ID: 322271
Sample Name: PO456789.exe
Cookbook: default.jbs
Time: 20:29:45
Date: 24/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

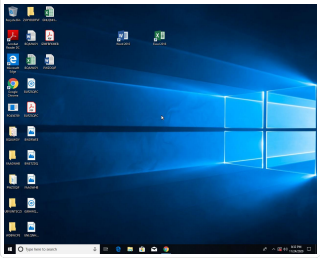
Analysis Report PO456789.exe

Overview

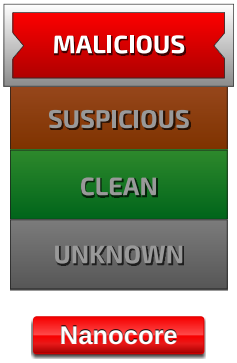
General Information

Sample Name:	PO456789.exe
Analysis ID:	322271
MD5:	6997fbda2b03ac3.
SHA1:	4d16de6b50332c..
SHA256:	6ed6aebe6d0b83..

Most interesting Screenshot:



Detection



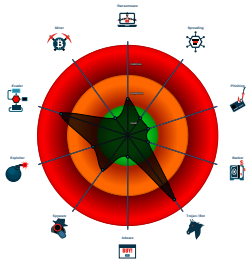
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- .NET source code contains very larg…
- Connects to many ports of the same…
- Hides that the sample has been dow…
- Protects its processes via BreakOnT…
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**

- PO456789.exe (PID: 5916 cmdline: 'C:\Users\user\Desktop\PO456789.exe' MD5: 6997FBDA2B03AC3C34FEC92ED6375E40)
  - cmd.exe (PID: 4228 cmdline: 'C:\Windows\System32\cmd.exe' /c copy 'C:\Users\user\Desktop\PO456789.exe' 'C:\Users\user\AppData\Local\fifyt.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 4816 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5988 cmdline: 'C:\Windows\System32\cmd.exe' /c, 'C:\Users\user\AppData\Local\fifyt.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6092 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - fifyt.exe (PID: 6272 cmdline: C:\Users\user\AppData\Local\fifyt.exe MD5: 6997FBDA2B03AC3C34FEC92ED6375E40)
      - cmd.exe (PID: 4940 cmdline: 'C:\Windows\System32\cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6544 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - reg.exe (PID: 4780 cmdline: REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe' MD5: CEE2A7E57DF2A159A065A34913A055C2)
      - InstallUtil.exe (PID: 6712 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
        - schtasks.exe (PID: 6716 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpC4E7.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
          - conhost.exe (PID: 6952 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - schtasks.exe (PID: 6996 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpC96C.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
          - conhost.exe (PID: 6924 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cmd.exe (PID: 6732 cmdline: 'C:\Windows\System32\cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6792 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - reg.exe (PID: 6776 cmdline: REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe' MD5: CEE2A7E57DF2A159A065A34913A055C2)
      - cmd.exe (PID: 6692 cmdline: 'C:\Windows\System32\cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6720 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - reg.exe (PID: 6968 cmdline: REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe' MD5: CEE2A7E57DF2A159A065A34913A055C2)
      - cmd.exe (PID: 204 cmdline: 'C:\Windows\System32\cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 4592 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - reg.exe (PID: 4228 cmdline: REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe' MD5: CEE2A7E57DF2A159A065A34913A055C2)
      - cmd.exe (PID: 6112 cmdline: 'C:\Windows\System32\cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 2240 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - reg.exe (PID: 5920 cmdline: REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe' MD5: CEE2A7E57DF2A159A065A34913A055C2)
      - cmd.exe (PID: 7160 cmdline: 'C:\Windows\System32\cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 7028 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - reg.exe (PID: 6896 cmdline: REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe' MD5: CEE2A7E57DF2A159A065A34913A055C2)
      - cmd.exe (PID: 6988 cmdline: 'C:\Windows\System32\cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6264 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - reg.exe (PID: 6996 cmdline: REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe' MD5: CEE2A7E57DF2A159A065A34913A055C2)
- InstallUtil.exe (PID: 4812 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe 0 MD5: EFEC8C379D165E3F33B536739AEE26A3)
  - conhost.exe (PID: 4864 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- fifyt.exe (PID: 5048 cmdline: 'C:\Users\user\AppData\Local\fifyt.exe' MD5: 6997FBDA2B03AC3C34FEC92ED6375E40)
  - InstallUtil.exe (PID: 7016 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
- dhcpmon.exe (PID: 6560 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: EFEC8C379D165E3F33B536739AEE26A3)
  - conhost.exe (PID: 5616 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)

- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "C2: ": [
    "185.244.30.212"
  ],
  "Version: ": "NanoCore Client, Version=1.2.2.0"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.916744758.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000009.00000002.916744758.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000009.00000002.916744758.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000009.00000002.922011910.000000000530000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000009.00000002.922011910.000000000530000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
Click to see the 40 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.InstallUtil.exe.62c0000.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
9.2.InstallUtil.exe.62c0000.4.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
9.2.InstallUtil.exe.62c0000.4.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
9.2.InstallUtil.exe.5530000.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
9.2.InstallUtil.exe.5530000.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
Click to see the 11 entries				

Sigma Overview

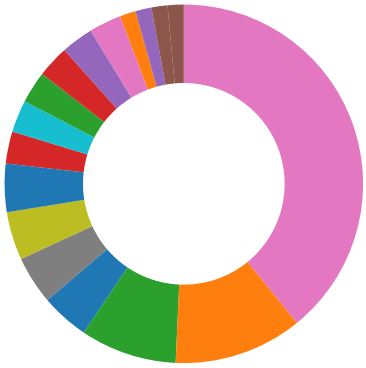
System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview

- AV Detection
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing



- E-Banking Fraud
- Operating System Destruction
- 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

Yara detected Nanocore RAT

Networking:

Connects to many ports of the same IP (likely port scanning)

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

Operating System Destruction:

Protects its processes via BreakOnTermination flag

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

Persistence and Installation Behavior:

Uses cmd line tools excessively to alter registry or file data

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:

