ID: 402423
Sample Name:
cd61fe0ebfe9f6326cd5a4df9747e72c.exe
Cookbook: default.jbs
Time: 06:12:09
Date: 03/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

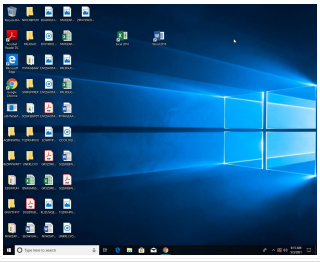
Analysis Report cd61fe0ebfe9f6326cd5a4df9747e72c.exe

Overview

General Information

Sample Name:	cd61fe0ebfe9f6326cd5a4df9747e72c.exe
Analysis ID:	402423
MD5:	cafe59d79e00e21.
SHA1:	d7fbfd97e93dec7..
SHA256:	4b603d683f97520.
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

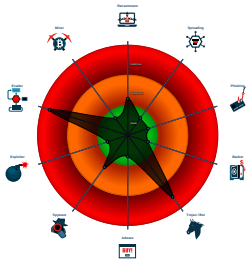
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…

Classification



Startup

- **System is w10x64**
- cd61fe0ebfe9f6326cd5a4df9747e72c.exe (PID: 5644 cmdline: 'C:\Users\user\Desktop\cd61fe0ebfe9f6326cd5a4df9747e72c.exe' MD5: CAFE59D79E00E211548D5E569931E70E)
  - cd61fe0ebfe9f6326cd5a4df9747e72c.exe (PID: 2160 cmdline: {path} MD5: CAFE59D79E00E211548D5E569931E70E)
    - schtasks.exe (PID: 5828 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp8193.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5772 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5868 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp84B1.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5872 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- cd61fe0ebfe9f6326cd5a4df9747e72c.exe (PID: 5932 cmdline: C:\Users\user\Desktop\cd61fe0ebfe9f6326cd5a4df9747e72c.exe 0 MD5: CAFE59D79E00E211548D5E569931E70E)
  - cd61fe0ebfe9f6326cd5a4df9747e72c.exe (PID: 2224 cmdline: {path} MD5: CAFE59D79E00E211548D5E569931E70E)
- dhcpmon.exe (PID: 3156 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: CAFE59D79E00E211548D5E569931E70E)
  - dhcpmon.exe (PID: 5844 cmdline: {path} MD5: CAFE59D79E00E211548D5E569931E70E)
  - dhcpmon.exe (PID: 5064 cmdline: {path} MD5: CAFE59D79E00E211548D5E569931E70E)
- dhcpmon.exe (PID: 6124 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: CAFE59D79E00E211548D5E569931E70E)
  - dhcpmon.exe (PID: 3468 cmdline: {path} MD5: CAFE59D79E00E211548D5E569931E70E)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "25d2fcba-c6f2-4766-acfe-f43fa2f1",
  "Group": "saviour",
  "Domain1": "cloudhost.myfirewall.org",
  "Domain2": "cloudhost.myfirewall.org",
  "Port": 5456,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "cloudhost.myfirewall.org",
  "BackupDNSServer": "cloudhost.myfirewall.org",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.292598003.0000000002A2 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000001.00000002.489985311.000000000594 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000001.00000002.489985311.000000000594 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
0000000E.00000002.305109543.000000000040 2000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8J YUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000E.00000002.305109543.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 67 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
14.2.dhcpmon.exe.2fbec20.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
14.2.dhcpmon.exe.2fbec20.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
12.2.dhcpmon.exe.42205dc.5.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
12.2.dhcpmon.exe.42205dc.5.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost

Source	Rule	Description	Author	Strings
12.2.dhcpmon.exe.42205dc.5.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 124 entries				

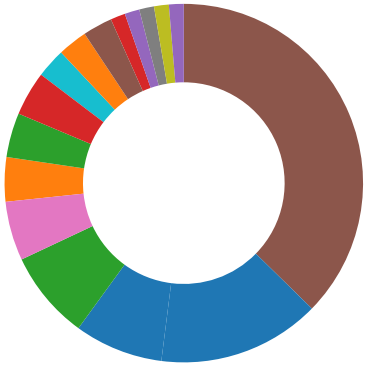
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

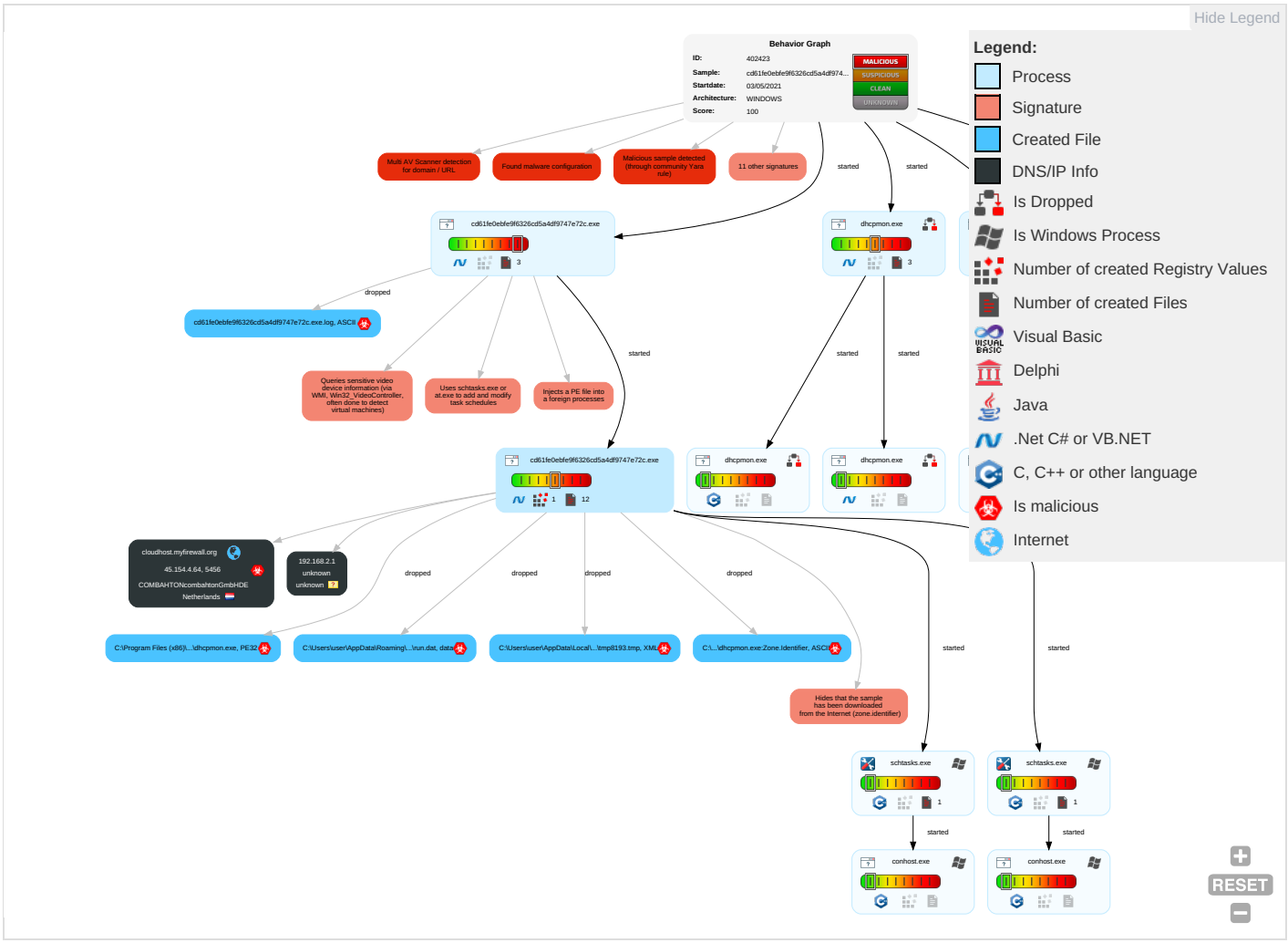
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 2	Input Capture 1 1	Security Software Discovery 3 1 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Virtualization/Sandbox Evasion 1 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	System Information Discovery 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

