ID: 797493
Sample Name: 646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe
Cookbook: default.jbs
Time: 00:26:06
Date: 03/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

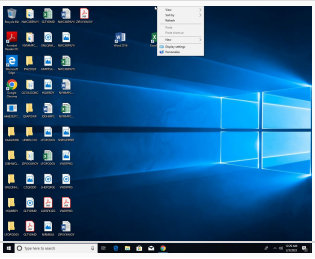
Windows Analysis Report

646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe

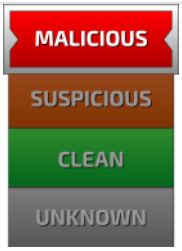
Overview

General Information

Sample Name:	646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe
Analysis ID:	797493
MD5:	e01a14abc90a…
SHA1:	1dbe3b0d1e76…
SHA256:	646b292f7a793..
Tags:	exe NanoCore RAT
Infos:	



Detection



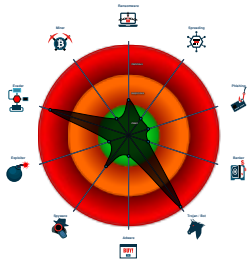
Nanocore

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Cassandra Crypter
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Antivirus / Scanner detection for sub…
- Sigma detected: Scheduled temp fil…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic

Classification



Process Tree

- **System is w10x64**
- 646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe (PID: 1228 cmdline: C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe MD5: E01A14ABC90ACECB1FE2ABA8D3ADB71F)
  - schtasks.exe (PID: 1308 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\hbVCUlv" /XML "C:\Users\user\AppData\Local\Temp\tmp9381.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1236 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe (PID: 5724 cmdline: C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe MD5: E01A14ABC90ACECB1FE2ABA8D3ADB71F)
    - schtasks.exe (PID: 5060 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmpBC6A.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 2024 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5128 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" / xml "C:\Users\user\AppData\Local\Temp\tmpBDD3.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 1504 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- 646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe (PID: 1900 cmdline: C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe 0 MD5: E01A14ABC90ACECB1FE2ABA8D3ADB71F)
  - schtasks.exe (PID: 5004 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\hbVCUlv" /XML "C:\Users\user\AppData\Local\Temp\tmpA582.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 640 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe (PID: 5244 cmdline: C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe MD5: E01A14ABC90ACECB1FE2ABA8D3ADB71F)
- hbVCUlv.exe (PID: 6028 cmdline: C:\Users\user\AppData\Roaming\hbVCUlv.exe MD5: E01A14ABC90ACECB1FE2ABA8D3ADB71F)
  - schtasks.exe (PID: 5172 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\hbVCUlv" /XML "C:\Users\user\AppData\Local\Temp\tmp8DA5.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5232 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - hbVCUlv.exe (PID: 1228 cmdline: C:\Users\user\AppData\Roaming\hbVCUlv.exe MD5: E01A14ABC90ACECB1FE2ABA8D3ADB71F)
- dhcpmon.exe (PID: 4788 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: E01A14ABC90ACECB1FE2ABA8D3ADB71F)
  - schtasks.exe (PID: 6044 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\hbVCUlv" /XML "C:\Users\user\AppData\Local\Temp\tmpA776.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6076 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 6088 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: E01A14ABC90ACECB1FE2ABA8D3ADB71F)
- dhcpmon.exe (PID: 4600 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: E01A14ABC90ACECB1FE2ABA8D3ADB71F)
  - schtasks.exe (PID: 4492 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\hbVCUlv" /XML "C:\Users\user\AppData\Local\Temp\tmpCABE.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 476 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 5072 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: E01A14ABC90ACECB1FE2ABA8D3ADB71F)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "10210cfb-2ea1-47f3-8c75-6fce83e4",
  "Group": "oob",
  "Domain1": "brianbriano.ddns.net",
  "Domain2": "127.0.0.1",
  "Port": 10001,
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000002.343692976.0000000002801000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000010.00000002.343692976.0000000002801000.00000004.00000800.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x238a7:$a: NanoCore • 0x23900:$a: NanoCore • 0x2393d:$a: NanoCore • 0x239b6:$a: NanoCore • 0x23909:$b: ClientPlugin • 0x23946:$b: ClientPlugin • 0x24244:$b: ClientPlugin • 0x24251:$b: ClientPlugin • 0x1b605:$e: KeepAlive • 0x23d91:$g: LogClientMessage • 0x23d11:$i: get_Connected • 0x158d9:$j: #=q • 0x15909:$j: #=q • 0x15945:$j: #=q • 0x1596d:$j: #=q • 0x1599d:$j: #=q • 0x159cd:$j: #=q • 0x159fd:$j: #=q • 0x15a2d:$j: #=q • 0x15a49:$j: #=q • 0x15a79:$j: #=q

Source	Rule	Description	Author	Strings
00000010.00000002.343692976.0000000002801000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x2393d:$a1: NanoCore.ClientPluginHost • 0x23900:$a2: NanoCore.ClientPlugin • 0x16e13:$b1: get_BuilderSettings • 0x23cd4:$b1: get_BuilderSettings • 0x2398b:$b4: IClientAppHost • 0x23d45:$b6: AddHostEntry • 0x16d82:$b7: LogClientException • 0x23db4:$b7: LogClientException • 0x23d29:$b8: PipeExists • 0x23978:$b9: IClientLoggingHost
00000000.00000002.307508938.0000000002B6A000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CassandraCrypter	Yara detected Cassandra Crypter	Joe Security	
00000008.00000002.318734843.0000000002ECA000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_CassandraCrypter	Yara detected Cassandra Crypter	Joe Security	
Click to see the 54 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe.5e90000.6.unpack	INDICATOR_EXE_Packed_Cassandra	Detects executables packed with Cassandra/CyaX	ditekSHen	• 0x74f:$pdb: \CyaX\obj\Debug\CyaX.pdb
12.2.646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
12.2.646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
12.2.646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
12.2.646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe.400000.0.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xfef5:$x1: NanoCore Client • 0xff05:$x1: NanoCore Client • 0x1014d:$x2: NanoCore.ClientPlugin • 0x1018d:$x3: NanoCore.ClientPluginHost • 0x10142:$i1: IClientApp • 0x10163:$i2: IClientData • 0x1016f:$i3: IClientNetwork • 0x1017e:$i4: IClientAppHost • 0x101a7:$i5: IClientDataHost • 0x101b7:$i6: IClientLoggingHost • 0x101ca:$i7: IClientNetworkHost • 0x101dd:$i8: IClientUIHost • 0x101eb:$i9: IClientNameObjectCollection • 0x10207:$i10: IClientReadOnlyNameObjectCollection • 0xff54:$s1: ClientPlugin • 0x10156:$s1: ClientPlugin • 0x1064a:$s2: EndPoint • 0x10653:$s3: IPAddress • 0x1065d:$s4: IPEndPoint • 0x12093:$s6: get_ClientSettings • 0x12637:$s7: get_Connected
Click to see the 92 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Persistence and Installation Behavior

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 184.105.237.195

Timestamp:	192.168.2.4184.105.237.19549710100012025019 02/03/23-00:28:31.654776
SID:	2025019
Source Port:	49710
Destination Port:	10001
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 184.105.237.195

Timestamp:	192.168.2.4184.105.237.19549710100012816766 02/03/23-00:28:33.834752
SID:	2816766
Source Port:	49710
Destination Port:	10001
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 184.105.237.195

Timestamp:	192.168.2.4184.105.237.19549696100012025019 02/03/23-00:27:05.348657
SID:	2025019
Source Port:	49696
Destination Port:	10001
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 184.105.237.195

Timestamp:	192.168.2.4184.105.237.19549714100012025019 02/03/23-00:28:55.473039
SID:	2025019
Source Port:	49714
Destination Port:	10001
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 184.105.237.195

Timestamp:	192.168.2.4184.105.237.19549703100012025019 02/03/23-00:27:48.578100
SID:	2025019
Source Port:	49703
Destination Port:	10001
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 184.105.237.195