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

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

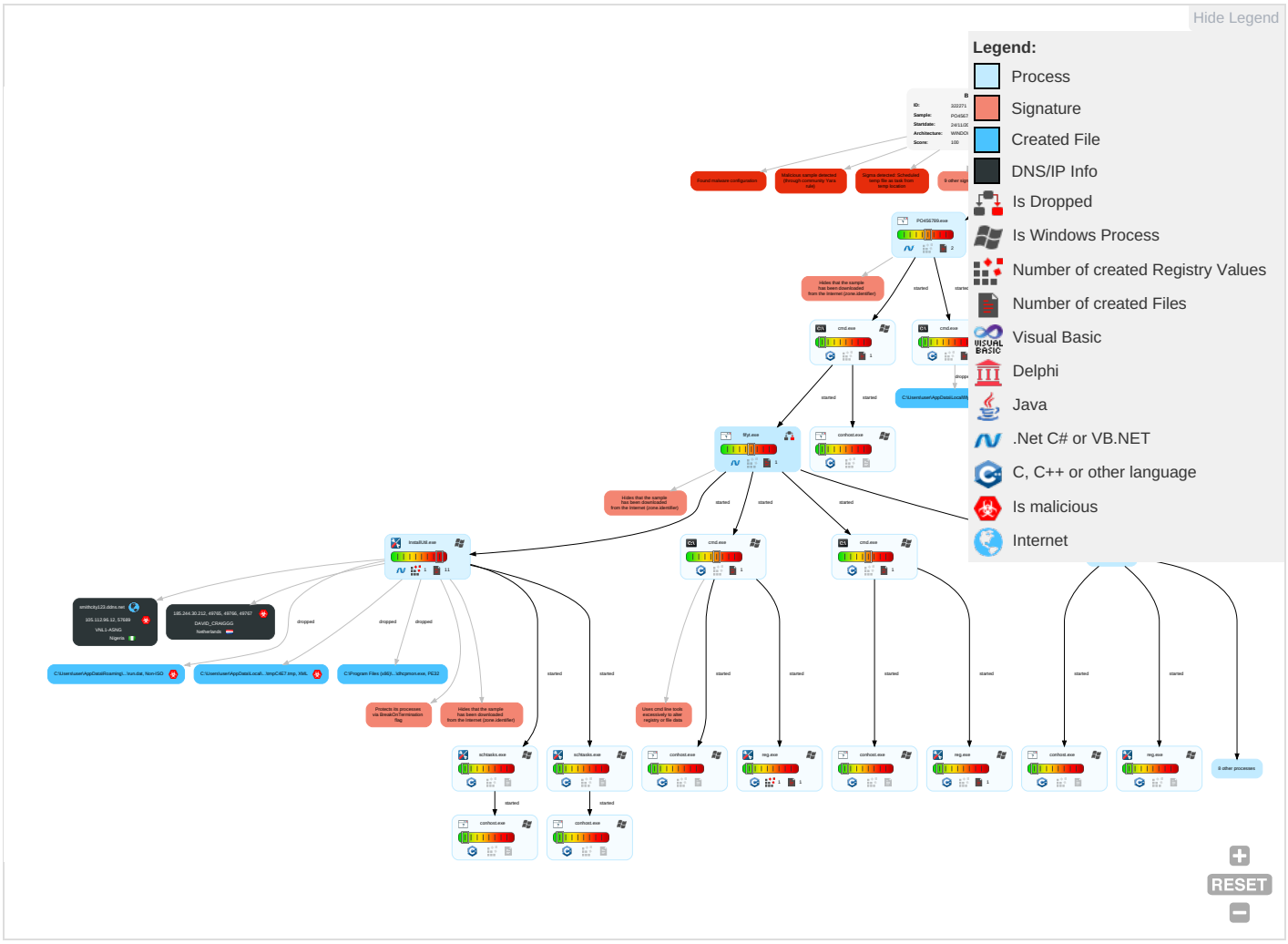
Detected Nanocore Rat

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

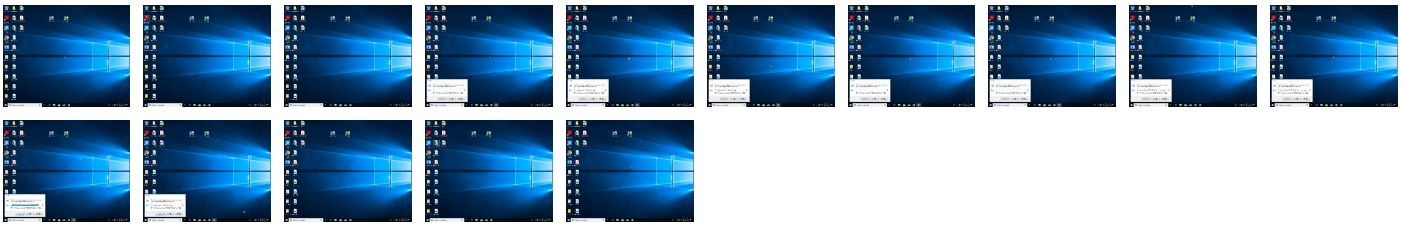
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.2.InstallUtil.exe.62c0000.4.unpack	100%	Avira	TR/NanoCore.fadte		Download File
32.2.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

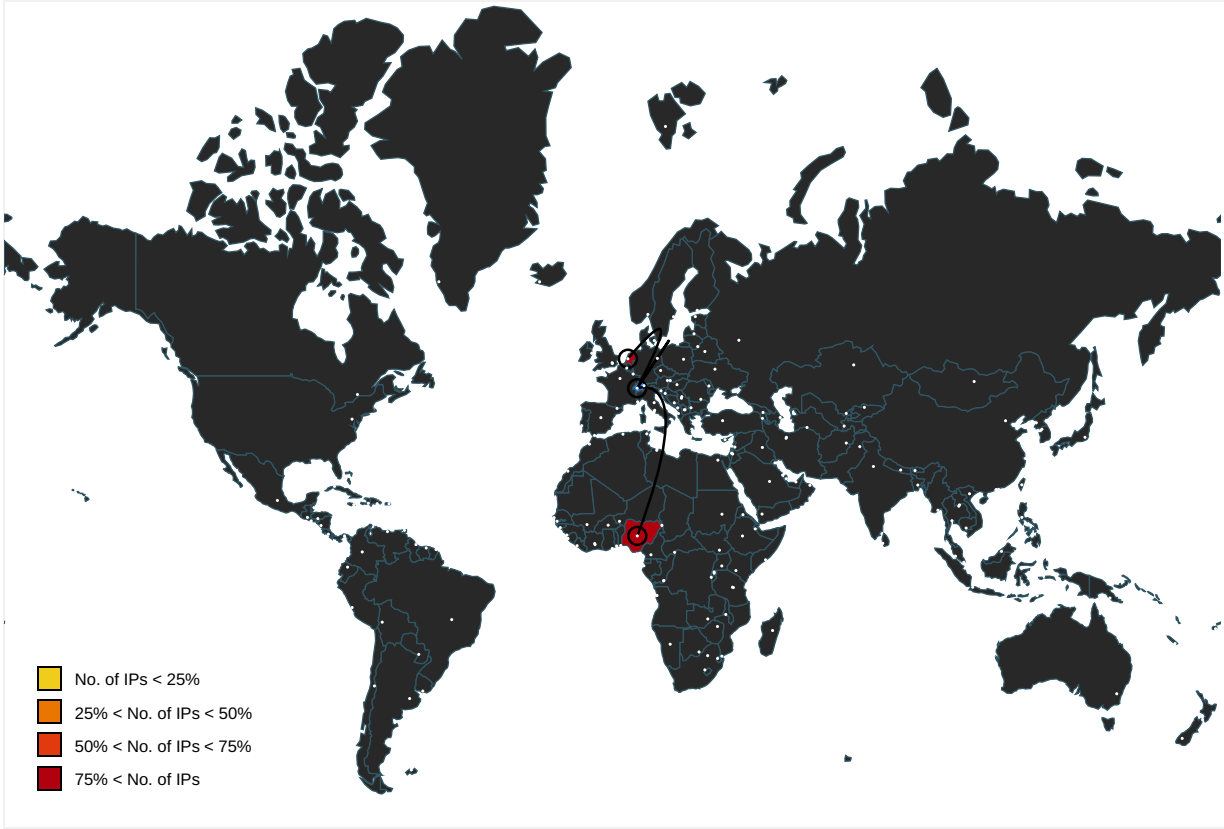
No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
smithcity123.ddns.net	105.112.96.12	true	true		unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.244.30.212	unknown	Netherlands		209623	DAVID_CRAIGGG	true
105.112.96.12	unknown	Nigeria		36873	VNL1-ASNG	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	322271
Start date:	24.11.2020
Start time:	20:29:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO456789.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	40

Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@220/11@6/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.6% (good quality ratio 0.3%) • Quality average: 39.3% • Quality standard deviation: 41.2%
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. • Exclude process from analysis (whitelisted): backgroundTaskHost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 13.88.21.125, 51.104.144.132, 93.184.221.240, 52.155.217.156, 20.54.26.129, 92.122.213.247, 92.122.213.194, 51.11.168.160 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, skypedataprdcoleus15.cloudapp.net, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, wu.wpc.apr-52dd2.edgecastdns.net, skypedataprdcolwus15.cloudapp.net, au-bg-shim.trafficmanager.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:30:46	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run fiffyt C:\Users\user\AppData\Local\fifyt.exe
20:30:52	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe" s>$(Arg0)
20:30:52	API Interceptor	923x Sleep call for process: InstallUtil.exe modified
20:30:54	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
20:30:54	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
20:31:02	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run fiffyt C:\Users\user\AppData\Local\fifyt.exe

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
smithcity123.ddns.net	FXlRSXcN37.exe	Get hash	malicious	Browse	• 185.165.153.124

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	kelvinx.exe	Get hash	malicious	Browse	• 185.140.53.132
	Order-2311.exe	Get hash	malicious	Browse	• 91.193.75.147
	YZD221120.exe	Get hash	malicious	Browse	• 91.193.75.147
	ORDER #201120A.exe	Get hash	malicious	Browse	• 185.244.30.92
	oUI0jQS8xQ.exe	Get hash	malicious	Browse	• 185.140.53.149
	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	• 185.140.53.139
	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	• 185.140.53.139
	Ups file de.exe	Get hash	malicious	Browse	• 185.140.53.221
	NyUnwsFSCa.exe	Get hash	malicious	Browse	• 185.140.53.149
	purchase order.exe	Get hash	malicious	Browse	• 185.140.53.233
	Remittance Details.xls	Get hash	malicious	Browse	• 185.140.53.184
	PaymentConfirmation.exe	Get hash	malicious	Browse	• 185.140.53.183
	ORDER #02676.doc.exe	Get hash	malicious	Browse	• 185.244.30.92
	b11305c6ab207f830062f80eeec728c4.exe	Get hash	malicious	Browse	• 185.140.53.233
	ShippingDoc.jar	Get hash	malicious	Browse	• 185.244.30.139
	1kn1ejwPxi.exe	Get hash	malicious	Browse	• 185.140.53.132
	D6vy84I7rJ.exe	Get hash	malicious	Browse	• 185.140.53.149
	7iatifHQEp.exe	Get hash	malicious	Browse	• 185.140.53.132
	Sbext4ZNBq.exe	Get hash	malicious	Browse	• 185.140.53.197
	xEdiPz1bC3.exe	Get hash	malicious	Browse	• 185.140.53.234
VNL1-ASNG	DHL_10177_R293_DOCUMENT.exe	Get hash	malicious	Browse	• 105.112.101.201
	ibgcrnNmhB.exe	Get hash	malicious	Browse	• 105.112.25.130
	purchase order.exe	Get hash	malicious	Browse	• 105.112.25.74
	packing list.xlsx.exe	Get hash	malicious	Browse	• 105.112.69.142
	9087654.exe	Get hash	malicious	Browse	• 105.112.101.151
	RFQ.exe	Get hash	malicious	Browse	• 105.112.100.239
	LOI.exe	Get hash	malicious	Browse	• 105.112.100.239
	corporate-tax.exe	Get hash	malicious	Browse	• 105.112.101.84
	QUOTATION - COVID 19 PROTECTION SOLUTIONS - final.exe	Get hash	malicious	Browse	• 105.112.124.8
	BDH9YAC4aQ.exe	Get hash	malicious	Browse	• 105.112.101.125
	JBIY8HTthL.exe	Get hash	malicious	Browse	• 105.112.101.125
	late-payment.exe	Get hash	malicious	Browse	• 105.112.45.74
	Doc0_01210_72820.exe	Get hash	malicious	Browse	• 105.112.100.246
	newage	Get hash	malicious	Browse	• 105.120.247.26
	54PDF Enclosed October Order.exe	Get hash	malicious	Browse	• 105.112.32.190
	47PDF Enclosed PO.exe	Get hash	malicious	Browse	• 105.112.42.182
	Packing List Detail.exe	Get hash	malicious	Browse	• 105.112.37.223
	5INQUIRY.exe	Get hash	malicious	Browse	• 105.112.96.111
	20New Enquiry.exe	Get hash	malicious	Browse	• 105.112.98.252

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PDF.Order#P.O.3041.exe	Get hash	malicious	Browse	• 105.112.96.11

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	31.exe	Get hash	malicious	Browse	
	ORDER FORM DENK.exe	Get hash	malicious	Browse	
	niMONOdcTZ.exe	Get hash	malicious	Browse	
	XiCfDFLACR.exe	Get hash	malicious	Browse	
	Q7kSO3iJN3.exe	Get hash	malicious	Browse	
	BL, Invoices.exe	Get hash	malicious	Browse	
	crypt.exe	Get hash	malicious	Browse	
	IEcYhddAMD.exe	Get hash	malicious	Browse	
	FRI5A2QZI7.exe	Get hash	malicious	Browse	
	kM16L0Vybr.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Generic.mg.e1df690a980825ac.exe	Get hash	malicious	Browse	
	9SI5dPQJ7G.exe	Get hash	malicious	Browse	
	FH11m70Scj.exe	Get hash	malicious	Browse	
	http://cdn.discordapp.com/attachments/776234221668270104/776349109195898880/AWB_DHL733918737WA56301224799546260.pdf.7z	Get hash	malicious	Browse	
	bKs9QjrX1q.exe	Get hash	malicious	Browse	
	Y7ET38qc5y.exe	Get hash	malicious	Browse	
	IIOCxnn1ho.exe	Get hash	malicious	Browse	
	Jn3wr6uaNK.exe	Get hash	malicious	Browse	
	ODoXtvoj7j.exe	Get hash	malicious	Browse	
	jG1KyDSHKK.exe	Get hash	malicious	Browse	