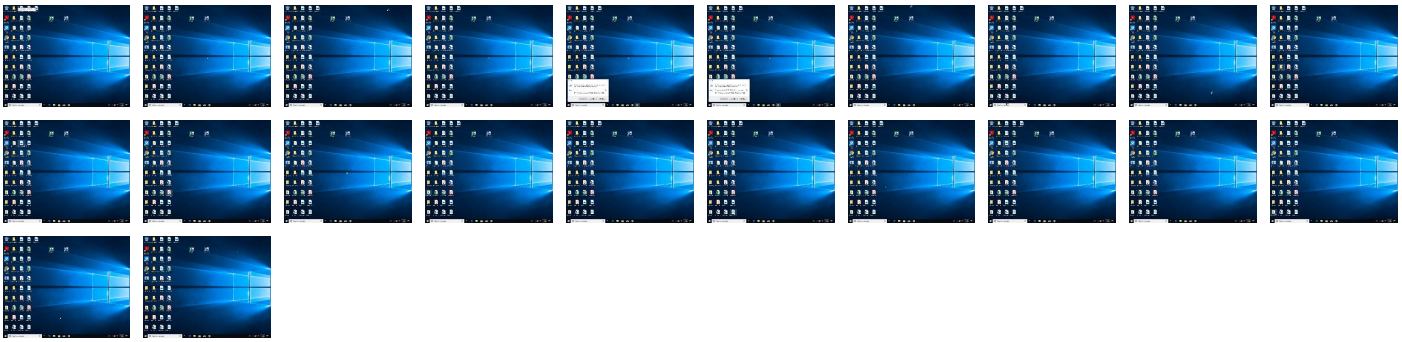
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
cd61fe0ebfe9f6326cd5a4df9747e72c.exe	26%	ReversingLabs	ByteCode-MSIL.Packed.Generic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	23%	ReversingLabs	ByteCode-MSIL.Packed.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.cd61fe0ebfe9f6326cd5a4df9747e72c.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
1.2.cd61fe0ebfe9f6326cd5a4df9747e72c.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
1.2.cd61fe0ebfe9f6326cd5a4df9747e72c.exe.6890000.10.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

Source	Detection	Scanner	Label	Link
cloudhost.myfirewall.org	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
cloudhost.myfirewall.org	8%	Virustotal		Browse
cloudhost.myfirewall.org	0%	Avira URL Cloud	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	0%	URL Reputation	safe	
http://www.carterandcone.comn-u	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.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fontbureau.commc	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.fonts.comY	0%	Avira URL Cloud	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.fonts.comEF	0%	Avira URL Cloud	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.carterandcone.comWxU	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.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.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.carterandcone.com;y	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cloudhost.myfirewall.org	45.154.4.64	true	true	• 8%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
cloudhost.myfirewall.org	true	• 8%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000002.243134558.0000000007242000.00000004.00000001.sdmp, cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000006.00000002.278971780.0000000005EF0000.00000002.00000001.sdmp, dhcpmon.exe, 00000007.00000002.279684540.0000000006000000.00000002.00000001.sdmp, dhcpmon.exe, 00000009.00000002.299680250.0000000006130000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000002.243134558.0000000007242000.00000004.00000001.sdmp, cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000006.00000002.278971780.0000000005EF0000.00000002.00000001.sdmp, dhcpmon.exe, 00000007.00000002.279684540.0000000006000000.00000002.00000001.sdmp, dhcpmon.exe, 00000009.00000002.299680250.0000000006130000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000002.2431 34558.0000000007242000.0000000 4.00000001.sdmp, cd61fe0ebfe9f 6326cd5a4df9747e72c.exe, 00000 006.00000002.278971780.0000000 005EF0000.00000002.00000001.sdmp, dhcpmon.exe, 00000007.0000 0002.279684540.000000000600000 0.00000002.00000001.sdmp, dhcp mon.exe, 00000009.00000002.299 680250.0000000006130000.000000 02.00000001.sdmp	false		high
http://www.carterandcone.comn-u	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000003.2151 19178.000000000606E000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000002.2431 34558.0000000007242000.0000000 4.00000001.sdmp, cd61fe0ebfe9f 6326cd5a4df9747e72c.exe, 00000 006.00000002.278971780.0000000 005EF0000.00000002.00000001.sdmp, dhcpmon.exe, 00000007.0000 0002.279684540.000000000600000 0.00000002.00000001.sdmp, dhcp mon.exe, 00000009.00000002.299 680250.0000000006130000.000000 02.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000002.2431 34558.0000000007242000.0000000 4.00000001.sdmp, cd61fe0ebfe9f 6326cd5a4df9747e72c.exe, 00000 006.00000002.278971780.0000000 005EF0000.00000002.00000001.sdmp, dhcpmon.exe, 00000007.0000 0002.279684540.000000000600000 0.00000002.00000001.sdmp, dhcp mon.exe, 00000009.00000002.299 680250.0000000006130000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000002.2431 34558.0000000007242000.0000000 4.00000001.sdmp, cd61fe0ebfe9f 6326cd5a4df9747e72c.exe, 00000 006.00000002.278971780.0000000 005EF0000.00000002.00000001.sdmp, dhcpmon.exe, 00000007.0000 0002.279684540.000000000600000 0.00000002.00000001.sdmp, dhcp mon.exe, 00000009.00000002.299 680250.0000000006130000.000000 02.00000001.sdmp	false		high
http://www.fontbureau.commc	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000003.2332 57404.0000000006038000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	dhcpmon.exe, 00000009.00000002 .299680250.0000000006130000.00 000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	dhcpmon.exe, 00000009.00000002 .299680250.0000000006130000.00 000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000002.2431 34558.0000000007242000.0000000 4.00000001.sdmp, cd61fe0ebfe9f 6326cd5a4df9747e72c.exe, 00000 006.00000002.278971780.0000000 005EF0000.00000002.00000001.sdmp, dhcpmon.exe, 00000007.0000 0002.279684540.000000000600000 0.00000002.00000001.sdmp, dhcp mon.exe, 00000009.00000002.299 680250.0000000006130000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000003.2151 19178.000000000606E000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