Timestamp:	192.168.2.4184.105.237.19549697100012025019 02/03/23-00:27:11.697985
SID:	2025019
Source Port:	49697

Destination Port:	10001
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 184.105.237.195	−
Timestamp:	192.168.2.4184.105.237.1954969810001202501902/03/23-00:27:19.121500
SID:	2025019
Source Port:	49698
Destination Port:	10001
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 184.105.237.195	−
Timestamp:	192.168.2.4184.105.237.1954970910001202501902/03/23-00:28:24.651689
SID:	2025019
Source Port:	49709
Destination Port:	10001
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 184.105.237.195	−
Timestamp:	192.168.2.4184.105.237.1954970210001202501902/03/23-00:27:42.402353
SID:	2025019
Source Port:	49702
Destination Port:	10001
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 184.105.237.195	−
Timestamp:	192.168.2.4184.105.237.1954969810001281676602/03/23-00:27:21.094469
SID:	2816766
Source Port:	49698
Destination Port:	10001
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 184.105.237.195	−
Timestamp:	192.168.2.4184.105.237.1954971510001281676602/03/23-00:29:05.373729
SID:	2816766
Source Port:	49715
Destination Port:	10001
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 184.105.237.195	−
Timestamp:	192.168.2.4184.105.237.1954969710001281676602/03/23-00:27:13.460347
SID:	2816766
Source Port:	49697
Destination Port:	10001
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 184.105.237.195	−
Timestamp:	192.168.2.4184.105.237.1954970810001202501902/03/23-00:28:17.926799
SID:	2025019
Source Port:	49708
Destination Port:	10001
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 184.105.237.195	
Timestamp:	192.168.2.4184.105.237.195496961000128167660 02/03/23-00:27:07.112967
SID:	2816766
Source Port:	49696
Destination Port:	10001
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 184.105.237.195	
Timestamp:	192.168.2.4184.105.237.195497031000128167660 02/03/23-00:27:50.380926
SID:	2816766
Source Port:	49703
Destination Port:	10001
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 184.105.237.195	
Timestamp:	192.168.2.4184.105.237.195497141000128167660 02/03/23-00:28:58.124908
SID:	2816766
Source Port:	49714
Destination Port:	10001
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 184.105.237.195	
Timestamp:	192.168.2.4184.105.237.195497041000128167660 02/03/23-00:27:57.519906
SID:	2816766
Source Port:	49704
Destination Port:	10001
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 184.105.237.195	
Timestamp:	192.168.2.4184.105.237.195497081000128167660 02/03/23-00:28:19.942981
SID:	2816766
Source Port:	49708
Destination Port:	10001
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 184.105.237.195	
Timestamp:	192.168.2.4184.105.237.195497091000128167660 02/03/23-00:28:26.847077
SID:	2816766
Source Port:	49709
Destination Port:	10001
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.4 - Destination IP: 184.105.237.195	
Timestamp:	192.168.2.4184.105.237.195496971000128167180 02/03/23-00:27:12.093478
SID:	2816718
Source Port:	49697
Destination Port:	10001
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 184.105.237.195	
Timestamp:	192.168.2.4184.105.237.195497041000128025019 02/03/23-00:27:55.553197
SID:	2025019
Source Port:	49704

Destination Port:	10001
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 184.105.237.195	−
Timestamp:	192.168.2.4184.105.237.195497151000012025019 02/03/23-00:29:04.002318
SID:	2025019
Source Port:	49715
Destination Port:	10001
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 184.105.237.195	−
Timestamp:	192.168.2.4184.105.237.195497021000012816766 02/03/23-00:27:44.172937
SID:	2816766
Source Port:	49702
Destination Port:	10001
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.4 - Destination IP: 184.105.237.195	−
Timestamp:	192.168.2.4184.105.237.195497081000012816718 02/03/23-00:28:19.942981
SID:	2816718
Source Port:	49708
Destination Port:	10001
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Multi AV Scanner detection for submitted file
- Antivirus / Scanner detection for submitted sample
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropped file
- Yara detected Nanocore RAT
- Machine Learning detection for sample
- Machine Learning detection for dropped file

Networking

- Snort IDS alert for network traffic
- C2 URLs / IPs found in malware configuration
- Uses dynamic DNS services

E-Banking Fraud

- Yara detected Nanocore RAT

System Summary

- Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Yara detected Cassandra Crypter

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

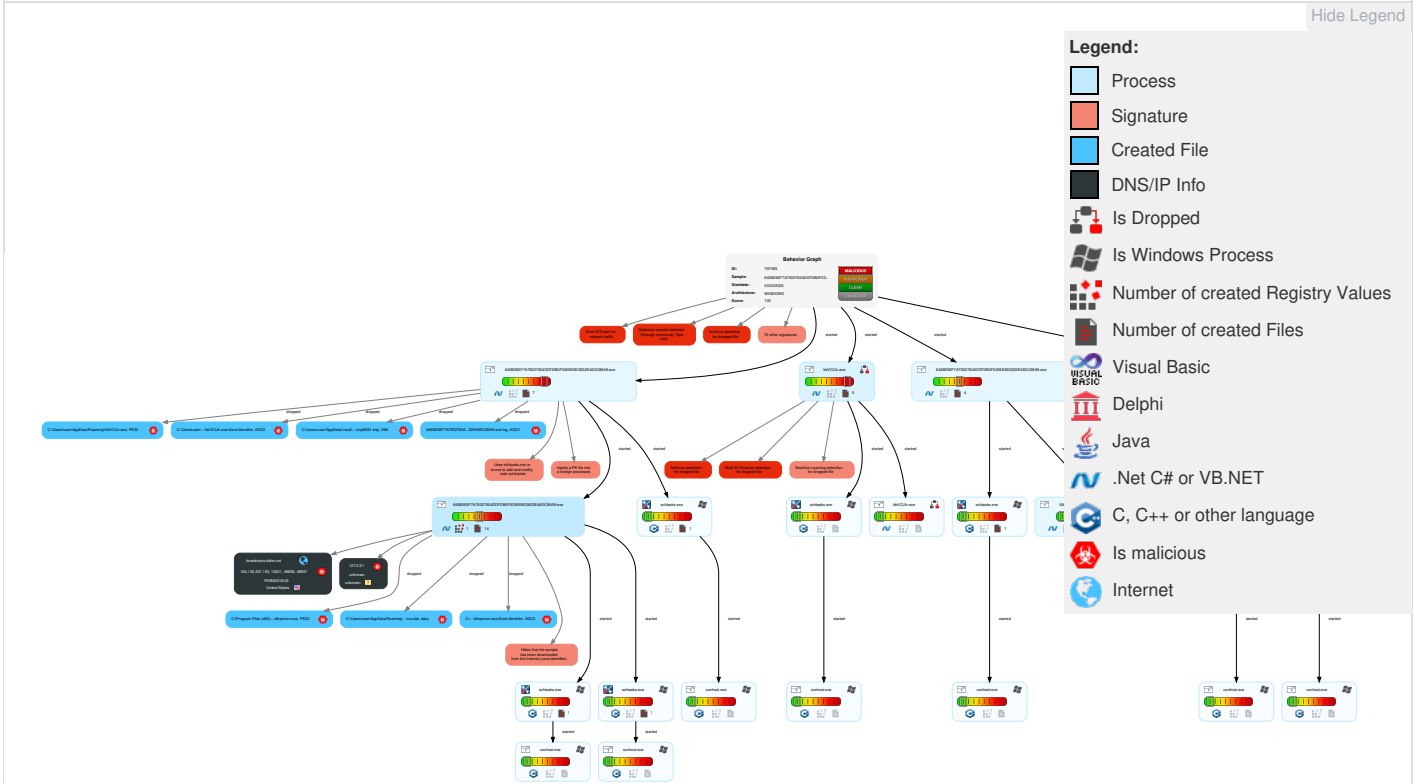
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	1 Scheduled Task/Job	1 Access Token Manipulation	1 Disable or Modify Tools	2 1 Input Capture	1 Account Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	Boot or Logon Initialization Scripts	1 1 2 Process Injection	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 File and Directory Discovery	Remote Desktop Protocol	2 1 Input Capture	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Scheduled Task/Job	2 Obfuscated Files or Information	Security Account Manager	3 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 3 Software Packing	NTDS	2 2 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Remote Access Software	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	2 Masquerading	LSA Secrets	2 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	1 Non-Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	2 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	2 1 Application Layer Protocol	Jamming or Denial of Service		Abuse Accessibility Features