Created / dropped Files

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	41064
Entropy (8bit):	6.164873449128079
Encrypted:	false
SSDEEP:	384:FtpFVLK0MsihB9VKS7xdgE7KJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+sPZTd:ZBMs2SqdD86Iq8gZZFyViML3an
MD5:	EFEC8C379D165E3F33B536739AEE26A3
SHA1:	C875908ACBA5CAC1E0B40F06A83F0F156A2640FA
SHA-256:	46DEE184523A584E56DF93389F81992911A1BA6B1F05AD7D803C6AB1450E18CB
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCFF
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Joe Sandbox View:	• Filename: 31.exe, Detection: malicious, Browse • Filename: ORDER FORM DENK.exe, Detection: malicious, Browse • Filename: niMONOdcTZ.exe, Detection: malicious, Browse • Filename: XiCfDFLACR.exe, Detection: malicious, Browse • Filename: Q7kSO3iJN3.exe, Detection: malicious, Browse • Filename: BL, Invoices.exe, Detection: malicious, Browse • Filename: crypt.exe, Detection: malicious, Browse • Filename: IEcYhddAMD.exe, Detection: malicious, Browse • Filename: FRI5A2QZI7.exe, Detection: malicious, Browse • Filename: kM16L0Vybr.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Generic.mg.e1df690a980825ac.exe, Detection: malicious, Browse • Filename: 9SI5dPQJ7G.exe, Detection: malicious, Browse • Filename: FH11m70Scj.exe, Detection: malicious, Browse • Filename: , Detection: malicious, Browse • Filename: bKs9QjrX1q.exe, Detection: malicious, Browse • Filename: Y7ET38qc5y.exe, Detection: malicious, Browse • Filename: IIOCxnn1ho.exe, Detection: malicious, Browse • Filename: Jn3wr6uaNK.exe, Detection: malicious, Browse • Filename: ODoXtvoj7j.exe, Detection: malicious, Browse • Filename: jG1KyDSHKK.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....0..T.....r... .....@.. ....`.....4r..O.....b..h>.....p..... ..... ..H.....text....R... ...T..... ..`.rsrc.....V.....@..@.rel oc.....`.....@..B.....hr.....H.....".|J.....lm.....o.....2~.....o....*.r...p(....*VrK..p(....s.....*..0.....(....(....o....o....(....o.... .....T(....o....(....o....o ...o!....4(....o....(....o....o ...o".....(....rm..ps#...o....($.....(%....o&....ry..p.....%.r...p.%.(.....(....('....((.....o)...('.....*.*.....".(*...*..{Q...-...}Q.....(+...(....(,....(+...*"..(- ...*..(....*..(.....r...p.(/...o0...s....}T...*....0.. .....~S...-.s

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\InstallUtil.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	329
Entropy (8bit):	5.324195011891804
Encrypted:	false
SSDEEP:	6:Q3La/xwc1K9rDLIP12MUAvvr3tDLIP12MUAvvR+uTL2LDY3U21v:Q3La/h1K9rDLI4M9tDLI4MWuPk21v
MD5:	0F3825E2D8885E05820523A5D8DFEF9C
SHA1:	E6AA2D5D00CE5F875C75B9490F21F2D6B3F0DED3
SHA-256:	2F3769543004FF49CB3B6EF06AC5FD6A402DB0C2546E365639338CA2F4049EBE
SHA-512:	D8FBAEEABF2D33EAF4FF5AADEBF86C233145502560A42B88EBDE455AE2B001F52728E4CE6C59DBCCA37CBF25BA485F5FC5527E992AB66957C6252CF1956F23 7C
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Configuration.Install, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Vers ion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6 \System.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO456789.exe.log	
Process:	C:\Users\user\Desktop\PO456789.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1546
Entropy (8bit):	5.346743488670314
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjovjHKx1qHj:iqXeqm00YqhQnouRqjorqxwD
MD5:	EC192028815A73A0E57822511039BF45
SHA1:	56B71389DEC83E8077FC8AF6DA490430EA64190F
SHA-256:	3827EF46D6BAB96F1ABAEAEFF5ABF04569543CD10E8AA6113B4DB419D6E5B03E
SHA-512:	0CBDE42DF33CC0B5CE880A14996F7F7ACA6BA398468952A609046BA7E37243554B04E4B7856CC1318333AC142B8D432D4B1BF2A0434E12BF80387A671F64B991
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf 3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"Present ationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f #\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",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,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

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:	modified
Size (bytes):	329
Entropy (8bit):	5.324195011891804

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Encrypted:	false
SSDEEP:	6:Q3La/xwc1K9rDLIP12MUAvvr3tDLIP12MUAvvR+uTL2LDY3U21v:Q3La/h1K9rDLI4M9tDLI4MWuPk21v
MD5:	0F3825E2D8885E05820523A5D8DFEF9C
SHA1:	E6AA2D5D00CE5F875C75B9490F21F2D6B3F0DED3
SHA-256:	2F3769543004FF49CB3B6EF06AC5FD6A402DB0C2546E365639338CA2F4049EBE
SHA-512:	D8FBAEEABF2D33EAF4FF5AADEBF86C233145502560A42B88EBDE455AE2B001F52728E4CE6C59DBCCA37CBF25BA485F5FC5527E992AB66957C6252CF1956F23 7C
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Configuration.Install, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Vers ion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6 \System.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmpC4E7.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1324
Entropy (8bit):	5.130789568721151
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mlxtn:cbk4oL600QydbQxIYODOLedq3Zlj
MD5:	576BBAF398045C3843D452EC83208236
SHA1:	8ED5B2500AE7A40CBFA6E9018A1D1F1E70CB1374
SHA-256:	33C0C2D72FA383E5988CE640FEBC5AC6A2BD71D4AE660B99E52234952E17467B
SHA-512:	E7CC0EA0B351C6A8618E14F03C00E88EF83E2F169E0B4D66513F580F0A9352FBFE429E57186362B69407150D566BBDADCA2F7B574FC748CC140B3249BE67F96A
Malicious:	**true**
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>.. <StopIfGoingOnBatterie s>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAv ailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </Idl eSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpC96C.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
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
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>.. <StopIfGoingOnBatterie s>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAv ailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </Idl eSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\fifyt.exe	
Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	595456
Entropy (8bit):	6.277264014356029
Encrypted:	false
SSDEEP:	12288:Gn5PqttqmMwFHo3ggmmz7dBfRdGacGJQb+oT8:YlqSmMwFHQggvzBBfRdGac+
MD5:	6997FBDA2B03AC3C34FEC92ED6375E40
SHA1:	4D16DE6B50332CC05FCA066125937C364DDA961F
SHA-256:	6ED6AEBE6D0B839AB5A5BEBAD7D58D72445146AFA8EE9742F9B0E287F007B3C4

