	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:14:51.350522041 CET	53	59420	8.8.8.8	192.168.2.3
Jan 20, 2021 17:15:07.953716993 CET	58784	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:15:08.320425987 CET	53	58784	8.8.8.8	192.168.2.3
Jan 20, 2021 17:15:13.571491957 CET	63978	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:15:13.628048897 CET	53	63978	8.8.8.8	192.168.2.3
Jan 20, 2021 17:15:16.234194040 CET	62938	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:15:16.310164928 CET	53	62938	8.8.8.8	192.168.2.3
Jan 20, 2021 17:15:16.842221975 CET	55708	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:15:16.903183937 CET	53	55708	8.8.8.8	192.168.2.3
Jan 20, 2021 17:15:17.525993109 CET	56803	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:15:17.582118034 CET	53	56803	8.8.8.8	192.168.2.3
Jan 20, 2021 17:15:18.020863056 CET	57145	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:15:18.077400923 CET	53	57145	8.8.8.8	192.168.2.3
Jan 20, 2021 17:15:18.668761969 CET	55359	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:15:18.727881908 CET	53	55359	8.8.8.8	192.168.2.3
Jan 20, 2021 17:15:19.055500031 CET	58306	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:15:19.111709118 CET	53	58306	8.8.8.8	192.168.2.3
Jan 20, 2021 17:15:19.295212030 CET	64124	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:15:19.343066931 CET	53	64124	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 20, 2021 17:15:19.796638966 CET	49361	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:15:19.852883101 CET	53	49361	8.8.8.8	192.168.2.3
Jan 20, 2021 17:15:20.430563927 CET	63150	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:15:20.486757994 CET	53	63150	8.8.8.8	192.168.2.3
Jan 20, 2021 17:15:21.181947947 CET	53279	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:15:21.232682943 CET	53	53279	8.8.8.8	192.168.2.3
Jan 20, 2021 17:15:21.677417994 CET	56881	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:15:21.733674049 CET	53	56881	8.8.8.8	192.168.2.3
Jan 20, 2021 17:15:24.502064943 CET	53642	53	192.168.2.3	8.8.8.8
Jan 20, 2021 17:15:24.559706926 CET	53	53642	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 20, 2021 17:12:53.715147018 CET	192.168.2.3	8.8.8.8	0x8479	Standard query (0)	kcfresh.duckdns.org	A (IP address)	IN (0x0001)
Jan 20, 2021 17:12:59.203219891 CET	192.168.2.3	8.8.8.8	0xe3ae	Standard query (0)	kcfresh.duckdns.org	A (IP address)	IN (0x0001)
Jan 20, 2021 17:13:04.612528086 CET	192.168.2.3	8.8.8.8	0x8ef4	Standard query (0)	kcfresh.duckdns.org	A (IP address)	IN (0x0001)
Jan 20, 2021 17:13:10.573229074 CET	192.168.2.3	8.8.8.8	0xe472	Standard query (0)	kcfresh.ddns.net	A (IP address)	IN (0x0001)
Jan 20, 2021 17:13:27.398511887 CET	192.168.2.3	8.8.8.8	0xca6e	Standard query (0)	kcfresh.ddns.net	A (IP address)	IN (0x0001)
Jan 20, 2021 17:13:44.700119019 CET	192.168.2.3	8.8.8.8	0x351d	Standard query (0)	kcfresh.ddns.net	A (IP address)	IN (0x0001)
Jan 20, 2021 17:14:01.463038921 CET	192.168.2.3	8.8.8.8	0x94d4	Standard query (0)	kcfresh.duckdns.org	A (IP address)	IN (0x0001)
Jan 20, 2021 17:14:06.915060997 CET	192.168.2.3	8.8.8.8	0xc850	Standard query (0)	kcfresh.duckdns.org	A (IP address)	IN (0x0001)
Jan 20, 2021 17:14:12.313934088 CET	192.168.2.3	8.8.8.8	0x9af0	Standard query (0)	kcfresh.duckdns.org	A (IP address)	IN (0x0001)
Jan 20, 2021 17:14:17.765189886 CET	192.168.2.3	8.8.8.8	0x8715	Standard query (0)	kcfresh.ddns.net	A (IP address)	IN (0x0001)
Jan 20, 2021 17:14:34.662410975 CET	192.168.2.3	8.8.8.8	0x70d	Standard query (0)	kcfresh.ddns.net	A (IP address)	IN (0x0001)
Jan 20, 2021 17:14:51.294055939 CET	192.168.2.3	8.8.8.8	0x5b8e	Standard query (0)	kcfresh.ddns.net	A (IP address)	IN (0x0001)
Jan 20, 2021 17:15:07.953716993 CET	192.168.2.3	8.8.8.8	0x40c7	Standard query (0)	kcfresh.duckdns.org	A (IP address)	IN (0x0001)
Jan 20, 2021 17:15:13.571491957 CET	192.168.2.3	8.8.8.8	0x7292	Standard query (0)	kcfresh.duckdns.org	A (IP address)	IN (0x0001)
Jan 20, 2021 17:15:19.055500031 CET	192.168.2.3	8.8.8.8	0x5a57	Standard query (0)	kcfresh.duckdns.org	A (IP address)	IN (0x0001)
Jan 20, 2021 17:15:24.502064943 CET	192.168.2.3	8.8.8.8	0x377b	Standard query (0)	kcfresh.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