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Access Token Manipulation	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 1 2 Process Injection	Proc Filesystem	1 System Owner/User Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe	82%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe	74%	Virustotal		Browse
646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe	100%	Avira	HEUR/AGEN.1202153	
646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\hbVCUlv.exe	100%	Avira	HEUR/AGEN.1202153	

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Avira	HEUR/AGEN.1202153	
C:\Users\user\AppData\Roaming\hbVCUlv.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	82%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	74%	Virustotal		Browse
C:\Users\user\AppData\Roaming\hbVCUlv.exe	82%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.2.646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.2.646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe.5e10000.6.unpack	100%	Avira	TR/NanoCore.fadte		Download File
0.0.646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe.500000.0.unpack	100%	Avira	HEUR/AGEN.1202153		Download File

Domains

Source	Detection	Scanner	Label	Link
brianbriano.ddns.net	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
127.0.0.1	0%	Avira URL Cloud	safe	
brianbriano.ddns.net	0%	Avira URL Cloud	safe	
127.0.0.1	1%	Virustotal		Browse
brianbriano.ddns.net	4%	Virustotal		Browse

Domains and IPs

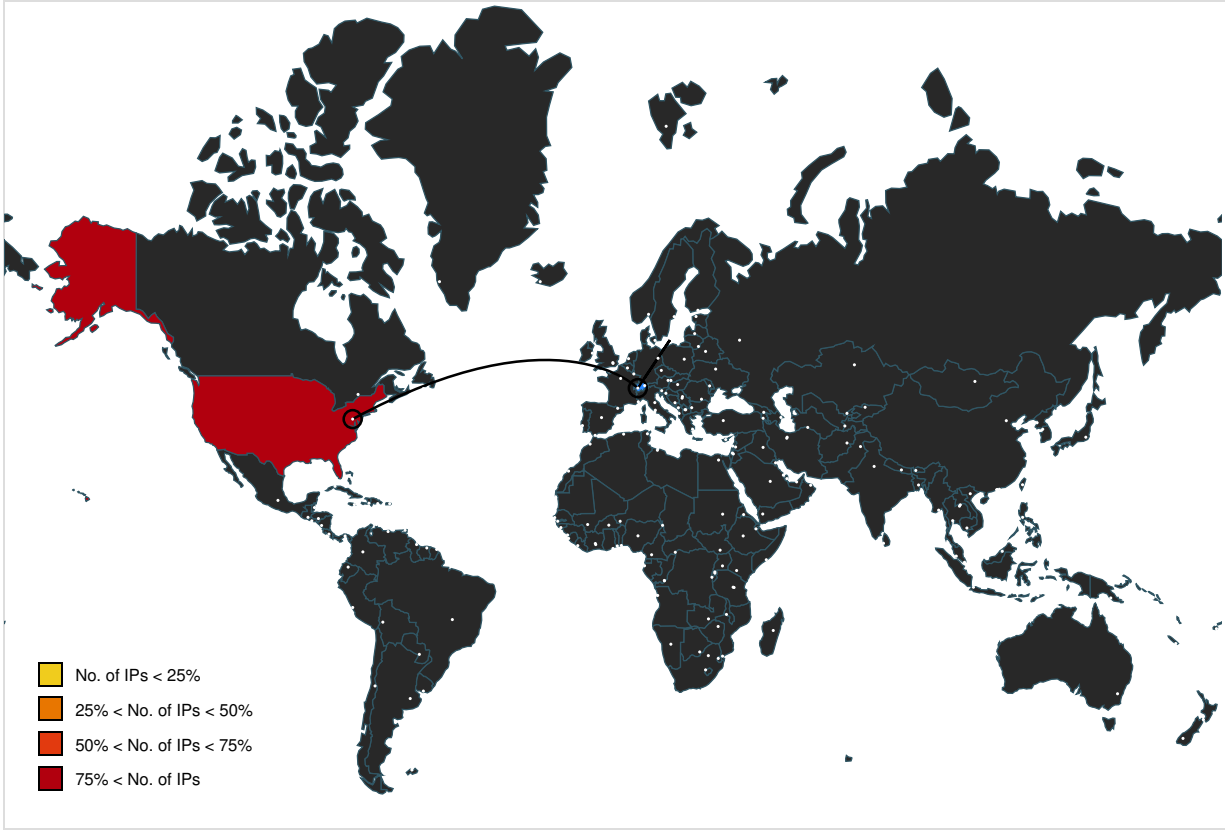
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
brianbriano.ddns.net	184.105.237.195	true	true	• 4%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
brianbriano.ddns.net	true	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown
127.0.0.1	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
184.105.237.195	brianbriano.ddns.net	United States		395100	RVBA2016US	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	797493
Start date and time:	2023-02-03 00:26:06 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
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
Sample file name:	646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@36/16@11/2

EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe
- TCP Packets have been reduced to 100
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- 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
00:27:00	API Interceptor	845x Sleep call for process: 646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe modified
00:27:02	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe" s>$(Arg0)
00:27:03	Task Scheduler	Run new task: hbVCUlv path: C:\Users\user\AppData\Roaming\hbVCUlv.exe
00:27:05	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
00:27:05	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
00:27:07	API Interceptor	2x Sleep call for process: dhcpmon.exe modified
00:27:08	API Interceptor	1x Sleep call for process: hbVCUlv.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	397312
Entropy (8bit):	7.9410139482036834
Encrypted:	false
SSDEEP:	6144:f3g6+/BLtz4FIRvUHGNid8tWDBtfctKnKlNSyPOYFq4vCwg8D3ICNiz4ypR42:Y6+/BLtvkGCuYqKifOYnFg8TluizB
MD5:	E01A14ABC90ACECB1FE2ABA8D3ADB71F
SHA1:	1DBE3B0D1E76EEF6E1CD8C28E59A67B067EB6988
SHA-256:	646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9860986016FDBA3D64627
SHA-512:	F3A5374DEA5C38CE1DBDFDFC2607CBC6347C12A8A12D256636B4A0B4A83A4ACA03E1DE2EC4506F28DE962FD0CC2C916E7FDB86994566AC1865FBF4C603120 77D
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 82% • Antivirus: Virustotal, Detection: 74%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....]..... .....n#... .....@.. ....@.....#..W....@.....`..... ..... ..H.....text...t.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....P#.....H.....h...._.....XY...j.....0..k.....r...p}.....r...p}.....r%..p}.....r7..p}.....rl..p}.....r[..p}.....rm..p}.....r...p}.. ...r...p}.....(.....*..0..t.....(....&.....".".!.!....8.....#.#,...+..%..$.$,...+... ....%.%,. ....+.. .....&.&,...X.+.....'.',...+..%..(.(,...+.....).),....+..%...*.*,....+.....+.+,....+. .%...,.,....+.... ....-.-,. .....+... .....,....X..+...