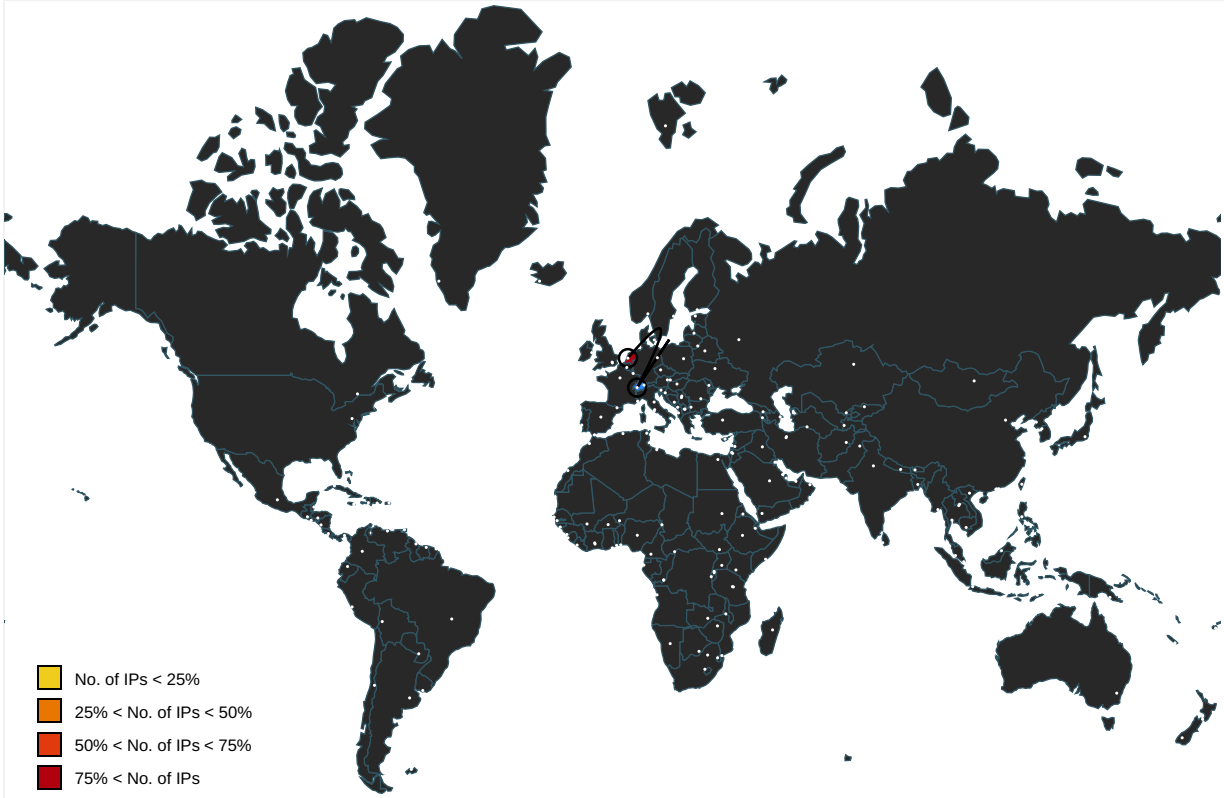
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.come.com	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000003.233257404.0000000006038000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comY	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000003.213423068.000000000604B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000002.243134558.0000000007242000.00000004.00000001.sdmp, cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000006.00000002.278971780.0000000005EF0000.00000002.00000001.sdmp, dhcpmon.exe, 00000007.00000002.279684540.0000000006000000.00000002.00000001.sdmp, dhcpmon.exe, 00000009.00000002.299680250.0000000006130000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000002.243134558.0000000007242000.00000004.00000001.sdmp, cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000006.00000002.278971780.0000000005EF0000.00000002.00000001.sdmp, dhcpmon.exe, 00000007.00000002.279684540.0000000006000000.00000002.00000001.sdmp, dhcpmon.exe, 00000009.00000002.299680250.0000000006130000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000002.243134558.0000000007242000.00000004.00000001.sdmp, cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000006.00000002.278971780.0000000005EF0000.00000002.00000001.sdmp, dhcpmon.exe, 00000007.00000002.279684540.0000000006000000.00000002.00000001.sdmp, dhcpmon.exe, 00000009.00000002.299680250.0000000006130000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000002.243134558.0000000007242000.00000004.00000001.sdmp, cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000006.00000002.278971780.0000000005EF0000.00000002.00000001.sdmp, dhcpmon.exe, 00000007.00000002.279684540.0000000006000000.00000002.00000001.sdmp, dhcpmon.exe, 00000009.00000002.299680250.0000000006130000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000002.243134558.0000000007242000.00000004.00000001.sdmp, cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000006.00000002.278971780.0000000005EF0000.00000002.00000001.sdmp, dhcpmon.exe, 00000007.00000002.279684540.0000000006000000.00000002.00000001.sdmp, dhcpmon.exe, 00000009.00000002.299680250.0000000006130000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000002.243134558.0000000007242000.00000004.00000001.sdmp, cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000006.00000002.278971780.0000000005EF0000.00000002.00000001.sdmp, dhcpmon.exe, 00000007.00000002.279684540.0000000006000000.00000002.00000001.sdmp, dhcpmon.exe, 00000009.00000002.299680250.0000000006130000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000002.2431 34558.0000000007242000.0000000 4.00000001.sdmp, cd61fe0ebfe9f 6326cd5a4df9747e72c.exe, 00000 006.00000002.278971780.0000000 005EF0000.00000002.00000001.sdmp, dhcpmon.exe, 00000007.0000 0002.279684540.000000000600000 0.00000002.00000001.sdmp, dhcp mon.exe, 00000009.00000002.299 680250.0000000006130000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comEF	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000003.2134 13683.000000000606E000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000002.2431 34558.0000000007242000.0000000 4.00000001.sdmp, cd61fe0ebfe9f 6326cd5a4df9747e72c.exe, 00000 006.00000002.278971780.0000000 005EF0000.00000002.00000001.sdmp, dhcpmon.exe, 00000007.0000 0002.279684540.000000000600000 0.00000002.00000001.sdmp, dhcp mon.exe, 00000009.00000002.299 680250.0000000006130000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000002.2431 34558.0000000007242000.0000000 4.00000001.sdmp, cd61fe0ebfe9f 6326cd5a4df9747e72c.exe, 00000 006.00000002.278971780.0000000 005EF0000.00000002.00000001.sdmp, dhcpmon.exe, 00000007.0000 0002.279684540.000000000600000 0.00000002.00000001.sdmp, dhcp mon.exe, 00000009.00000002.299 680250.0000000006130000.000000 02.00000001.sdmp	false		high
http://www.carterandcone.comWxU	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000003.2151 19178.000000000606E000.0000000 4.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comm	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000003.2332 57404.0000000006038000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000002.2431 34558.0000000007242000.0000000 4.00000001.sdmp, cd61fe0ebfe9f 6326cd5a4df9747e72c.exe, 00000 006.00000002.278971780.0000000 005EF0000.00000002.00000001.sdmp, dhcpmon.exe, 00000007.0000 0002.279684540.000000000600000 0.00000002.00000001.sdmp, dhcp mon.exe, 00000009.00000002.299 680250.0000000006130000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000002.2431 34558.0000000007242000.0000000 4.00000001.sdmp, cd61fe0ebfe9f 6326cd5a4df9747e72c.exe, 00000 006.00000002.278971780.0000000 005EF0000.00000002.00000001.sdmp, dhcpmon.exe, 00000007.0000 0002.279684540.000000000600000 0.00000002.00000001.sdmp, dhcp mon.exe, 00000009.00000002.299 680250.0000000006130000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers8	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000002.2431 34558.0000000007242000.0000000 4.00000001.sdmp, cd61fe0ebfe9f 6326cd5a4df9747e72c.exe, 00000 006.00000002.278971780.0000000 005EF0000.00000002.00000001.sdmp, dhcpmon.exe, 00000007.0000 0002.279684540.000000000600000 0.00000002.00000001.sdmp, dhcp mon.exe, 00000009.00000002.299 680250.0000000006130000.000000 02.00000001.sdmp	false		high
http://www.fontbureau.comgrito	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000003.2332 57404.0000000006038000.0000000 4.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000003.2142 36957.000000000606E000.0000000 4.00000001.sdmp, cd61fe0ebfe9f 6326cd5a4df9747e72c.exe, 00000 000.00000003.213440503.0000000 00606E000.00000004.00000001.sdmp, cd61fe0ebfe9f6326cd5a4df97 47e72c.exe, 00000006.00000002. 278971780.0000000005EF0000.000 00002.00000001.sdmp, dhcpmon.exe, 00000007.00000002.27968454 0.0000000006000000.00000002.00 000001.sdmp, dhcpmon.exe, 0000 0009.00000002.299680250.000000 0006130000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000002.2431 34558.0000000007242000.0000000 4.00000001.sdmp, cd61fe0ebfe9f 6326cd5a4df9747e72c.exe, 00000 006.00000002.278971780.0000000 005EF0000.00000002.00000001.sdmp, dhcpmon.exe, 00000007.0000 0002.279684540.000000000600000 0.00000002.00000001.sdmp, dhcp mon.exe, 00000009.00000002.299 680250.0000000006130000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000002.2431 34558.0000000007242000.0000000 4.00000001.sdmp, cd61fe0ebfe9f 6326cd5a4df9747e72c.exe, 00000 006.00000002.278971780.0000000 005EF0000.00000002.00000001.sdmp, dhcpmon.exe, 00000007.0000 0002.279684540.000000000600000 0.00000002.00000001.sdmp, dhcp mon.exe, 00000009.00000002.299 680250.0000000006130000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000002.2431 34558.0000000007242000.0000000 4.00000001.sdmp, cd61fe0ebfe9f 6326cd5a4df9747e72c.exe, 00000 006.00000002.278971780.0000000 005EF0000.00000002.00000001.sdmp, dhcpmon.exe, 00000007.0000 0002.279684540.000000000600000 0.00000002.00000001.sdmp, dhcp mon.exe, 00000009.00000002.299 680250.0000000006130000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000002.2431 34558.0000000007242000.0000000 4.00000001.sdmp, cd61fe0ebfe9f 6326cd5a4df9747e72c.exe, 00000 006.00000002.278971780.0000000 005EF0000.00000002.00000001.sdmp, dhcpmon.exe, 00000007.0000 0002.279684540.000000000600000 0.00000002.00000001.sdmp, dhcp mon.exe, 00000009.00000002.299 680250.0000000006130000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.com;y	cd61fe0ebfe9f6326cd5a4df9747e72c.exe, 00000000.00000003.2151 19178.000000000606E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.154.4.64	cloudhost.myfirewall.org	Netherlands		30823	COMBAHTONcombahtonGmbHDE	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	402423
Start date:	03.05.2021
Start time:	06:12:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	cd61fe0ebfe9f6326cd5a4df9747e72c.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:	25
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@20/8@7/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • Excluded IPs from analysis (whitelisted): 40.88.32.150, 168.61.161.212, 104.43.139.144, 13.64.90.137, 2.20.84.85 • Excluded domains from analysis (whitelisted): skypedataprdcoleus15.cloudapp.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, watson.telemetry.microsoft.com, prod.fs.microsoft.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net • Report 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.