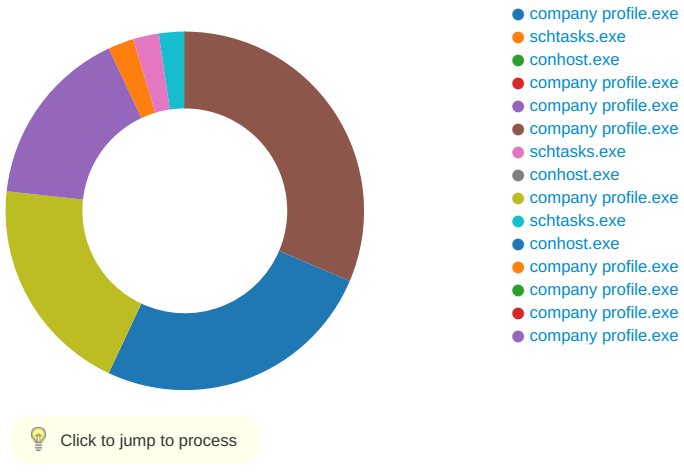
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 20, 2021 17:12:53.936311007 CET	8.8.8.8	192.168.2.3	0x8479	No error (0)	kcfresh.duckdns.org		185.140.53.227	A (IP address)	IN (0x0001)
Jan 20, 2021 17:12:59.251117945 CET	8.8.8.8	192.168.2.3	0xe3ae	No error (0)	kcfresh.duckdns.org		185.140.53.227	A (IP address)	IN (0x0001)
Jan 20, 2021 17:13:04.668864012 CET	8.8.8.8	192.168.2.3	0x8ef4	No error (0)	kcfresh.duckdns.org		185.140.53.227	A (IP address)	IN (0x0001)
Jan 20, 2021 17:13:10.630872011 CET	8.8.8.8	192.168.2.3	0xe472	No error (0)	kcfresh.ddns.net		105.112.102.172	A (IP address)	IN (0x0001)
Jan 20, 2021 17:13:27.457781076 CET	8.8.8.8	192.168.2.3	0xca6e	No error (0)	kcfresh.ddns.net		105.112.102.172	A (IP address)	IN (0x0001)
Jan 20, 2021 17:13:44.757843018 CET	8.8.8.8	192.168.2.3	0x351d	No error (0)	kcfresh.ddns.net		105.112.102.172	A (IP address)	IN (0x0001)
Jan 20, 2021 17:14:01.684941053 CET	8.8.8.8	192.168.2.3	0x94d4	No error (0)	kcfresh.duckdns.org		185.140.53.227	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 20, 2021 17:14:06.971584082 CET	8.8.8.8	192.168.2.3	0xc850	No error (0)	kcfresh.duckdns.org		185.140.53.227	A (IP address)	IN (0x0001)
Jan 20, 2021 17:14:12.535736084 CET	8.8.8.8	192.168.2.3	0x9af0	No error (0)	kcfresh.duckdns.org		185.140.53.227	A (IP address)	IN (0x0001)
Jan 20, 2021 17:14:17.825486898 CET	8.8.8.8	192.168.2.3	0x8715	No error (0)	kcfresh.ddns.net		105.112.102.172	A (IP address)	IN (0x0001)
Jan 20, 2021 17:14:34.718652010 CET	8.8.8.8	192.168.2.3	0x70d	No error (0)	kcfresh.ddns.net		105.112.102.172	A (IP address)	IN (0x0001)
Jan 20, 2021 17:14:51.350522041 CET	8.8.8.8	192.168.2.3	0x5b8e	No error (0)	kcfresh.ddns.net		105.112.102.172	A (IP address)	IN (0x0001)
Jan 20, 2021 17:15:08.320425987 CET	8.8.8.8	192.168.2.3	0x40c7	No error (0)	kcfresh.duckdns.org		185.140.53.227	A (IP address)	IN (0x0001)
Jan 20, 2021 17:15:13.628048897 CET	8.8.8.8	192.168.2.3	0x7292	No error (0)	kcfresh.duckdns.org		185.140.53.227	A (IP address)	IN (0x0001)
Jan 20, 2021 17:15:19.111709118 CET	8.8.8.8	192.168.2.3	0x5a57	No error (0)	kcfresh.duckdns.org		185.140.53.227	A (IP address)	IN (0x0001)
Jan 20, 2021 17:15:24.559706926 CET	8.8.8.8	192.168.2.3	0x377b	No error (0)	kcfresh.ddns.net		105.112.102.172	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: company profile.exe PID: 5960 Parent PID: 5652