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

Process:	C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe.log

Process:	C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	655
Entropy (8bit):	5.273171405160065
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0Ug+9Yz9t0U2ukyrFk70U2WUXBQav:MLF20NaL329hJ5g5z2p22rW29XBT
MD5:	03EBEB80A2ECD58DB99E84A9304352A3
SHA1:	D2C4D662AC774D29740474423B81D61E47B90995
SHA-256:	C8D208E1F41C7F58BC657B74A16F5BA0F496BFE31093D70252A0870CCFB93734
SHA-512:	ECDD31A6DA669E91EAD7E9685EDFE2F128C12280CFBE38135190A0D63291C827002996BFC70A9BD57790E466C4355242B985FA3E087FEA6F6AFAB6AFA6EE7A EE
Malicious:	**true**
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_3 2\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Wind ows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Management\4de9980 4c29261edb63c93616550f034\System.Management.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log

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

File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	771
Entropy (8bit):	5.270465016990876
Encrypted:	false
SSDEEP:	24:MLF20NaL329hJ5g5z2p22rW29XBp2+g2+:MwLLG9h3gl2Y2rx9XBY+g2+
MD5:	3018D5969A55A0F1ADC29EAE9ED164BF
SHA1:	284FC77F7EF0ABDECE86BA01496D879BE71DE65C
SHA-256:	8F12BEC94AF00C112F34873CCA7FC7D85F9851B7ACFD2A20B079868C93078F89
SHA-512:	9E073D4B4F4CC713485235DB89DA06461AE051CACADFF2A4B916A7CBFC0A59CC542988D5530D9FFB28B7E9D98712EB653DB6A613EC1E47C53262AAEEA2C665FE
Malicious:	false
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Management\4de99804c29261edb63c93616550f034\System.Management.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\527c933194f3a99a816d83c619a3e1d3\System.Xml.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\hbVCUlv.exe.log

Process:	C:\Users\user\AppData\Roaming\hbVCUlv.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	655
Entropy (8bit):	5.273171405160065
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0Ug+9Yz9t0U2ukyrFk70U2WUXBQav:MLF20NaL329hJ5g5z2p22rW29XBT
MD5:	03EBEB80A2ECD58DB99E84A9304352A3
SHA1:	D2C4D662AC774D29740474423B81D61E47B90995
SHA-256:	C8D208E1F41C7F58BC657B74A16F5BA0F496BFE31093D70252A0870CCFB93734
SHA-512:	ECDD31A6DA669E91EAD7E9685EDFE2F128C12280CFBE38135190A0D63291C827002996BFC70A9BD57790E466C4355242B985FA3E087FEA6F6AFAB6AFA6EE7AEE
Malicious:	false
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Management\4de99804c29261edb63c93616550f034\System.Management.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp8DA5.tmp

Process:	C:\Users\user\AppData\Roaming\hbVCUlv.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1640
Entropy (8bit):	5.179780179213497
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGlOtn:cbhK79lNQR/rydbz9l3YODOLNdq3wo
MD5:	6022357E4EA537D40786932DE20A1358
SHA1:	19205EFC9A07988C786049A83E856E98DD4159B2
SHA-256:	B9769BCD55F8D8B8E1D476E2DC7DE95B0A60A049C011459AEEB6E20DCA577487
SHA-512:	9E962CDF6CFDB26F50C30746D376CCDA8969A0E3959B2164189EC979275587DE66BBF4AF0B7086FF4C957223E10250740C9C73D56299313546C6DD688F7CEB5
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmp9381.tmp

Process:	C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1640

Entropy (8bit):	5.179780179213497
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGlOtn:cbhK79lNQR/rydbz9l3YODOLNdq3wo
MD5:	6022357E4EA537D40786932DE20A1358
SHA1:	19205EFC9A07988C786049A83E856E98DD4159B2
SHA-256:	B9769BCD55F8D8B8E1D476E2DC7DE95B0A60A049C011459AEEB6E20DCA577487
SHA-512:	9E962CDF6CFDB26F50C30746D376CCDA8969A0E3959B2164189EC979275587DE66BBF4AF0B7086FF4C957223E10250740C9C73D56299313546C6DD688F7CEB5
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>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmpA582.tmp

Process:	C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1640
Entropy (8bit):	5.179780179213497
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGlOtn:cbhK79lNQR/rydbz9l3YODOLNdq3wo
MD5:	6022357E4EA537D40786932DE20A1358
SHA1:	19205EFC9A07988C786049A83E856E98DD4159B2
SHA-256:	B9769BCD55F8D8B8E1D476E2DC7DE95B0A60A049C011459AEEB6E20DCA577487
SHA-512:	9E962CDF6CFDB26F50C30746D376CCDA8969A0E3959B2164189EC979275587DE66BBF4AF0B7086FF4C957223E10250740C9C73D56299313546C6DD688F7CEB5
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmpA776.tmp

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1640
Entropy (8bit):	5.179780179213497
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGlOtn:cbhK79lNQR/rydbz9l3YODOLNdq3wo
MD5:	6022357E4EA537D40786932DE20A1358
SHA1:	19205EFC9A07988C786049A83E856E98DD4159B2
SHA-256:	B9769BCD55F8D8B8E1D476E2DC7DE95B0A60A049C011459AEEB6E20DCA577487
SHA-512:	9E962CDF6CFDB26F50C30746D376CCDA8969A0E3959B2164189EC979275587DE66BBF4AF0B7086FF4C957223E10250740C9C73D56299313546C6DD688F7CEB5
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmpBC6A.tmp

Process:	C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1335
Entropy (8bit):	5.21334491153168
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0YJvxtn:cbk4oL600QydbQxlYODOLedq3dj

MD5:	5EFC0529B9E30CA47CD07FE32A116CE5
SHA1:	04BAE26926213546EFA3101E607830956E250965
SHA-256:	2ACF199A1C4E458BEDF6637C9AF392F46FE3E4A2C6B49DBA7225C423B66565F1
SHA-512:	221F4EE95FDC69793D6B215E2F26F18DB5798AFC07F21BFF5D5B5EA012D7D6BC9817E168385CA47FE325C1F05C8A586DA88A02A4780B3A3C2A0D3709349BFB5C
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>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpBDD3.tmp

Process:	C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755734
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>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

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

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1640
Entropy (8bit):	5.179780179213497
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGlOtn:cbhK79lNQR/rydbz9l3YODOLNdq3wo
MD5:	6022357E4EA537D40786932DE20A1358
SHA1:	19205EFC9A07988C786049A83E856E98DD4159B2
SHA-256:	B9769BCD55F8D8B8E1D476E2DC7DE95B0A60A049C011459AEEB6E20DCA577487
SHA-512:	9E962CDF6CFDB26F50C30746D376CCDA8969A0E3959B2164189EC979275587DE66BBF4AF0B7086FF4C957223E10250740C9C73D56299313546C6DD688F7CEB5
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

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

Process:	C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:b:b
MD5:	53BCE1FE311D8C9EF524EAC0EA6B9223

SHA1:	74A39B5401D2AE234872ED096F95037DF103DD6D
SHA-256:	6C748A4D30923BADBF05144B5696150E66B08D5AE4BECAF530767DD6CC323C57
SHA-512:	77BC6062E9B4E1594A55785B1FFD50313196BE81E547F01949EA0286994469744829492 5FB6CD8931353798DC7BE14A7BB67A42C1D0180BD1B1E716EE0BBE9E9
Malicious:	**true**
Preview:	iN..t..H

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

Process:	C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	72
Entropy (8bit):	4.62466971024535
Encrypted:	false
SSDEEP:	3:oNt+WfWTRTnbbQ7hhlVjQVJBkA:oNwvR3Q70Vl
MD5:	569EF1FFEF994FEA2DF27631236433B6
SHA1:	19550BC4046FB45E2A1894679B2C6DEA62C3BB58
SHA-256:	897465B24325FFF96F887BA14800AB111803B42FC267258D38145E9AC61B9B20
SHA-512:	7795B2B84233F9FACDA20365E4D7E9B0D0EED5EEA1522E6F977EFA52DE9551557D0AC2EA66E7AC12476B9D88084DEBC35DD2075CBC20392E76B85605D89FB2 D0
Malicious:	false
Preview:	C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe

C:\Users\user\AppData\Roaming\hbVCUlv.exe

Process:	C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	397312
Entropy (8bit):	7.9410139482036834
Encrypted:	false
SSDEEP:	6144:f3g6+/BLtz4FIRvUHGNid8tWDBtfctKnKlNSyPOYFq4vCwg8D3ICNiz4ypR42:Y6+/BLtvkGCuYqKifOYnFg8TIuizB
MD5:	E01A14ABC90ACECB1FE2ABA8D3ADB71F
SHA1:	1DBE3B0D1E76EEF6E1CD8C28E59A67B067EB6988
SHA-256:	646B292F7A79327604DDFDB0F535EE8D3832E46DC86A980986016FDBA3D64627
SHA-512:	F3A5374DEA5C38CE1DBDFDFC2607CBC6347C12A8A12D256636B4A0B4A83A4ACA03E1DE2EC4506F28DE962FD0CC2C916E7FDB86994566AC1865FBF4C603120 77D
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 82%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....]..... .....n#... .....@.. ....@.....#..W....@..... `..... ..... ..H.....text...t.... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....P#.....H.....h...._.....XY...j.....0..k.....r...p}.....r...p}.....r%..p}.....r7..p}.....rl..p}.....r[..p}.....rm..p}.....r...p}.. ...r...p}.....(.....*..0..t.....(....&.....".".!.!....8.....#.#,...+..%..$.$,...+... ....%.%,. ....+.. .....&.&,...X.+.....'.',...+..%..(.(,...+.....).),....+..%...*.*,....+.....+.+,....+. .%...,.,....+.... ....-.-,. .....+... .....,....X..+...