Simulations

Behavior and APIs

Time	Type	Description
06:13:08	API Interceptor	941x Sleep call for process: cd61fe0ebfe9f6326cd5a4df9747e72c.exe modified
06:13:15	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
06:13:16	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\cd61fe0ebfe9f6326cd5a4df9747e72c.exe" s>$(Arg0)
06:13:17	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
06:13:23	API Interceptor	4x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.154.4.64	8mOB0MBW71.exe	Get hash	malicious	Browse	
	16j7nmOOPS.exe	Get hash	malicious	Browse	
	RFQ_Quotation_33645.jar	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ_Quotation_33645.jar	Get hash	malicious	Browse	
	c86d280b0c5cb985372fa7a0260cabb9.exe	Get hash	malicious	Browse	
	edc1948e07209992d4eb51b64c3c102a.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cloudhost.myfirewall.org	PyQdnx9PHg.exe	Get hash	malicious	Browse	• 31.210.21.252
	GO1eovBADG.exe	Get hash	malicious	Browse	• 45.85.90.92
	9nNELqsesC.exe	Get hash	malicious	Browse	• 46.183.220.67
	180421 PDA Request for Quotation.doc	Get hash	malicious	Browse	• 46.183.220.67
	edc1948e07209992d4eb51b64c3c102a.exe	Get hash	malicious	Browse	• 45.154.4.64
	1RevKocjWoyhJ3y.exe	Get hash	malicious	Browse	• 45.154.4.68
	bbbe7872ea466446da60c4da50020cbb.exe	Get hash	malicious	Browse	• 79.134.225.105
	e92b274943f4a3a557881ee0dd57772d.exe	Get hash	malicious	Browse	• 79.134.225.105
	256ec8f8f67b59c5e085b0bb63afcd13.exe	Get hash	malicious	Browse	• 79.134.225.105
	9a08c8a2b49d6348f2ef35f85a1c6351.exe	Get hash	malicious	Browse	• 79.134.225.105
	zSDBuG8gDl.exe	Get hash	malicious	Browse	• 185.229.243.67
	65d1beae1fc7eb126cd4a9b277afb942.exe	Get hash	malicious	Browse	• 79.134.225.96
	f2a22415c1b108ce91fd76e3320431d0.exe	Get hash	malicious	Browse	• 79.134.225.105
	1d8eff2bc76e46dc186fa501e24f5cb1.exe	Get hash	malicious	Browse	• 79.134.225.105
	5134b758f8eb77424254ce67f4697ffe.exe	Get hash	malicious	Browse	• 79.134.225.96
	1d8eff2bc76e46dc186fa501e24f5cb1.exe	Get hash	malicious	Browse	• 79.134.225.96
	460f7e6048ed3ca91f1573a7410fedd6.exe	Get hash	malicious	Browse	• 79.134.225.96
	1d78424ce6944359d546dbcbc030f19e.exe	Get hash	malicious	Browse	• 79.134.225.105