General

Start time:	17:12:32
Start date:	20/01/2021

Path:	C:\Users\user\Desktop\company profile.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\company profile.exe'
Imagebase:	0xec0000
File size:	1499648 bytes
MD5 hash:	02F3EEF9DA2EF90D0CF59BFACA176886
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.252435267.000000000341D000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.253304124.00000000043C1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.253304124.00000000043C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.253304124.00000000043C1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.253470598.0000000004415000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.253470598.0000000004415000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.253470598.0000000004415000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	unknown
C:\Users\user\AppData\Roaming\UnShSbgF.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CEF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp75B1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CEF7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\company profile.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3BC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp75B1.tmp	success or wait	1	6CEF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\UnShSbgF.exe	unknown	1499648	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 05 00 d9 df 07 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 de 05 00 00 00 11 00 00 00 00 00 0a 40 17 00 00 80 0f 00 00 20 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 60 17 00 00 04 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......`.......... ....0..............@....... ....@.. .......................` ....@................	success or wait	1	6CEF1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp75B1.tmp	unknown	1641	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	6CEF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\company profile.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 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 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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.Windows.Forms, Vers	success or wait	1	6E3BC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Users\user\Desktop\company profile.exe	unknown	1499648	success or wait	1	6CEF1B4F	ReadFile

Analysis Process: schtasks.exe PID: 5976 Parent PID: 5960

General

Start time:	17:12:45
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\UnShSbgF' /XML 'C:\Users\user\AppData\Local\Temp\tmp75B1.tmp'
Imagebase:	0x1310000
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\tmp75B1.tmp	unknown	2	success or wait	1	131AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp75B1.tmp	unknown	1642	success or wait	1	131ABD9	ReadFile

Analysis Process: conhost.exe PID: 2212 Parent PID: 5976

General

Start time:	17:12:46
Start date:	20/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: company profile.exe PID: 204 Parent PID: 5960

General

Start time:	17:12:47
Start date:	20/01/2021
Path:	C:\Users\user\Desktop\company profile.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x2f0000
File size:	1499648 bytes
MD5 hash:	02F3EEF9DA2EF90D0CF59BFACA176886
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: company profile.exe PID: 2540 Parent PID: 5960

General

Start time:	17:12:48
Start date:	20/01/2021
Path:	C:\Users\user\Desktop\company profile.exe

Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x1d0000
File size:	1499648 bytes
MD5 hash:	02F3EEF9DA2EF90D0CF59BFACA176886
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: company profile.exe PID: 6080 Parent PID: 5960