C:\Users\user\AppData\Roaming\hbVCUlv.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.9410139482036834
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe
File size:	397312
MD5:	e01a14abc90acecb1fe2aba8d3adb71f
SHA1:	1dbe3b0d1e76eef6e1cd8c28e59a67b067eb6988
SHA256:	646b292f7a79327604ddfdb0f535ee8d3832e46dc86a980986016fdba3d64627
SHA512:	f3a5374dea5c38ce1dbdfdfc2607cbc6347c12a8a12d256636b4a0b4a83a4aca03e1de2ec4506f28de962fd0cc2c916e7fdb86994566ac1865fbf4c60312077d
SSDEEP:	6144:f3g6+/BLtz4FIRvUHGNid8tWDBtfctKnKlNSyPOYFq4vCwg8D3ICNiz4ypR42:Y6+/BLtvkGCuYqKifOYnFg8TIuizB
TLSH:	1F8412017718E795D38CA7F8AA74626C4371B6A81932F32F4C6B30E7D563BE2472185B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....].....n#... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x46236e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x5DC20BC4 [Tue Nov 5 23:54:44 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x62314	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x64000	0x800	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x66000	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	0x60374	0x60400	False	0.9524173092532467	data	7.954638266049198	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x64000	0x800	0x800	False	0.32958984375	data	3.450513412054433	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x66000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x64090	0x37c	data		
RT_MANIFEST	0x6441c	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

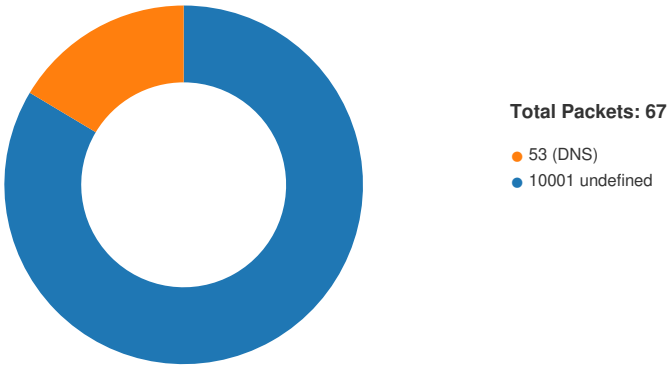
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4184.105.237.19549710100012025019 02/03/23-00:28:31.654776	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49710	10001	192.168.2.4	184.105.237.195
192.168.2.4184.105.237.19549710100012816766 02/03/23-00:28:33.834752	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49710	10001	192.168.2.4	184.105.237.195
192.168.2.4184.105.237.19549696100012025019 02/03/23-00:27:05.348657	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49696	10001	192.168.2.4	184.105.237.195
192.168.2.4184.105.237.19549714100012025019 02/03/23-00:28:55.473039	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49714	10001	192.168.2.4	184.105.237.195
192.168.2.4184.105.237.19549703100012025019 02/03/23-00:27:48.578100	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49703	10001	192.168.2.4	184.105.237.195
192.168.2.4184.105.237.19549697100012025019 02/03/23-00:27:11.697985	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49697	10001	192.168.2.4	184.105.237.195
192.168.2.4184.105.237.19549698100012025019 02/03/23-00:27:19.121500	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49698	10001	192.168.2.4	184.105.237.195
192.168.2.4184.105.237.19549709100012025019 02/03/23-00:28:24.651689	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49709	10001	192.168.2.4	184.105.237.195
192.168.2.4184.105.237.19549702100012025019 02/03/23-00:27:42.402353	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49702	10001	192.168.2.4	184.105.237.195
192.168.2.4184.105.237.19549698100012816766 02/03/23-00:27:21.094469	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49698	10001	192.168.2.4	184.105.237.195
192.168.2.4184.105.237.19549715100012816766 02/03/23-00:29:05.373729	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49715	10001	192.168.2.4	184.105.237.195
192.168.2.4184.105.237.19549697100012816766 02/03/23-00:27:13.460347	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49697	10001	192.168.2.4	184.105.237.195

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4184.105.237.19549708100012025019 02/03/23-00:28:17.926799	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49708	10001	192.168.2.4	184.105.237.195
192.168.2.4184.105.237.19549696100012816766 02/03/23-00:27:07.112967	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49696	10001	192.168.2.4	184.105.237.195
192.168.2.4184.105.237.19549703100012816766 02/03/23-00:27:50.380926	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49703	10001	192.168.2.4	184.105.237.195
192.168.2.4184.105.237.19549714100012816766 02/03/23-00:28:58.124908	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49714	10001	192.168.2.4	184.105.237.195
192.168.2.4184.105.237.19549704100012816766 02/03/23-00:27:57.519906	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49704	10001	192.168.2.4	184.105.237.195
192.168.2.4184.105.237.19549708100012816766 02/03/23-00:28:19.942981	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49708	10001	192.168.2.4	184.105.237.195
192.168.2.4184.105.237.19549709100012816766 02/03/23-00:28:26.847077	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49709	10001	192.168.2.4	184.105.237.195
192.168.2.4184.105.237.19549697100012816718 02/03/23-00:27:12.093478	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49697	10001	192.168.2.4	184.105.237.195
192.168.2.4184.105.237.19549704100012025019 02/03/23-00:27:55.553197	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49704	10001	192.168.2.4	184.105.237.195
192.168.2.4184.105.237.19549715100012025019 02/03/23-00:29:04.002318	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49715	10001	192.168.2.4	184.105.237.195
192.168.2.4184.105.237.19549702100012816766 02/03/23-00:27:44.172937	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49702	10001	192.168.2.4	184.105.237.195
192.168.2.4184.105.237.19549708100012816718 02/03/23-00:28:19.942981	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49708	10001	192.168.2.4	184.105.237.195

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 3, 2023 00:27:05.013998985 CET	49696	10001	192.168.2.4	184.105.237.195