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
COMBAHTONcombahtonGmbHDE	SecuriteInfo.com.Trojan.GenericKD.46134463.32139.exe	Get hash	malicious	Browse	• 152.89.247.94
	SecuriteInfo.com.Trojan.GenericKD.46134463.32139.exe	Get hash	malicious	Browse	• 152.89.247.94
	Payu transfer form.scr.exe	Get hash	malicious	Browse	• 45.154.4.187
	6Lxyp86O5r.exe	Get hash	malicious	Browse	• 185.223.28.241
	Payu transfer form.scr.exe	Get hash	malicious	Browse	• 45.154.4.187
	t.exe	Get hash	malicious	Browse	• 185.234.72.193
	Payu Remittance.scr.exe	Get hash	malicious	Browse	• 45.154.4.187
	8mOB0MBW71.exe	Get hash	malicious	Browse	• 45.154.4.64
	16j7nmOOPS.exe	Get hash	malicious	Browse	• 45.154.4.64
	PRODUCT LIST.exe	Get hash	malicious	Browse	• 152.89.247.26
	ggg6d3cpLN.exe	Get hash	malicious	Browse	• 45.147.229.85
	RFQ_Quotation_33645.jar	Get hash	malicious	Browse	• 45.154.4.64
	RFQ_Quotation_33645.jar	Get hash	malicious	Browse	• 45.154.4.64
	COBxDiCIPE.exe	Get hash	malicious	Browse	• 185.234.72.84
	q8kLYww20p.exe	Get hash	malicious	Browse	• 185.150.25.183
	WVfZC9E9zy.xlsm	Get hash	malicious	Browse	• 160.20.147.241
	c86d280b0c5cb985372fa7a0260cabb9.exe	Get hash	malicious	Browse	• 45.154.4.64
	edc1948e07209992d4eb51b64c3c102a.exe	Get hash	malicious	Browse	• 45.154.4.64
	1kg67oWywx.exe	Get hash	malicious	Browse	• 45.153.240.131
	4CEbLdyJkK.exe	Get hash	malicious	Browse	• 160.20.147.195

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Process:	C:\Users\user\Desktop\cd61fe0ebfe9f6326cd5a4df9747e72c.exe

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	817664
Entropy (8bit):	7.372197931665627
Encrypted:	false
SSDEEP:	24576:mcoLAtztGneLJo9ilgwrTB5PLZ6mz9U4F:rGnkJo9Mgwr15N6mzqQ
MD5:	CAFE59D79E00E211548D5E569931E70E
SHA1:	D7FBFD97E93DEC7490EF06C24E2D373127CE56EB
SHA-256:	4B603D683F975207871344AA9790AC649BD15C98CCEECF626B92A1D3D8FD85F4
SHA-512:	5FFB8743EAF17CA74EFF460731F5E1835943DCF4C603D0137B1CF5236CA9981E4141A5C4997D006473B7272E14C11C431B1CE57D7C2CEA818934719D832C6AB/
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 23%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....l.`.....p..... .....@.. ..@.....,...W..... ..... ..H.....text....n... ...p..... ..`.reloc.....r.....@..B.rsrc..... .....t.....@..@.....h.....H.....HE...H.....o.....z.(.....}.....(....o....}....*..*...0.....{.....E.....8...Z...u.....*..}.....].4S}.....}.. ...*..}..... ..Q.}.....}.....*..}.....{.... Km.a}.....}.....*..}..... ,...}.....}.....*..}.....{.... ..=.a}.....}.....*..}..... ....}.....}.....*..}..... "G.R}.....}.....*..}.....*...{....*.s....z.2.{.....4...*....0..<.....{.....3.. {....(....o....3...}.....+..s.....{....}..

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\cd61fe0ebfe9f6326cd5a4df9747e72c.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\cd61fe0ebfe9f6326cd5a4df9747e72c.exe.log	
Process:	C:\Users\user\Desktop\cd61fe0ebfe9f6326cd5a4df9747e72c.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp8193.tmp	
Process:	C:\Users\user\Desktop\cd61fe0ebfe9f6326cd5a4df9747e72c.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1322
Entropy (8bit):	5.152508680113646
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0fuhxtn:cbk4oL600QydbQxIYODOLedq3wyj
MD5:	2E01729C4CBFA0824FA19C502719E1F0
SHA1:	6183FF20CE8E71DEABC0ABC7413395D2E02E5EB8
SHA-256:	96F7EF60688D6A41E8DAAD7A371C7F2A7D7C5F708BACD4D56A43DDE8B39F5E51
SHA-512:	A72B5096B25BB08949DE4F0162D691DD7DCA1DB60DC885FB741FE8618F6E80F6F304DE03DC1C5C12637F3EF2E551EDC55FA7D2885F846D5DDCC637E19635B8B
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 />.. <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\tmp84B1.tmp	
Process:	C:\Users\user\Desktop\cd61fe0ebfe9f6326cd5a4df9747e72c.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\cd61fe0ebfe9f6326cd5a4df9747e72c.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
SSDEEP:	3:rM8t:Q8t
MD5:	77632B38511A41BC3CE512B7978C4FAE
SHA1:	E0C5DEB12A9147E2BF51B16CAB9F80A66DBABD4B
SHA-256:	3A271C465E23FBF037C0F8EEC583907F50C191A784C25D39D69D7201D6028DE5
SHA-512:	6DB8F6C8251804470F240957A14C0F6A0DCE8756C18906274315F7FE4180E23AA08BE19A1C6AED5AB767C97D8CDD5F98EA72F5D8BF487607B968A6538CF9135
Malicious:	**true**
Preview:	.45..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\cd61fe0ebfe9f6326cd5a4df9747e72c.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	59
Entropy (8bit):	4.577226947520249
Encrypted:	false
SSDEEP:	3:oNWXp5vGBTADDtS3XGkAn:oNWXpFGBTAnt+XbAn
MD5:	373D4A56D721AF230683199455B12D66
SHA1:	984A973960B5A38C02B9D40D720BC8AC3196CD08
SHA-256:	987F84DCEBA7442776AB9D69C1967C7645C260DD45FC8D3442DA15456C986A39
SHA-512:	E23C87238CADF40A7B84FB1BC54BB60466F241FC2514B97755D99D4CE09A931AA0D4E3BC3A910D92FC65AB6FB58F364ACFD4D497C7304A8C305F814326A1BBF
Malicious:	false
Preview:	C:\Users\user\Desktop\cd61fe0ebfe9f6326cd5a4df9747e72c.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.372197931665627
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	cd61fe0ebfe9f6326cd5a4df9747e72c.exe
File size:	817664
MD5:	cafe59d79e00e211548d5e569931e70e
SHA1:	d7fbfd97e93dec7490ef06c24e2d373127ce56eb
SHA256:	4b603d683f975207871344aa9790ac649bd15c98cceecf626b92a1d3d8fd85f4
SHA512:	5ffb8743eaf17ca74eff460731f5e1835943dcf4c603d0137b1cf5236ca9981e4141a5c4997d006473b7272e14c11c431b1ce57d7c2cea818934719d832c6aba
SSDEEP:	24576:mcoLAtztGneLJo9ilgwrTB5PLZ6mz9U4F:rGnkJo9Mgwr15N6mzqQ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....I.`.....p..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4c8e86