General

Start time:	17:12:48
Start date:	20/01/2021
Path:	C:\Users\user\Desktop\company profile.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xdb0000
File size:	1499648 bytes
MD5 hash:	02F3EEF9DA2EF90D0CF59BFACA176886
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: 00000006.00000002.586154490.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.586154490.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.586154490.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.590173141.00000000031E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.594725698.0000000004229000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.594725698.0000000004229000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.596680972.0000000005BD0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.596680972.0000000005BD0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.597017105.0000000006840000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.597017105.0000000006840000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.597017105.0000000006840000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CEFBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CEF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp132E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CEF7038	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CEF1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CEFBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CEFBEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp132E.tmp	success or wait	1	6CEF6A95	DeleteFileW
C:\Users\user\Desktop\company profile.exe:Zone.Identifier	success or wait	1	6CE72935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	64 f8 7b ac a9 bd d8 48	d.{....H	success or wait	1	6CEF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp132E.tmp	unknown	1305	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	6CEF1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	42	43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 44 65 73 6b 74 6f 70 5c 63 6f 6d 70 61 6e 79 20 70 72 6f 66 69 6c 65 2e 65 78 65	C:\Users\user\Desktop\company profile.exe	success or wait	1	6CEF1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Users\user\Desktop\company profile.exe	unknown	4096	success or wait	1	6E06D72F	unknown
C:\Users\user\Desktop\company profile.exe	unknown	512	success or wait	1	6E06D72F	unknown

Analysis Process: schtasks.exe PID: 5864 Parent PID: 6080

General

Start time:	17:12:51
Start date:	20/01/2021

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\tmp132E.tmp'
Imagebase:	0xb90000
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\tmp132E.tmp	unknown	2	success or wait	1	B9AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp132E.tmp	unknown	1306	success or wait	1	B9ABD9	ReadFile

Analysis Process: conhost.exe PID: 5636 Parent PID: 5864

General

Start time:	17:12:51
Start date:	20/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: company profile.exe PID: 4920 Parent PID: 528

General

Start time:	17:12:54
Start date:	20/01/2021
Path:	C:\Users\user\Desktop\company profile.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\company profile.exe' 0
Imagebase:	0x850000
File size:	1499648 bytes
MD5 hash:	02F3EEF9DA2EF90D0CF59BFACA176886
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000B.00000002.309768585.0000000002DB3000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.312703625.0000000003CE1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.312703625.0000000003CE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.312703625.0000000003CE1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.312777066.0000000003D37000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.312777066.0000000003D37000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.312777066.0000000003D37000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	unknown
C:\Users\user\AppData\Local\Temp\tmpCFD7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CEF7038	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpCFD7.tmp	success or wait	1	6CEF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpCFD7.tmp	unknown	1641	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	6CEF1B4F	WriteFile

File Read

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

Analysis Process: schtasks.exe PID: 6368 Parent PID: 4920

General

Start time:	17:13:12
Start date:	20/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\UnShSbgF' /XML 'C:\Users\user\AppData\Local\Temp\tmpCFD7.tmp'
Imagebase:	0xb90000
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\tmpCFD7.tmp	unknown	2	success or wait	1	B9AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpCFD7.tmp	unknown	1642	success or wait	1	B9ABD9	ReadFile

Analysis Process: conhost.exe PID: 6376 Parent PID: 6368

General

Start time:	17:13:13
Start date:	20/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: company profile.exe PID: 6412 Parent PID: 4920

General

Start time:	17:13:13
Start date:	20/01/2021
Path:	C:\Users\user\Desktop\company profile.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x3b0000
File size:	1499648 bytes
MD5 hash:	02F3EEF9DA2EF90D0CF59BFACA176886
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: company profile.exe PID: 6420 Parent PID: 4920

General

Start time:	17:13:14
Start date:	20/01/2021
Path:	C:\Users\user\Desktop\company profile.exe
Wow64 process (32bit):	false

Commandline:	{path}
Imagebase:	0x3d0000
File size:	1499648 bytes
MD5 hash:	02F3EEF9DA2EF90D0CF59BFACA176886
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: company profile.exe PID: 6440 Parent PID: 4920

General

Start time:	17:13:15
Start date:	20/01/2021
Path:	C:\Users\user\Desktop\company profile.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0xf0000
File size:	1499648 bytes
MD5 hash:	02F3EEF9DA2EF90D0CF59BFACA176886
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: company profile.exe PID: 6456 Parent PID: 4920

General

Start time:	17:13:15
Start date:	20/01/2021
Path:	C:\Users\user\Desktop\company profile.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x570000
File size:	1499648 bytes
MD5 hash:	02F3EEF9DA2EF90D0CF59BFACA176886
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000002.329006639.0000000003AA9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000002.329006639.0000000003AA9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000002.328915349.0000000002AA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000002.328915349.0000000002AA1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000019.00000002.327635694.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000002.327635694.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000002.327635694.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

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

File Read

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

Disassembly

Code Analysis