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 3, 2023 00:27:05.208734035 CET	10001	49696	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:05.208848000 CET	49696	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:05.348656893 CET	49696	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:05.544926882 CET	10001	49696	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:05.545007944 CET	49696	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:05.741916895 CET	10001	49696	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:05.742041111 CET	49696	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:05.937634945 CET	10001	49696	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:05.938749075 CET	49696	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:06.132921934 CET	10001	49696	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:06.133028030 CET	49696	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:06.326924086 CET	10001	49696	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:06.327065945 CET	49696	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:06.522933006 CET	10001	49696	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:06.523025990 CET	49696	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:06.719455957 CET	10001	49696	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:06.719588995 CET	49696	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:06.916315079 CET	10001	49696	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:06.916836023 CET	49696	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:07.112868071 CET	10001	49696	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:07.112967014 CET	49696	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:07.275751114 CET	49696	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:07.307995081 CET	10001	49696	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:07.308048010 CET	49696	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:11.500554085 CET	49697	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:11.697468996 CET	10001	49697	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:11.697550058 CET	49697	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:11.697984934 CET	49697	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:11.894057035 CET	10001	49697	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:11.895531893 CET	49697	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:12.093377113 CET	10001	49697	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:12.093477964 CET	49697	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:12.288959026 CET	10001	49697	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:12.289061069 CET	49697	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:12.483809948 CET	10001	49697	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:12.484217882 CET	49697	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:12.678292990 CET	10001	49697	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:12.678432941 CET	49697	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:12.872711897 CET	10001	49697	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:12.875804901 CET	49697	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:13.070967913 CET	10001	49697	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:13.071103096 CET	49697	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:13.265883923 CET	10001	49697	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:13.265960932 CET	49697	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:13.460284948 CET	10001	49697	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:13.460346937 CET	49697	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:13.603579044 CET	49697	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:13.654912949 CET	10001	49697	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:13.655096054 CET	49697	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:18.835866928 CET	49698	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:19.029932022 CET	10001	49698	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:19.033951998 CET	49698	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:19.121500015 CET	49698	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:19.315598965 CET	10001	49698	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:19.317471027 CET	49698	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:19.511491060 CET	10001	49698	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:19.529211998 CET	49698	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:19.723428965 CET	10001	49698	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:19.725918055 CET	49698	10001	192.168.2.4	184.105.237.195

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 3, 2023 00:27:19.919888973 CET	10001	49698	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:19.921041012 CET	49698	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:20.116961002 CET	10001	49698	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:20.117067099 CET	49698	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:20.311744928 CET	10001	49698	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:20.312031031 CET	49698	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:20.508069992 CET	10001	49698	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:20.508608103 CET	49698	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:20.702568054 CET	10001	49698	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:20.706109047 CET	49698	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:20.900022030 CET	10001	49698	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:20.900327921 CET	49698	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:21.094309092 CET	10001	49698	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:21.094469070 CET	49698	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:21.107709885 CET	49698	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:21.288347006 CET	10001	49698	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:21.288449049 CET	49698	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:42.206159115 CET	49702	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:42.401283979 CET	10001	49702	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:42.401417971 CET	49702	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:42.402353048 CET	49702	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:42.597618103 CET	10001	49702	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:42.597693920 CET	49702	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:42.793983936 CET	10001	49702	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:42.794060946 CET	49702	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:42.989381075 CET	10001	49702	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:42.989494085 CET	49702	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:43.186486959 CET	10001	49702	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:43.187222958 CET	49702	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:43.382625103 CET	10001	49702	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:43.383800983 CET	49702	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:43.581367970 CET	10001	49702	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:43.582508087 CET	49702	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:43.777828932 CET	10001	49702	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:43.778004885 CET	49702	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:43.973201036 CET	10001	49702	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:43.976073980 CET	49702	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:44.172787905 CET	10001	49702	184.105.237.195	192.168.2.4
Feb 3, 2023 00:27:44.172936916 CET	49702	10001	192.168.2.4	184.105.237.195
Feb 3, 2023 00:27:44.264945030 CET	49702	10001	192.168.2.4	184.105.237.195

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 3, 2023 00:27:04.961555958 CET	50911	53	192.168.2.4	8.8.8.8
Feb 3, 2023 00:27:04.984492064 CET	53	50911	8.8.8.8	192.168.2.4
Feb 3, 2023 00:27:11.474503994 CET	59683	53	192.168.2.4	8.8.8.8
Feb 3, 2023 00:27:11.495126963 CET	53	59683	8.8.8.8	192.168.2.4
Feb 3, 2023 00:27:18.814075947 CET	64167	53	192.168.2.4	8.8.8.8
Feb 3, 2023 00:27:18.833225965 CET	53	64167	8.8.8.8	192.168.2.4
Feb 3, 2023 00:27:42.185161114 CET	58565	53	192.168.2.4	8.8.8.8
Feb 3, 2023 00:27:42.204382896 CET	53	58565	8.8.8.8	192.168.2.4
Feb 3, 2023 00:27:48.357934952 CET	52239	53	192.168.2.4	8.8.8.8
Feb 3, 2023 00:27:48.379580975 CET	53	52239	8.8.8.8	192.168.2.4
Feb 3, 2023 00:27:55.328177929 CET	56807	53	192.168.2.4	8.8.8.8
Feb 3, 2023 00:27:55.347703934 CET	53	56807	8.8.8.8	192.168.2.4
Feb 3, 2023 00:28:17.707776070 CET	61007	53	192.168.2.4	8.8.8.8
Feb 3, 2023 00:28:17.729979992 CET	53	61007	8.8.8.8	192.168.2.4
Feb 3, 2023 00:28:24.433948994 CET	60686	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 3, 2023 00:28:24.454770088 CET	53	60686	8.8.8.8	192.168.2.4
Feb 3, 2023 00:28:31.434386969 CET	61124	53	192.168.2.4	8.8.8.8
Feb 3, 2023 00:28:31.456299067 CET	53	61124	8.8.8.8	192.168.2.4
Feb 3, 2023 00:28:55.255594969 CET	59444	53	192.168.2.4	8.8.8.8
Feb 3, 2023 00:28:55.274615049 CET	53	59444	8.8.8.8	192.168.2.4
Feb 3, 2023 00:29:03.759879112 CET	55570	53	192.168.2.4	8.8.8.8
Feb 3, 2023 00:29:03.778939962 CET	53	55570	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 3, 2023 00:27:04.961555958 CET	192.168.2.4	8.8.8.8	0x88a5	Standard query (0)	brianbrian o.ddns.net	A (IP address)	IN (0x0001)	false
Feb 3, 2023 00:27:11.474503994 CET	192.168.2.4	8.8.8.8	0x6c59	Standard query (0)	brianbrian o.ddns.net	A (IP address)	IN (0x0001)	false
Feb 3, 2023 00:27:18.814075947 CET	192.168.2.4	8.8.8.8	0x18c9	Standard query (0)	brianbrian o.ddns.net	A (IP address)	IN (0x0001)	false
Feb 3, 2023 00:27:42.185161114 CET	192.168.2.4	8.8.8.8	0xcd7e	Standard query (0)	brianbrian o.ddns.net	A (IP address)	IN (0x0001)	false
Feb 3, 2023 00:27:48.357934952 CET	192.168.2.4	8.8.8.8	0x388d	Standard query (0)	brianbrian o.ddns.net	A (IP address)	IN (0x0001)	false
Feb 3, 2023 00:27:55.328177929 CET	192.168.2.4	8.8.8.8	0xe574	Standard query (0)	brianbrian o.ddns.net	A (IP address)	IN (0x0001)	false
Feb 3, 2023 00:28:17.707776070 CET	192.168.2.4	8.8.8.8	0x7f0b	Standard query (0)	brianbrian o.ddns.net	A (IP address)	IN (0x0001)	false
Feb 3, 2023 00:28:24.433948994 CET	192.168.2.4	8.8.8.8	0x426e	Standard query (0)	brianbrian o.ddns.net	A (IP address)	IN (0x0001)	false
Feb 3, 2023 00:28:31.434386969 CET	192.168.2.4	8.8.8.8	0x95d5	Standard query (0)	brianbrian o.ddns.net	A (IP address)	IN (0x0001)	false
Feb 3, 2023 00:28:55.255594969 CET	192.168.2.4	8.8.8.8	0xfc9f	Standard query (0)	brianbrian o.ddns.net	A (IP address)	IN (0x0001)	false
Feb 3, 2023 00:29:03.759879112 CET	192.168.2.4	8.8.8.8	0x7edd	Standard query (0)	brianbrian o.ddns.net	A (IP address)	IN (0x0001)	false