General

Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x608F6C8D [Mon May 3 03:22:53 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc8e2c	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xcc000	0x5ec	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xca000	0xc	.reloc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xc6e8c	0xc7000	False	0.748219859061	data	7.37345059392	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0xca000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0xcc000	0x5ec	0x600	False	0.444010416667	data	4.2368443366	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xcc0a0	0x398	data		
RT_MANIFEST	0xcc438	0x1b4	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Microsoft 2010
Assembly Version	1.0.0.0
InternalName	HWZinl0yCvGMAUeP.exe
FileVersion	1.0.0.0
CompanyName	Microsoft
LegalTrademarks	
Comments	
ProductName	Singleton Vote Manager
ProductVersion	1.0.0.0
FileDescription	Singleton Vote Manager
OriginalFilename	HWZinl0yCvGMAUeP.exe

Network Behavior

Network Port Distribution

Total Packets: 46

- 53 (DNS)
- 5456 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 06:13:16.622473001 CEST	49700	5456	192.168.2.3	45.154.4.64
May 3, 2021 06:13:19.662369013 CEST	49700	5456	192.168.2.3	45.154.4.64
May 3, 2021 06:13:25.662859917 CEST	49700	5456	192.168.2.3	45.154.4.64
May 3, 2021 06:13:36.689135075 CEST	49704	5456	192.168.2.3	45.154.4.64
May 3, 2021 06:13:39.851622105 CEST	49704	5456	192.168.2.3	45.154.4.64
May 3, 2021 06:13:45.852155924 CEST	49704	5456	192.168.2.3	45.154.4.64
May 3, 2021 06:13:54.580380917 CEST	49705	5456	192.168.2.3	45.154.4.64
May 3, 2021 06:13:57.587424994 CEST	49705	5456	192.168.2.3	45.154.4.64
May 3, 2021 06:14:03.603514910 CEST	49705	5456	192.168.2.3	45.154.4.64
May 3, 2021 06:14:12.012996912 CEST	49706	5456	192.168.2.3	45.154.4.64
May 3, 2021 06:14:15.026315928 CEST	49706	5456	192.168.2.3	45.154.4.64
May 3, 2021 06:14:21.042445898 CEST	49706	5456	192.168.2.3	45.154.4.64
May 3, 2021 06:14:30.479223013 CEST	49707	5456	192.168.2.3	45.154.4.64
May 3, 2021 06:14:33.480999947 CEST	49707	5456	192.168.2.3	45.154.4.64
May 3, 2021 06:14:39.497117996 CEST	49707	5456	192.168.2.3	45.154.4.64
May 3, 2021 06:14:48.508419037 CEST	49708	5456	192.168.2.3	45.154.4.64
May 3, 2021 06:14:51.513839960 CEST	49708	5456	192.168.2.3	45.154.4.64
May 3, 2021 06:14:57.529858112 CEST	49708	5456	192.168.2.3	45.154.4.64
May 3, 2021 06:15:05.136528015 CEST	49709	5456	192.168.2.3	45.154.4.64
May 3, 2021 06:15:08.140086889 CEST	49709	5456	192.168.2.3	45.154.4.64
May 3, 2021 06:15:14.140600920 CEST	49709	5456	192.168.2.3	45.154.4.64