C:\Users\user\AppData\Local\fifyt.exe	
SHA-512:	C10EFA2A625D3BCCD43B81BC9EDFF5CA43FF9B6D57E8185C111DA7496FC0CDB23706DE9CEA1D8ADD20ECB7B1F252290DA68C3A37A73585C1419C8C56B6C54AC
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....D.....n*... ...@....@.. ....`.....*..O....@.....`..... ....H.....text...t.... ....`.rsrc.....@.....@..@.reloc.....` .....@..B.....P*.....H.....*.....V.....&\.....z....;y....E.(Z..l.....X8...F.5._.[{.....Q..I./...FQ.ED.....2...f...AU...[.....>tM.S<....>.o.f.....1 (aPs..X.B.z.]..'J...$.i._Dp.....>.f.Z....C!.....s..b+N..+.....2&...n6.R..e'.....n.(....#...?qt....d.?.Uq./T...k<Wu....k....A..-.....c... s>>F..P...{.N.a\..3.....`|...{.'^@.S...+_`..7.....9.....'u \...P.0$..E}..y..O.....eL...\.z.^fB&....bW.o.9.6....cm.....tG.C..\.RG.H..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:GXK3tn:AKdn
MD5:	274BB67DF1F631159FB981CAE1616E40
SHA1:	F87AEE2FB9B9568ECF78E441AE04EEC5AB9CF4BC
SHA-256:	EEB9380E9350BDDEDB8BE2332F7A9AC5D08732853279AED361B55DA0933CE9D6
SHA-512:	1ABFA469868A8F3AAF96646CC58C179CD7393A38B83B80C29C7B149AD76D0C648898F8631790F48A8D28164C672FB5EB3C02EB167AD2500C398302718F7B8064
Malicious:	**true**
Preview:	o..r...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	61
Entropy (8bit):	4.84649200170358
Encrypted:	false
SSDEEP:	3:oMty8WddSNARI0dAn:oMLW6qRndA
MD5:	1EFF0939B507F9B297DCB06A4C0413B8
SHA1:	8131E01D9969CD60A0241E71727E56749AB53B31
SHA-256:	C8BBFDF650E881719F8E623E5FF54AAFE25B64B351E44077B511071AB08AE903
SHA-512:	81E8AE0346984643A56CA92323F7687E648130AB61A5AA8E4706DD1B2FC56B1974C06923003343B53391E1018D07BA5090222899F5FA4F4F8327995763BF84FE
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	359
Entropy (8bit):	4.8928974699064005
Encrypted:	false
SSDEEP:	6:zx3M7bWXRLuRc4LQtUmYRZBXVNYxxEQgz3MBL3RgKRLLyqbbUcfvfAL/BM7GRJpF:zKnWXQRzA4BFNYxx5ggBDX7HfvfU66rF
MD5:	1CEB9B01195234DD4E4CEBEFC4425CA6
SHA1:	674D41B247D4F20F5C0F04DF476539555FD94EED
SHA-256:	9A941C6BA5D12DF1D05D345125CA38DCA56C2BE4FF4FEF02B29C4B4F4E67B433
SHA-512:	0FCDF334529F9F659D53666EE4F33216A6BB58E52BDA61181A0E7EC75FDD1FA8A681C4FA8CC671372D7F8089AD94C7C12DCA85BBC50A2182C265D79AFEC479C
Malicious:	false
Preview:	Microsoft (R) .NET Framework Installation utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....Exception occurred while initializing the installation:..System.IO.FileNotFoundException: Could not load file or assembly 'file:///C:\Windows\system32\0' or one of its dependencies. The system cannot find the file specified....

Static File Info

General

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.277264014356029
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:	PO456789.exe
File size:	595456
MD5:	6997fbda2b03ac3c34fec92ed6375e40
SHA1:	4d16de6b50332cc05fca066125937c364dda961f
SHA256:	6ed6aebe6d0b839ab5a5bebad7d58d72445146afa8ee9742f9b0e287f007b3c4
SHA512:	c10efa2a625d3bccd43b81bc9edff5ca43ff9b6d57e8185c111da7496fc0cdb23706de9cea1d8add20ecb7b1f252290da68c3a37a73585c1419c8c56b6c574ac
SSDEEP:	12288:Gn5PqttqmMwFHo3ggmmz7dBfRdGacGJQb+oT8:YlqSmMwFHQggvzBBfRdGac+
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....D.....n*... ...@....@.. .....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x492a6e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x44ECE4BC [Wed Aug 23 23:29:00 2006 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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x92a1c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x94000	0x596	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x96000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x90a74	0x90c00	False	0.590951870142	data	6.28617887105	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x94000	0x596	0x600	False	0.4140625	data	4.06252531054	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x96000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x940a0	0x30c	data		
RT_MANIFEST	0x943ac	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

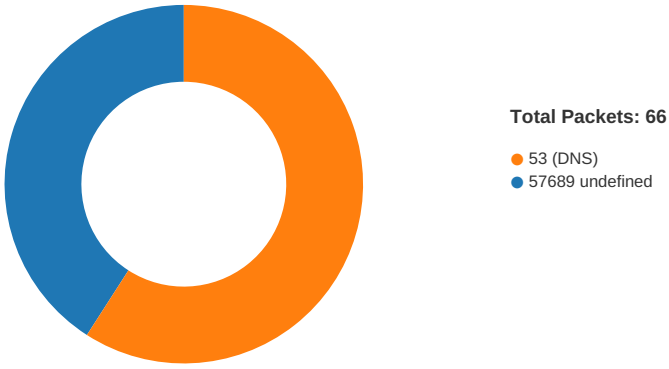
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2020
Assembly Version	1.0.0.0
InternalName	Stub37.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	Stub37
ProductVersion	1.0.0.0
FileDescription	Stub37
OriginalFilename	Stub37.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2020 20:30:54.693972111 CET	49733	57689	192.168.2.4	105.112.96.12
Nov 24, 2020 20:30:57.750633955 CET	49733	57689	192.168.2.4	105.112.96.12
Nov 24, 2020 20:31:03.915282011 CET	49733	57689	192.168.2.4	105.112.96.12
Nov 24, 2020 20:31:12.010874033 CET	49741	57689	192.168.2.4	105.112.96.12
Nov 24, 2020 20:31:15.025546074 CET	49741	57689	192.168.2.4	105.112.96.12
Nov 24, 2020 20:31:21.026057005 CET	49741	57689	192.168.2.4	105.112.96.12
Nov 24, 2020 20:31:29.038765907 CET	49754	57689	192.168.2.4	105.112.96.12
Nov 24, 2020 20:31:32.042599916 CET	49754	57689	192.168.2.4	105.112.96.12
Nov 24, 2020 20:31:38.074345112 CET	49754	57689	192.168.2.4	105.112.96.12
Nov 24, 2020 20:31:45.705604076 CET	49765	57689	192.168.2.4	185.244.30.212
Nov 24, 2020 20:31:45.764708042 CET	57689	49765	185.244.30.212	192.168.2.4
Nov 24, 2020 20:31:46.278141022 CET	49765	57689	192.168.2.4	185.244.30.212
Nov 24, 2020 20:31:46.337778091 CET	57689	49765	185.244.30.212	192.168.2.4
Nov 24, 2020 20:31:46.840739012 CET	49765	57689	192.168.2.4	185.244.30.212
Nov 24, 2020 20:31:46.900777102 CET	57689	49765	185.244.30.212	192.168.2.4
Nov 24, 2020 20:31:51.232747078 CET	49766	57689	192.168.2.4	185.244.30.212
Nov 24, 2020 20:31:51.292907000 CET	57689	49766	185.244.30.212	192.168.2.4
Nov 24, 2020 20:31:51.794209957 CET	49766	57689	192.168.2.4	185.244.30.212
Nov 24, 2020 20:31:51.854765892 CET	57689	49766	185.244.30.212	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2020 20:31:52.357130051 CET	49766	57689	192.168.2.4	185.244.30.212
Nov 24, 2020 20:31:52.416743040 CET	57689	49766	185.244.30.212	192.168.2.4
Nov 24, 2020 20:31:56.420990944 CET	49767	57689	192.168.2.4	185.244.30.212
Nov 24, 2020 20:31:56.480937958 CET	57689	49767	185.244.30.212	192.168.2.4
Nov 24, 2020 20:31:56.982134104 CET	49767	57689	192.168.2.4	185.244.30.212
Nov 24, 2020 20:31:57.041433096 CET	57689	49767	185.244.30.212	192.168.2.4
Nov 24, 2020 20:31:57.545876980 CET	49767	57689	192.168.2.4	185.244.30.212
Nov 24, 2020 20:31:57.605487108 CET	57689	49767	185.244.30.212	192.168.2.4
Nov 24, 2020 20:32:01.706033945 CET	49768	57689	192.168.2.4	105.112.96.12
Nov 24, 2020 20:32:04.701545954 CET	49768	57689	192.168.2.4	105.112.96.12
Nov 24, 2020 20:32:10.702197075 CET	49768	57689	192.168.2.4	105.112.96.12
Nov 24, 2020 20:32:18.344161987 CET	49773	57689	192.168.2.4	105.112.96.12
Nov 24, 2020 20:32:21.359322071 CET	49773	57689	192.168.2.4	105.112.96.12
Nov 24, 2020 20:32:27.359617949 CET	49773	57689	192.168.2.4	105.112.96.12
Nov 24, 2020 20:32:35.016170979 CET	49774	57689	192.168.2.4	105.112.96.12
Nov 24, 2020 20:32:38.016824007 CET	49774	57689	192.168.2.4	105.112.96.12
Nov 24, 2020 20:32:44.017311096 CET	49774	57689	192.168.2.4	105.112.96.12