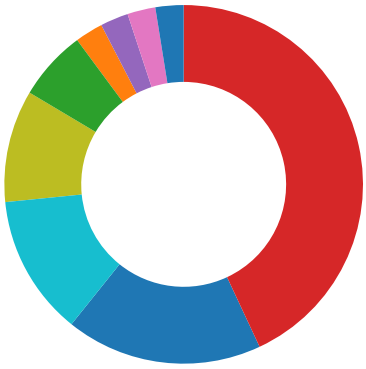
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 3, 2023 00:27:04.984492064 CET	8.8.8.8	192.168.2.4	0x88a5	No error (0)	brianbrian o.ddns.net		184.105.237.195	A (IP address)	IN (0x0001)	false
Feb 3, 2023 00:27:11.495126963 CET	8.8.8.8	192.168.2.4	0x6c59	No error (0)	brianbrian o.ddns.net		184.105.237.195	A (IP address)	IN (0x0001)	false
Feb 3, 2023 00:27:18.833225965 CET	8.8.8.8	192.168.2.4	0x18c9	No error (0)	brianbrian o.ddns.net		184.105.237.195	A (IP address)	IN (0x0001)	false
Feb 3, 2023 00:27:42.204382896 CET	8.8.8.8	192.168.2.4	0xcd7e	No error (0)	brianbrian o.ddns.net		184.105.237.195	A (IP address)	IN (0x0001)	false
Feb 3, 2023 00:27:48.379580975 CET	8.8.8.8	192.168.2.4	0x388d	No error (0)	brianbrian o.ddns.net		184.105.237.195	A (IP address)	IN (0x0001)	false
Feb 3, 2023 00:27:55.347703934 CET	8.8.8.8	192.168.2.4	0xe574	No error (0)	brianbrian o.ddns.net		184.105.237.195	A (IP address)	IN (0x0001)	false
Feb 3, 2023 00:28:17.729979992 CET	8.8.8.8	192.168.2.4	0x7f0b	No error (0)	brianbrian o.ddns.net		184.105.237.195	A (IP address)	IN (0x0001)	false
Feb 3, 2023 00:28:24.454770088 CET	8.8.8.8	192.168.2.4	0x426e	No error (0)	brianbrian o.ddns.net		184.105.237.195	A (IP address)	IN (0x0001)	false
Feb 3, 2023 00:28:31.456299067 CET	8.8.8.8	192.168.2.4	0x95d5	No error (0)	brianbrian o.ddns.net		184.105.237.195	A (IP address)	IN (0x0001)	false
Feb 3, 2023 00:28:55.274615049 CET	8.8.8.8	192.168.2.4	0xfc9f	No error (0)	brianbrian o.ddns.net		184.105.237.195	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 3, 2023 00:29:03.778939962 CET	8.8.8.8	192.168.2.4	0x7edd	No error (0)	brianbrian o.ddns.net		184.105.237.195	A (IP address)	IN (0x0001)	false

Statistics

Behavior



- 646B292F7A79327604DDFDB0F53..
- schtasks.exe
- conhost.exe
- 646B292F7A79327604DDFDB0F53..
- schtasks.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- 646B292F7A79327604DDFDB0F53..
- hbVCUlv.exe
- schtasks.exe
- conhost.exe
- 646B292F7A79327604DDFDB0F53..
- dhcpmon.exe
- schtasks.exe
- conhost.exe
- dhcpmon.exe
- schtasks.exe
- conhost.exe
- hbVCUlv.exe
- dhcpmon.exe
- schtasks.exe
- conhost.exe
- dhcpmon.exe

Click to jump to process

System Behavior

Analysis Process: 646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe PID: 1228, Parent PID: 3528

General

Target ID:	0
Start time:	00:26:58
Start date:	03/02/2023
Path:	C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe
Imagebase:	0x500000
File size:	397312 bytes
MD5 hash:	E01A14ABC90ACECB1FE2ABA8D3ADB71F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_CassandraCrypter, Description: Yara detected Cassandra Crypter, Source: 00000000.00000002.307508938.0000000002B6A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: SUSP_NET_NAME_ConfuserEx, Description: Detects ConfuserEx packed file, Source: 00000000.00000002.314033178.00000000051D0000.00000004.08000000.00040000.00000000.sdmp, Author: Arnim Rupp • Rule: INDICATOR_EXE_Packed_Cassandra, Description: Detects executables packed with Cassandra/CyaX, Source: 00000000.00000002.314033178.00000000051D0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.311567488.0000000003B31000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.311567488.0000000003B31000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.311567488.0000000003B31000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.311567488.0000000003B31000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CassandraCrypter, Description: Yara detected Cassandra Crypter, Source: 00000000.00000002.314578400.0000000005E90000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_EXE_Packed_Cassandra, Description: Detects executables packed with Cassandra/CyaX, Source: 00000000.00000002.314578400.0000000005E90000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CBD60AC	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	6CBD60AC	unknown
C:\Users\user\AppData\Roaming\hbVCUlv.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	E4BD78	CopyFileW
C:\Users\user\AppData\Roaming\hbVCUlv.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	E4BD78	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp9381.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4BC0824	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBC34A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp9381.tmp	success or wait	1	4BC0DF6	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\hbVCUlv.exe	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd 0b fd 5d 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 08 00 00 04 06 00 00 0a 00 00 00 00 00 00 6e 23 06 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 06 00 00 02 00 00 00 00 00 00 02 00 40 fd 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.$PEL]n# @ @	success or wait	4	E4BD78	CopyFileW
C:\Users\user\AppData\Roaming\hbVCUlv.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	E4BD78	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp9381.tmp	0	1640	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 6e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft .com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user </Author> </RegistrationIn	success or wait	1	4BC0AB3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe.log	0	655	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",03,"	success or wait	1	6CEAA33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6CC05544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6CC05544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6CC08738	ReadFile

Analysis Process: schtasks.exe PID: **1308**, Parent PID: **1228**

General

Target ID:	1
Start time:	00:27:00
Start date:	03/02/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\hbVCUlv" /XML "C:\Users\user\AppData\Local\Temp\tmp9381.tmp
Imagebase:	0xcc0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp9381.tmp	unknown	2	success or wait	1	CCAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp9381.tmp	unknown	1641	success or wait	1	CCABD9	ReadFile

Analysis Process: conhost.exe PID: 1236, Parent PID: 1308

General

Target ID:	2
Start time:	00:27:00
Start date:	03/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
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: 646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe PID: 5724, Parent PID: 1228

General

Target ID:	3
Start time:	00:27:01
Start date:	03/02/2023
Path:	C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe
Imagebase:	0x9c0000
File size:	397312 bytes
MD5 hash:	E01A14ABC90ACECB1FE2ABA8D3ADB71F
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: 00000003.00000002.578951789.0000000005B70000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.578951789.0000000005B70000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.578951789.0000000005B70000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.578951789.0000000005B70000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.573594094.0000000003201000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.579080815.0000000005E10000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.579080815.0000000005E10000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.579080815.0000000005E10000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.579080815.0000000005E10000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.579080815.0000000005E10000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CBD60AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CBD60AC	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	5440D15	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	5440E0F	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	5440D15	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	5441094	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	5441094	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpBC6A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5441290	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	5440E0F	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpBDD3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5441290	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	5440D15	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	5440D15	CreateDirectoryW
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	6CBD60AC	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	6CBD60AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpBC6A.tmp	success or wait	1	130BF0E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpBDD3.tmp	success or wait	1	130BF0E	DeleteFileW
C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe:Zone.Identifier	success or wait	1	5441625	DeleteFileA

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	0	8	69 4e 08 fd 74 05 fd 48	iNtH	success or wait	1	5440FC7	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd 0b fd 5d 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 08 00 00 04 06 00 00 0a 00 00 00 00 00 00 6e 23 06 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 06 00 00 02 00 00 00 00 00 00 02 00 40 fd 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.$PEL]n# @ @	success or wait	4	5441094	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	5441094	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpBC6A.tmp	0	1335	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" x mlns="http://schemas.microsoft .com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	5440FC7	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	0	72	43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 44 65 73 6b 74 6f 70 5c 36 34 36 42 32 39 32 46 37 41 37 39 33 32 37 36 30 34 44 44 46 44 42 30 46 35 33 35 45 45 38 44 33 38 33 32 45 34 36 44 43 38 36 41 39 2e 65 78 65	C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe	success or wait	1	5440FC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpBDD3.tmp	0	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	5440FC7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6CC05544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6CC05544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6CC08738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6CCABF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6CCABF06	unknown
C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe	unknown	4096	success or wait	1	6CCABF06	unknown
C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe	unknown	512	success or wait	1	6CCABF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6CC05544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	6CC05544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5440FC7	ReadFile