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 06:12:53.469957113 CEST	54130	53	192.168.2.3	8.8.8.8
May 3, 2021 06:12:53.520760059 CEST	53	54130	8.8.8.8	192.168.2.3
May 3, 2021 06:12:54.490751028 CEST	56961	53	192.168.2.3	8.8.8.8
May 3, 2021 06:12:54.539424896 CEST	53	56961	8.8.8.8	192.168.2.3
May 3, 2021 06:12:55.392870903 CEST	59353	53	192.168.2.3	8.8.8.8
May 3, 2021 06:12:55.446100950 CEST	53	59353	8.8.8.8	192.168.2.3
May 3, 2021 06:12:56.179971933 CEST	52238	53	192.168.2.3	8.8.8.8
May 3, 2021 06:12:56.228651047 CEST	53	52238	8.8.8.8	192.168.2.3
May 3, 2021 06:12:57.057734966 CEST	49873	53	192.168.2.3	8.8.8.8
May 3, 2021 06:12:57.114573002 CEST	53	49873	8.8.8.8	192.168.2.3
May 3, 2021 06:12:57.992364883 CEST	53196	53	192.168.2.3	8.8.8.8
May 3, 2021 06:12:58.051346064 CEST	53	53196	8.8.8.8	192.168.2.3
May 3, 2021 06:12:59.227421045 CEST	56777	53	192.168.2.3	8.8.8.8
May 3, 2021 06:12:59.284674883 CEST	53	56777	8.8.8.8	192.168.2.3
May 3, 2021 06:13:00.317862988 CEST	58643	53	192.168.2.3	8.8.8.8
May 3, 2021 06:13:00.369373083 CEST	53	58643	8.8.8.8	192.168.2.3
May 3, 2021 06:13:01.572945118 CEST	60985	53	192.168.2.3	8.8.8.8
May 3, 2021 06:13:01.624459028 CEST	53	60985	8.8.8.8	192.168.2.3
May 3, 2021 06:13:02.770304918 CEST	50200	53	192.168.2.3	8.8.8.8
May 3, 2021 06:13:02.820998907 CEST	53	50200	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 06:13:03.684628963 CEST	51281	53	192.168.2.3	8.8.8.8
May 3, 2021 06:13:03.733345985 CEST	53	51281	8.8.8.8	192.168.2.3
May 3, 2021 06:13:04.689282894 CEST	49199	53	192.168.2.3	8.8.8.8
May 3, 2021 06:13:04.746345997 CEST	53	49199	8.8.8.8	192.168.2.3
May 3, 2021 06:13:05.649189949 CEST	50620	53	192.168.2.3	8.8.8.8
May 3, 2021 06:13:05.700603962 CEST	53	50620	8.8.8.8	192.168.2.3
May 3, 2021 06:13:06.856580973 CEST	64938	53	192.168.2.3	8.8.8.8
May 3, 2021 06:13:06.910275936 CEST	53	64938	8.8.8.8	192.168.2.3
May 3, 2021 06:13:07.891201973 CEST	60152	53	192.168.2.3	8.8.8.8
May 3, 2021 06:13:07.940021992 CEST	53	60152	8.8.8.8	192.168.2.3
May 3, 2021 06:13:08.798947096 CEST	57544	53	192.168.2.3	8.8.8.8
May 3, 2021 06:13:08.847690105 CEST	53	57544	8.8.8.8	192.168.2.3
May 3, 2021 06:13:10.204770088 CEST	55984	53	192.168.2.3	8.8.8.8
May 3, 2021 06:13:10.253529072 CEST	53	55984	8.8.8.8	192.168.2.3
May 3, 2021 06:13:16.544682026 CEST	64185	53	192.168.2.3	8.8.8.8
May 3, 2021 06:13:16.610896111 CEST	53	64185	8.8.8.8	192.168.2.3
May 3, 2021 06:13:26.608794928 CEST	65110	53	192.168.2.3	8.8.8.8
May 3, 2021 06:13:26.681531906 CEST	53	65110	8.8.8.8	192.168.2.3
May 3, 2021 06:13:36.598557949 CEST	58361	53	192.168.2.3	8.8.8.8
May 3, 2021 06:13:36.660099983 CEST	53	58361	8.8.8.8	192.168.2.3
May 3, 2021 06:13:54.522099018 CEST	63492	53	192.168.2.3	8.8.8.8
May 3, 2021 06:13:54.579246998 CEST	53	63492	8.8.8.8	192.168.2.3
May 3, 2021 06:14:11.950134993 CEST	60831	53	192.168.2.3	8.8.8.8
May 3, 2021 06:14:12.009407997 CEST	53	60831	8.8.8.8	192.168.2.3
May 3, 2021 06:14:30.416460037 CEST	60100	53	192.168.2.3	8.8.8.8
May 3, 2021 06:14:30.477823019 CEST	53	60100	8.8.8.8	192.168.2.3
May 3, 2021 06:14:48.437777042 CEST	53195	53	192.168.2.3	8.8.8.8
May 3, 2021 06:14:48.506958008 CEST	53	53195	8.8.8.8	192.168.2.3
May 3, 2021 06:15:05.074812889 CEST	50141	53	192.168.2.3	8.8.8.8
May 3, 2021 06:15:05.135440111 CEST	53	50141	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 3, 2021 06:13:16.544682026 CEST	192.168.2.3	8.8.8.8	0x9ed6	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
May 3, 2021 06:13:36.598557949 CEST	192.168.2.3	8.8.8.8	0x50d7	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
May 3, 2021 06:13:54.522099018 CEST	192.168.2.3	8.8.8.8	0xb7fe	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
May 3, 2021 06:14:11.950134993 CEST	192.168.2.3	8.8.8.8	0xa4b7	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
May 3, 2021 06:14:30.416460037 CEST	192.168.2.3	8.8.8.8	0x72ad	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
May 3, 2021 06:14:48.437777042 CEST	192.168.2.3	8.8.8.8	0xe510	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)
May 3, 2021 06:15:05.074812889 CEST	192.168.2.3	8.8.8.8	0xef7f	Standard query (0)	cloudhost.myfirewall.org	A (IP address)	IN (0x0001)

DNS Answers

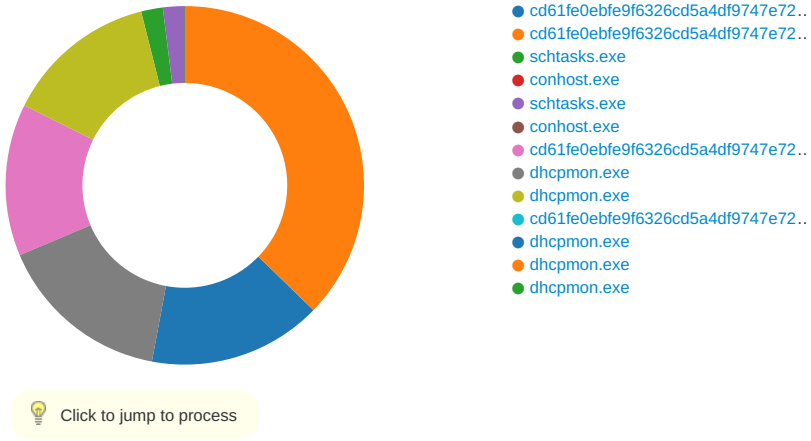
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 3, 2021 06:13:16.610896111 CEST	8.8.8.8	192.168.2.3	0x9ed6	No error (0)	cloudhost.myfirewall.org		45.154.4.64	A (IP address)	IN (0x0001)
May 3, 2021 06:13:36.660099983 CEST	8.8.8.8	192.168.2.3	0x50d7	No error (0)	cloudhost.myfirewall.org		45.154.4.64	A (IP address)	IN (0x0001)
May 3, 2021 06:13:54.579246998 CEST	8.8.8.8	192.168.2.3	0xb7fe	No error (0)	cloudhost.myfirewall.org		45.154.4.64	A (IP address)	IN (0x0001)
May 3, 2021 06:14:12.009407997 CEST	8.8.8.8	192.168.2.3	0xa4b7	No error (0)	cloudhost.myfirewall.org		45.154.4.64	A (IP address)	IN (0x0001)
May 3, 2021 06:14:30.477823019 CEST	8.8.8.8	192.168.2.3	0x72ad	No error (0)	cloudhost.myfirewall.org		45.154.4.64	A (IP address)	IN (0x0001)
May 3, 2021 06:14:48.506958008 CEST	8.8.8.8	192.168.2.3	0xe510	No error (0)	cloudhost.myfirewall.org		45.154.4.64	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 3, 2021 06:15:05.135440111 CEST	8.8.8.8	192.168.2.3	0xef7f	No error (0)	cloudhost.myfirewall.org		45.154.4.64	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: cd61fe0ebfe9f6326cd5a4df9747e72c.exe PID: 5644 Parent PID: 5776

General

Start time:	06:13:00
Start date:	03/05/2021
Path:	C:\Users\user\Desktop\cd61fe0ebfe9f6326cd5a4df9747e72c.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\cd61fe0ebfe9f6326cd5a4df9747e72c.exe'
Imagebase:	0xb70000
File size:	817664 bytes
MD5 hash:	CAFE59D79E00E211548D5E569931E70E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.237161561.00000000040E9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.237161561.00000000040E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.237161561.00000000040E9000.00000004.00000001.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	6DE9CF06	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	6DE9CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\cd61fe0ebfe9f6326cd5a4df9747e72c.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1AC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\cd61fe0ebfe9f6326cd5a4df9747e72c.exe.log	unknown	1308	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E1AC907	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	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDD03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCE1B4F	ReadFile

Analysis Process: cd61fe0ebfe9f6326cd5a4df9747e72c.exe PID: 2160 Parent PID: 5644