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2020 20:30:44.678797007 CET	49910	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:30:44.705682993 CET	53	49910	8.8.8.8	192.168.2.4
Nov 24, 2020 20:30:45.484963894 CET	55854	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:30:45.511976957 CET	53	55854	8.8.8.8	192.168.2.4
Nov 24, 2020 20:30:46.542421103 CET	64549	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:30:46.569574118 CET	53	64549	8.8.8.8	192.168.2.4
Nov 24, 2020 20:30:53.437715054 CET	63153	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:30:53.464725018 CET	53	63153	8.8.8.8	192.168.2.4
Nov 24, 2020 20:30:54.643064976 CET	52991	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:30:54.680453062 CET	53	52991	8.8.8.8	192.168.2.4
Nov 24, 2020 20:30:54.845729113 CET	53700	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:30:54.872944117 CET	53	53700	8.8.8.8	192.168.2.4
Nov 24, 2020 20:30:57.835988998 CET	51726	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:30:57.871826887 CET	53	51726	8.8.8.8	192.168.2.4
Nov 24, 2020 20:30:58.538731098 CET	56794	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:30:58.565850973 CET	53	56794	8.8.8.8	192.168.2.4
Nov 24, 2020 20:30:58.579524040 CET	56534	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:30:58.606662035 CET	53	56534	8.8.8.8	192.168.2.4
Nov 24, 2020 20:30:59.639020920 CET	56627	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:30:59.674792051 CET	53	56627	8.8.8.8	192.168.2.4
Nov 24, 2020 20:31:03.403490067 CET	56621	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:31:03.469991922 CET	53	56621	8.8.8.8	192.168.2.4
Nov 24, 2020 20:31:11.971190929 CET	63116	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:31:12.008527994 CET	53	63116	8.8.8.8	192.168.2.4
Nov 24, 2020 20:31:19.328739882 CET	64078	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:31:19.355988026 CET	53	64078	8.8.8.8	192.168.2.4
Nov 24, 2020 20:31:19.775859118 CET	64801	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:31:19.802894115 CET	53	64801	8.8.8.8	192.168.2.4
Nov 24, 2020 20:31:20.135490894 CET	61721	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:31:20.171039104 CET	53	61721	8.8.8.8	192.168.2.4
Nov 24, 2020 20:31:20.777755022 CET	51255	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:31:20.818367958 CET	53	51255	8.8.8.8	192.168.2.4
Nov 24, 2020 20:31:21.131675959 CET	61522	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:31:21.167100906 CET	53	61522	8.8.8.8	192.168.2.4
Nov 24, 2020 20:31:21.787940979 CET	52337	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:31:21.823509932 CET	53	52337	8.8.8.8	192.168.2.4
Nov 24, 2020 20:31:22.114726067 CET	55046	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:31:22.141712904 CET	53	55046	8.8.8.8	192.168.2.4
Nov 24, 2020 20:31:22.455543995 CET	49612	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:31:22.490964890 CET	53	49612	8.8.8.8	192.168.2.4
Nov 24, 2020 20:31:22.878814936 CET	49285	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:31:22.914417982 CET	53	49285	8.8.8.8	192.168.2.4
Nov 24, 2020 20:31:23.341555119 CET	50601	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 24, 2020 20:31:23.368742943 CET	53	50601	8.8.8.8	192.168.2.4
Nov 24, 2020 20:31:23.615839005 CET	60875	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:31:23.618319988 CET	56448	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:31:23.642846107 CET	53	60875	8.8.8.8	192.168.2.4
Nov 24, 2020 20:31:23.664068937 CET	53	56448	8.8.8.8	192.168.2.4
Nov 24, 2020 20:31:28.986315966 CET	59172	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:31:29.021948099 CET	53	59172	8.8.8.8	192.168.2.4
Nov 24, 2020 20:31:35.705284119 CET	62420	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:31:35.732440948 CET	53	62420	8.8.8.8	192.168.2.4
Nov 24, 2020 20:31:37.506514072 CET	60579	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:31:37.543237925 CET	53	60579	8.8.8.8	192.168.2.4
Nov 24, 2020 20:31:38.117646933 CET	50183	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:31:38.144689083 CET	53	50183	8.8.8.8	192.168.2.4
Nov 24, 2020 20:31:39.269773960 CET	61531	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:31:39.296787977 CET	53	61531	8.8.8.8	192.168.2.4
Nov 24, 2020 20:31:39.942400932 CET	49228	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:31:39.969536066 CET	53	49228	8.8.8.8	192.168.2.4
Nov 24, 2020 20:31:40.963196993 CET	59794	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:31:40.990212917 CET	53	59794	8.8.8.8	192.168.2.4
Nov 24, 2020 20:31:41.633445978 CET	55916	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:31:41.660645008 CET	53	55916	8.8.8.8	192.168.2.4
Nov 24, 2020 20:32:01.647542000 CET	52752	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:32:01.686784983 CET	53	52752	8.8.8.8	192.168.2.4
Nov 24, 2020 20:32:06.878326893 CET	60542	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:32:06.905380011 CET	53	60542	8.8.8.8	192.168.2.4
Nov 24, 2020 20:32:07.612168074 CET	60689	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:32:07.648063898 CET	53	60689	8.8.8.8	192.168.2.4
Nov 24, 2020 20:32:11.721676111 CET	64206	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:32:11.748917103 CET	53	64206	8.8.8.8	192.168.2.4
Nov 24, 2020 20:32:12.806418896 CET	50904	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:32:12.844140053 CET	53	50904	8.8.8.8	192.168.2.4
Nov 24, 2020 20:32:18.290870905 CET	57525	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:32:18.330842972 CET	53	57525	8.8.8.8	192.168.2.4
Nov 24, 2020 20:32:34.979161978 CET	53814	53	192.168.2.4	8.8.8.8
Nov 24, 2020 20:32:35.014664888 CET	53	53814	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 24, 2020 20:30:54.643064976 CET	192.168.2.4	8.8.8.8	0xd467	Standard query (0)	smithcity1 23.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2020 20:31:11.971190929 CET	192.168.2.4	8.8.8.8	0xb0cb	Standard query (0)	smithcity1 23.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2020 20:31:28.986315966 CET	192.168.2.4	8.8.8.8	0x1b84	Standard query (0)	smithcity1 23.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2020 20:32:01.647542000 CET	192.168.2.4	8.8.8.8	0x37f5	Standard query (0)	smithcity1 23.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2020 20:32:18.290870905 CET	192.168.2.4	8.8.8.8	0x91dc	Standard query (0)	smithcity1 23.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2020 20:32:34.979161978 CET	192.168.2.4	8.8.8.8	0x43e2	Standard query (0)	smithcity1 23.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