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	5441186	RegSetValueExW

Analysis Process: schtasks.exe PID: **5060**, Parent PID: **5724**

General

Target ID:	4
Start time:	00:27:02
Start date:	03/02/2023
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\tmpBC6A.tmp
Imagebase:	0xcc0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpBC6A.tmp	unknown	2	success or wait	1	CCAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpBC6A.tmp	unknown	1336	success or wait	1	CCABD9	ReadFile

Analysis Process: conhost.exe PID: **2024**, Parent PID: **5060**

General

Target ID:	5
Start time:	00:27:02
Start date:	03/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
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: **5128**, Parent PID: **5724**

General

Target ID:	6
Start time:	00:27:02
Start date:	03/02/2023
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\tmpBDD3.tmp
Imagebase:	0xcc0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpBDD3.tmp	unknown	2	success or wait	1	CCAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpBDD3.tmp	unknown	1311	success or wait	1	CCABD9	ReadFile

Analysis Process: conhost.exe PID: **1504**, Parent PID: **5128**

General

Target ID:	7
Start time:	00:27:02
Start date:	03/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
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: 646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe PID: **1900**, Parent PID: **1088**

General

Target ID:	8
Start time:	00:27:02
Start date:	03/02/2023
Path:	C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe 0
Imagebase:	0x820000
File size:	397312 bytes
MD5 hash:	E01A14ABC90ACECB1FE2ABA8D3ADB71F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CassandraCrypter, Description: Yara detected Cassandra Crypter, Source: 00000008.00000002.318734843.0000000002ECA000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6CBD60AC	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	6CBD60AC	unknown
C:\Users\user\AppData\Local\Temp\tmpA582.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4F203A8	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA582.tmp	success or wait	1	4F2097A	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA582.tmp	0	1640	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationIn	success or wait	1	4F20637	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6CC05544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6CC05544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6CC08738	ReadFile

Analysis Process: hbVCUlv.exe PID: **6028**, Parent PID: **1088**

General

Target ID:	9
Start time:	00:27:03
Start date:	03/02/2023
Path:	C:\Users\user\AppData\Roaming\hbVCUlv.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\hbVCUlv.exe
Imagebase:	0xf30000
File size:	397312 bytes
MD5 hash:	E01A14ABC90ACECB1FE2ABA8D3ADB71F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CassandraCrypter, Description: Yara detected Cassandra Crypter, Source: 00000009.00000002.331266992.000000000371A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 82%, ReversingLabs

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	6CBD60AC	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	6CBD60AC	unknown
C:\Users\user\AppData\Local\Temp\tmp8DA5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	59503A8	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\hbVCUlv.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6CBC34A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8DA5.tmp	success or wait	1	595097A	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8DA5.tmp	0	1640	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>computer\user</Author> </RegistrationIn	success or wait	1	5950637	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\hbVCUlv.exe.log	0	655	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",03,"	success or wait	1	6CEAA33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6CC05544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6CC05544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6CC08738	ReadFile

Analysis Process: schtasks.exe PID: **5004**, Parent PID: **1900**

General

Target ID:	10
Start time:	00:27:04
Start date:	03/02/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\hbVCUlv" /XML "C:\Users\user\AppData\Local\Temp\tmpA582.tmp
Imagebase:	0xcc0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA582.tmp	unknown	2	success or wait	1	CCAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA582.tmp	unknown	1641	success or wait	1	CCABD9	ReadFile

Analysis Process: conhost.exe PID: **640**, Parent PID: **5004**

General

Target ID:	11
Start time:	00:27:04
Start date:	03/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: 646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe PID: **5244**, Parent PID: **1900**

General

Target ID:	12
Start time:	00:27:05
Start date:	03/02/2023
Path:	C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\646B292F7A79327604DDFDB0F535EE8D3832E46DC86A9.exe
Imagebase:	0xf70000
File size:	397312 bytes
MD5 hash:	E01A14ABC90ACECB1FE2ABA8D3ADB71F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.342518655.0000000003621000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.342518655.0000000003621000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000C.00000002.342518655.0000000003621000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.342969185.0000000004621000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.342969185.0000000004621000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000C.00000002.342969185.0000000004621000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.332550764.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.332550764.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.332550764.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000C.00000002.332550764.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown

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	6CBD60AC	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	6CBD60AC	unknown

File Read						
File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6CC05544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6CC05544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6CC08738	ReadFile

Analysis Process: dhcpmon.exe PID: **4788**, Parent PID: **1088**

General	
Target ID:	13
Start time:	00:27:05
Start date:	03/02/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0xb10000
File size:	397312 bytes
MD5 hash:	E01A14ABC90ACECB1FE2ABA8D3ADB71F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CassandraCrypter, Description: Yara detected Cassandra Crypter, Source: 0000000D.00000002.324082470.000000000315A000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 82%, ReversingLabs • Detection: 74%, Virustotal, Browse

Analysis Process: schtasks.exe PID: **6044**, Parent PID: **4788**

General	
Target ID:	14
Start time:	00:27:07
Start date:	03/02/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\hbVCUlv" /XML "C:\Users\user\AppData\Local\Temp\tmpA776.tmp
Imagebase:	0xcc0000
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: **6076**, Parent PID: **6044**

General	
Target ID:	15
Start time:	00:27:07
Start date:	03/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes

MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: **6088**, Parent PID: **4788**

General

Target ID:	16
Start time:	00:27:08
Start date:	03/02/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x110000
File size:	397312 bytes
MD5 hash:	E01A14ABC90ACECB1FE2ABA8D3ADB71F
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: 00000010.00000002.343692976.0000000002801000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.343692976.0000000002801000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000010.00000002.343692976.0000000002801000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Analysis Process: schtasks.exe PID: **5172**, Parent PID: **6028**

General

Target ID:	17
Start time:	00:27:10
Start date:	03/02/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\hbVCUlv" /XML "C:\Users\user\AppData\Local\Temp\tmp8DA5.tmp
Imagebase:	0xcc0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **5232**, Parent PID: **5172**

General

Target ID:	18
Start time:	00:27:10
Start date:	03/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language

Analysis Process: hbVCUlv.exe PID: **1228**, Parent PID: **6028**

General	
Target ID:	19
Start time:	00:27:11
Start date:	03/02/2023
Path:	C:\Users\user\AppData\Roaming\hbVCUlv.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\hbVCUlv.exe
Imagebase:	0xa20000
File size:	397312 bytes
MD5 hash:	E01A14ABC90ACECB1FE2ABA8D3ADB71F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.355128673.0000000003151000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.355128673.0000000003151000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000013.00000002.355128673.0000000003151000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Analysis Process: dhcpmon.exe PID: **4600**, Parent PID: **3528**

General	
Target ID:	20
Start time:	00:27:13
Start date:	03/02/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0x200000
File size:	397312 bytes
MD5 hash:	E01A14ABC90ACECB1FE2ABA8D3ADB71F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: schtasks.exe PID: **4492**, Parent PID: **4600**

General	
Target ID:	21
Start time:	00:27:19
Start date:	03/02/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\hbVCUlv" /XML "C:\Users\user\AppData\Local\Temp\tmpCABE.tmp
Imagebase:	0xcc0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **476**, Parent PID: **4492**

General	
Target ID:	22
Start time:	00:27:19
Start date:	03/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: **5072**, Parent PID: **4600**

General	
Target ID:	23
Start time:	00:27:19
Start date:	03/02/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x770000
File size:	397312 bytes
MD5 hash:	E01A14ABC90ACECB1FE2ABA8D3ADB71F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Disassembly

No disassembly