General

Start time:	06:13:10
Start date:	03/05/2021
Path:	C:\Users\user\Desktop\cd61fe0ebfe9f6326cd5a4df9747e72c.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xea0000
File size:	817664 bytes
MD5 hash:	CAFE59D79E00E211548D5E569931E70E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.489985311.0000000005940000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.489985311.0000000005940000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.488801787.0000000004459000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.488801787.0000000004459000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.484987240.0000000003411000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.479870738.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.479870738.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.479870738.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.490630071.0000000006890000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.490630071.0000000006890000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.490630071.0000000006890000.00000004.00000001.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	6DE9CF06	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	6DE9CF06	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	6CCEBEFF	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	6CCE1E60	CreateFileW
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CCEBEFF	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CCEDD66	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CCEDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp8193.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CCE7038	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	6CCE1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp84B1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CCE7038	GetTempFileNameW
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	6CCEBEFF	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	6CCEBEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8193.tmp	success or wait	1	6CCE6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp84B1.tmp	success or wait	1	6CCE6A95	DeleteFileW
C:\Users\user\Desktop\cd61fe0ebfe9f6326cd5a4df9747e72c.exe:Zone.Identifier	success or wait	1	6CC62935	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	ea b4 a0 34 35 0e d9 48	...45..H	success or wait	1	6CCE1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 8d 6c 8f 60 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 70 0c 00 00 08 00 00 00 00 00 00 86 8e 0c 00 00 20 00 00 00 a0 0c 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 e0 0c 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....l.`.......... ....p............... ....@.. ....@.................	success or wait	4	6CCEDD66	CopyFileW
C:\Program Files (x86)\DHCP Mo nitor\dhcpmon.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CCEDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp8193.tmp	unknown	1322	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.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveTo ken</LogonType>	success or wait	1	6CCE1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	59	43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 44 65 73 6b 74 6f 70 5c 63 64 36 31 66 65 30 65 62 66 65 39 66 36 33 32 36 63 64 35 61 34 64 66 39 37 34 37 65 37 32 63 2e 65 78 65	C:\Users\user\Desktop\cd6 1fe0e bfe9f6326cd5a4df9747e72 c.exe	success or wait	1	6CCE1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp84B1.tmp	unknown	1310	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	6CCE1B4F	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	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCE1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6DE5D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6DE5D72F	unknown
C:\Users\user\Desktop\cd61fe0ebfe9f6326cd5a4df9747e72c.exe	unknown	4096	success or wait	1	6DE5D72F	unknown
C:\Users\user\Desktop\cd61fe0ebfe9f6326cd5a4df9747e72c.exe	unknown	512	success or wait	1	6DE5D72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	6CCE646A	RegSetValueExW

Analysis Process: schtasks.exe PID: 5828 Parent PID: 2160

General

Start time:	06:13:13
Start date:	03/05/2021
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\tmp8193.tmp'
Imagebase:	0x1f0000
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\tmp8193.tmp	unknown	2	success or wait	1	1FAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp8193.tmp	unknown	1323	success or wait	1	1FABD9	ReadFile

Analysis Process: conhost.exe PID: 5772 Parent PID: 5828

General

Start time:	06:13:13
Start date:	03/05/2021
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: schtasks.exe PID: 5868 Parent PID: 2160

General

Start time:	06:13:13
Start date:	03/05/2021

Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp84B1.tmp'
Imagebase:	0x1f0000
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\tmp84B1.tmp	unknown	2	success or wait	1	1FAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp84B1.tmp	unknown	1311	success or wait	1	1FABD9	ReadFile

Analysis Process: conhost.exe PID: 5872 Parent PID: 5868

General

Start time:	06:13:14
Start date:	03/05/2021
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: cd61fe0ebfe9f6326cd5a4df9747e72c.exe PID: 5932 Parent PID: 528

General

Start time:	06:13:16
Start date:	03/05/2021
Path:	C:\Users\user\Desktop\cd61fe0ebfe9f6326cd5a4df9747e72c.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\cd61fe0ebfe9f6326cd5a4df9747e72c.exe 0
Imagebase:	0xa00000
File size:	817664 bytes
MD5 hash:	CAFE59D79E00E211548D5E569931E70E
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: 00000006.00000002.274443364.0000000003F09000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.274443364.0000000003F09000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.274443364.0000000003F09000.00000004.00000001.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	6DE9CF06	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	6DE9CF06	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	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCE1B4F	ReadFile

Analysis Process: dhcpmon.exe PID: 3156 Parent PID: 528

General

Start time:	06:13:18
Start date:	03/05/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0xc00000
File size:	817664 bytes
MD5 hash:	CAFE59D79E00E211548D5E569931E70E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.274520141.0000000004059000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.274520141.0000000004059000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.274520141.0000000004059000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 23%, ReversingLabs
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	6DE9CF06	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	6DE9CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1AC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	unknown	1308	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e 089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E1AC907	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	6DE75705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE75705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCE1B4F	ReadFile

Analysis Process: dhcpmon.exe PID: 6124 Parent PID: 3388

General

Start time:	06:13:24
Start date:	03/05/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xd70000
File size:	817664 bytes
MD5 hash:	CAFE59D79E00E211548D5E569931E70E
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: 00000009.00000002.295474134.0000000004129000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.295474134.0000000004129000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.295474134.0000000004129000.00000004.00000001.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	6DE9CF06	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	6DE9CF06	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	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE75705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE7CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDD03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDD03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE75705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CCE1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CCE1B4F	ReadFile

Analysis Process: cd61fe0ebfe9f6326cd5a4df9747e72c.exe PID: 2224 Parent PID: 5932

General

Start time:	06:13:25
Start date:	03/05/2021
Path:	C:\Users\user\Desktop\cd61fe0ebfe9f6326cd5a4df9747e72c.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x590000
File size:	817664 bytes
MD5 hash:	CAFE59D79E00E211548D5E569931E70E
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: 0000000A.00000002.292598003.0000000002A21000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.284508167.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.284508167.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.284508167.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.292765353.0000000002A59000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.293253440.0000000003A29000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.293253440.0000000003A29000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: dhcpmon.exe PID: 5844 Parent PID: 3156

General

Start time:	06:13:25
Start date:	03/05/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x70000
File size:	817664 bytes

MD5 hash:	CAFE59D79E00E211548D5E569931E70E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: dhcpmon.exe PID: 5064 Parent PID: 3156

General

Start time:	06:13:26
Start date:	03/05/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xdb0000
File size:	817664 bytes
MD5 hash:	CAFE59D79E00E211548D5E569931E70E
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: 0000000C.00000002.290898353.00000000031D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.290898353.00000000031D1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.289163047.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.289163047.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.289163047.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.291112478.00000000041D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.291112478.00000000041D9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: dhcpmon.exe PID: 3468 Parent PID: 6124

General

Start time:	06:13:32
Start date:	03/05/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x9e0000
File size:	817664 bytes
MD5 hash:	CAFE59D79E00E211548D5E569931E70E
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: 0000000E.00000002.305109543.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.305109543.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.305109543.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.306683734.0000000003F89000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.306683734.0000000003F89000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.306608313.0000000002F81000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.306608313.0000000002F81000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Disassembly

Code Analysis