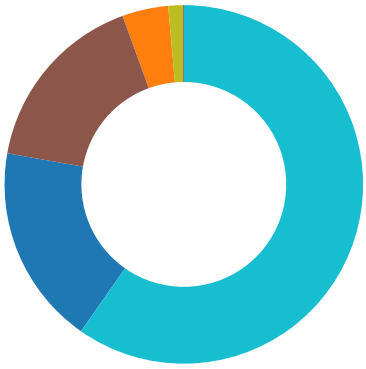
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 24, 2020 20:30:54.680453062 CET	8.8.8.8	192.168.2.4	0xd467	No error (0)	smithcity1 23.ddns.net		105.112.96.12	A (IP address)	IN (0x0001)
Nov 24, 2020 20:31:12.008527994 CET	8.8.8.8	192.168.2.4	0xb0cb	No error (0)	smithcity1 23.ddns.net		105.112.96.12	A (IP address)	IN (0x0001)
Nov 24, 2020 20:31:29.021948099 CET	8.8.8.8	192.168.2.4	0x1b84	No error (0)	smithcity1 23.ddns.net		105.112.96.12	A (IP address)	IN (0x0001)
Nov 24, 2020 20:32:01.686784983 CET	8.8.8.8	192.168.2.4	0x37f5	No error (0)	smithcity1 23.ddns.net		105.112.96.12	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 24, 2020 20:32:18.330842972 CET	8.8.8.8	192.168.2.4	0x91dc	No error (0)	smithcity1 23.ddns.net		105.112.96.12	A (IP address)	IN (0x0001)
Nov 24, 2020 20:32:35.014664888 CET	8.8.8.8	192.168.2.4	0x43e2	No error (0)	smithcity1 23.ddns.net		105.112.96.12	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



- PO456789.exe
- cmd.exe
- conhost.exe
- cmd.exe
- conhost.exe
- fifyt.exe
- cmd.exe
- conhost.exe
- reg.exe
- InstallUtil.exe
- cmd.exe
- conhost.exe
- reg.exe
- cmd.exe
- conhost.exe
- schtasks.exe
- reg.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- InstallUtil.exe
- conhost.exe
- cmd.exe
- conhost.exe
- reg.exe
- fifyt.exe
- dhcpmon.exe
- conhost.exe
- cmd.exe
- conhost.exe
- reg.exe
- InstallUtil.exe
- cmd.exe
- conhost.exe
- reg.exe
- cmd.exe
- conhost.exe
- reg.exe

Click to jump to process

System Behavior

Analysis Process: PO456789.exe PID: 5916 Parent PID: 5868

General

Start time:	20:30:34
Start date:	24/11/2020
Path:	C:\Users\user\Desktop\PO456789.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\Desktop\PO456789.exe'
Imagebase:	0xa10000
File size:	595456 bytes
MD5 hash:	6997FBDA2B03AC3C34FEC92ED6375E40
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: 00000000.00000002.667325612.00000000047CF000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.667325612.00000000047CF000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.667325612.00000000047CF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.666493336.00000000046D1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.666493336.00000000046D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.666493336.00000000046D1000.00000004.00000001.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\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO456789.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D48C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PO456789.exe:Zone.Identifier	success or wait	1	2BF8FB3	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO456789.exe.log	unknown	1546	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=	success or wait	1	6D48C907	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	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6D0B03DE	ReadFile

Analysis Process: cmd.exe PID: 4228 Parent PID: 5916

General

Start time:	20:30:37
Start date:	24/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c copy 'C:\Users\user\Desktop\PO456789.exe' 'C:\Users\user\AppData\Local\fifyt.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\fifyt.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	11D4E97	CopyFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\fifyt.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 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 bc e4 ec 44 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 0c 09 00 00 08 00 00 00 00 00 00 6e 2a 09 00 00 20 00 00 00 40 09 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 80 09 00 00 02 00 00 00 00 00 00 02 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......D.......... ....n*... ...@....@.. ....`................	success or wait	3	11D4E97	CopyFileExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PO456789.exe	unknown	512	success or wait	1	11D5742	ReadFile

Analysis Process: conhost.exe PID: 4816 Parent PID: 4228

General

Start time:	20:30:38
Start date:	24/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: cmd.exe PID: 5988 Parent PID: 5916

General

Start time:	20:30:39
Start date:	24/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c, 'C:\Users\user\AppData\Local\fifyt.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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

Analysis Process: conhost.exe PID: 6092 Parent PID: 5988

General

Start time:	20:30:40
Start date:	24/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: fifyt.exe PID: 6272 Parent PID: 5988

General

Start time:	20:30:40
Start date:	24/11/2020
Path:	C:\Users\user\AppData\Local\fifyt.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\fifyt.exe
Imagebase:	0x1c0000

File size:	595456 bytes
MD5 hash:	6997FBDA2B03AC3C34FEC92ED6375E40
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: 00000005.00000002.919007520.0000000003EFF000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.919007520.0000000003EFF000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.919007520.0000000003EFF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.918869911.0000000003E01000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.918869911.0000000003E01000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.918869911.0000000003E01000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6D0B03DE	ReadFile
C:\Users\user\AppData\Local\fifyt.exe	unknown	4096	success or wait	146	6BFC1B4F	ReadFile
C:\Users\user\AppData\Local\fifyt.exe	unknown	4096	success or wait	146	6BFC1B4F	ReadFile

Analysis Process: cmd.exe PID: 4940 Parent PID: 6272

General

Start time:	20:30:44
Start date:	24/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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

Analysis Process: conhost.exe PID: 6544 Parent PID: 4940

General

Start time:	20:30:44
Start date:	24/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: reg.exe PID: 4780 Parent PID: 4940

General

Start time:	20:30:45
Start date:	24/11/2020
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe'
Imagebase:	0x1120000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
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

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	fiffyt	unicode	C:\Users\user\AppData\Local\fifyt.exe	success or wait	1	1125A1D	RegSetValueExW

Analysis Process: InstallUtil.exe PID: 6712 Parent PID: 6272

General

Start time:	20:30:46
Start date:	24/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Imagebase:	0x860000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
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: 00000009.00000002.916744758.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.916744758.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.916744758.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.922011910.0000000005530000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.922011910.0000000005530000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.918066264.0000000002AF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.918936190.0000000003B39000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.918936190.0000000003B39000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.922273053.00000000062C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.922273053.00000000062C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.922273053.00000000062C0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

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	6D17CF06	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	6D17CF06	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	6BFCBEFF	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	6BFC1E60	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	6BFCBEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6BFCDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpC4E7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BFC7038	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	6BFC1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpC96C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BFC7038	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	6BFCBEFF	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	6BFCBEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC4E7.tmp	success or wait	1	6BFC6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpC96C.tmp	success or wait	1	6BFC6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	6f c4 c8 72 af 90 d8 48	o..r...H	success or wait	1	6BFC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	41064	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 07 5a 8e 5a 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 54 00 00 00 0c 00 00 00 00 00 00 86 72 00 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 c0 00 00 00 02 00 00 9a 80 01 00 03 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....Z.Z.......... ....0..T...........r... ....@.. ....`................	success or wait	1	6BFCDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpC4E7.tmp	unknown	1324	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.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	6BFC1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	61	43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 5c 76 34 2e 30 2e 33 30 33 31 39 5c 49 6e 73 74 61 6c 6c 55 74 69 6c 2e 65 78 65	C:\Windows\Microsoft.NET \Frame work\v4.0.30319\InstallUtil.exe	success or wait	1	6BFC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC96C.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	6BFC1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6D15CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6D15CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D13D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D13D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe	unknown	4096	success or wait	1	6D13D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe	unknown	512	success or wait	1	6D13D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe.config	unknown	8173	end of file	1	6D155705	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	6BFC646A	RegSetValueExW

Analysis Process: cmd.exe PID: 6732 Parent PID: 6272

General

Start time:	20:30:46
Start date:	24/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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

Analysis Process: conhost.exe PID: 6792 Parent PID: 6732

General

Start time:	20:30:46
Start date:	24/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: reg.exe PID: 6776 Parent PID: 6732

General

Start time:	20:30:47
Start date:	24/11/2020
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe'
Imagebase:	0x1120000
File size:	59392 bytes

MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
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

Analysis Process: cmd.exe PID: 6692 Parent PID: 6272

General

Start time:	20:30:48
Start date:	24/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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

Analysis Process: conhost.exe PID: 6720 Parent PID: 6692

General

Start time:	20:30:49
Start date:	24/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6716 Parent PID: 6712

General

Start time:	20:30:49
Start date:	24/11/2020
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\tmpC4E7.tmp'
Imagebase:	0xf40000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 6968 Parent PID: 6692

General

Start time:	20:30:49
Start date:	24/11/2020
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe'
Imagebase:	0x1120000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6952 Parent PID: 6716

General

Start time:	20:30:50
Start date:	24/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: 6996 Parent PID: 6712

General

Start time:	20:30:50
Start date:	24/11/2020
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\tmpC96C.tmp'
Imagebase:	0xf40000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6924 Parent PID: 6996

General

Start time:	20:30:51
Start date:	24/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: InstallUtil.exe PID: 4812 Parent PID: 968

General

Start time:	20:30:52
Start date:	24/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe 0
Imagebase:	0x870000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 4864 Parent PID: 4812

General

Start time:	20:30:52
Start date:	24/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 204 Parent PID: 6272

General

Start time:	20:30:53
Start date:	24/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true

Commandline:	'C:\Windows\System32\cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 4592 Parent PID: 204

General

Start time:	20:30:53
Start date:	24/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 4228 Parent PID: 204

General

Start time:	20:30:54
Start date:	24/11/2020
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe'
Imagebase:	0x1120000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: fifyt.exe PID: 5048 Parent PID: 3424

General

Start time:	20:30:54
Start date:	24/11/2020
Path:	C:\Users\user\AppData\Local\fifyt.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\fifyt.exe'
Imagebase:	0x860000
File size:	595456 bytes
MD5 hash:	6997FBDA2B03AC3C34FEC92ED6375E40
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: 0000001A.00000002.918889108.0000000004521000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000002.918889108.0000000004521000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000002.918889108.0000000004521000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001A.00000002.919031483.000000000461F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001A.00000002.919031483.000000000461F000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001A.00000002.919031483.000000000461F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: dhcpmon.exe PID: 6560 Parent PID: 968

General

Start time:	20:30:54
Start date:	24/11/2020
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x250000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: conhost.exe PID: 5616 Parent PID: 6560

General

Start time:	20:30:55
Start date:	24/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6112 Parent PID: 6272

General

Start time:	20:30:55
Start date:	24/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe'

Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 2240 Parent PID: 6112

General

Start time:	20:30:56
Start date:	24/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 5920 Parent PID: 6112

General

Start time:	20:30:56
Start date:	24/11/2020
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe'
Imagebase:	0x1120000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: InstallUtil.exe PID: 7016 Parent PID: 5048

General

Start time:	20:30:57
Start date:	24/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Imagebase:	0x520000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
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: 00000020.00000002.721312091.0000000003899000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000002.721312091.0000000003899000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000020.00000002.720376999.0000000002891000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000002.720376999.0000000002891000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000020.00000002.719448069.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000020.00000002.719448069.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000020.00000002.719448069.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: cmd.exe PID: 7160 Parent PID: 6272

General

Start time:	20:30:58
Start date:	24/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 7028 Parent PID: 7160

General

Start time:	20:30:59
Start date:	24/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 6896 Parent PID: 7160

General

Start time:	20:30:59
Start date:	24/11/2020
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true

Commandline:	REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe'
Imagebase:	0x1120000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: 6988 Parent PID: 6272

General

Start time:	20:31:01
Start date:	24/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6264 Parent PID: 6988

General

Start time:	20:31:01
Start date:	24/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: reg.exe PID: 6996 Parent PID: 6988

General

Start time:	20:31:02
Start date:	24/11/2020
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'fiffyt' /t REG_SZ /d 'C:\Users\user\AppData\Local\fifyt.exe'
Imagebase:	0x1120000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis