ID: 324206
Sample Name:
SecuriteInfo.com.Trojan.DownLoader36.7233.23906.21829
Cookbook: default.jbs
Time: 17:48:18
Date: 28/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

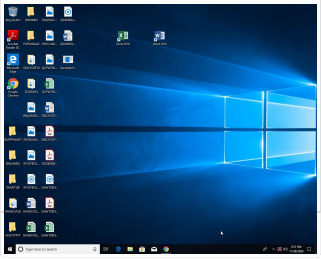
Analysis Report SecuriteInfo.com.Trojan.DownLoader36…

Overview

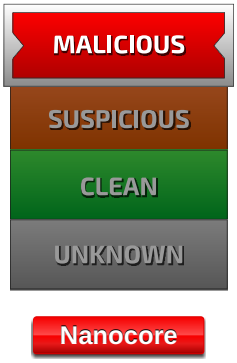
General Information

Sample Name:	SecuriteInfo.com.Trojan.DownLoader36.7233.23906.21829 (renamed file extension from 21829 to exe)
Analysis ID:	324206
MD5:	ee4555ac614048..
SHA1:	c7559fe7c094d46..
SHA256:	3a2278374596d3..

Most interesting Screenshot:



Detection

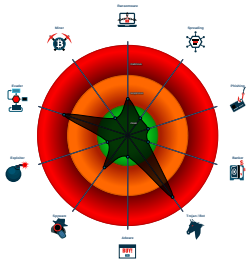


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Detected Nanocore Rat
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e…
- Yara detected Nanocore RAT
- Connects to many ports of the same…
- Hides that the sample has been dow…

Classification



Startup

- **System is w10x64**
- SecuriteInfo.com.Trojan.DownLoader36.7233.23906.exe (PID: 2440 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.DownLoader36.7233.23906.exe' MD5: EE4555AC614048E36AAE067B6A032951)
  - conhost.exe (PID: 5092 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 5316 cmdline: cmd /c schtasks /Create /TN images /XML 'C:\Users\user\AppData\Local\Temp\27c398b5630447af830b2dd2bc343446.xml' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - schtasks.exe (PID: 4928 cmdline: schtasks /Create /TN images /XML 'C:\Users\user\AppData\Local\Temp\27c398b5630447af830b2dd2bc343446.xml' MD5: 15FF7D8324231381BAD48A052F85DF04)
  - MSBuild.exe (PID: 2152 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe MD5: 88BBB7610152B48C2B3879473B17857E)
    - schtasks.exe (PID: 5920 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp182E.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5948 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 2168 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp1B1D.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 4120 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- MSBuild.exe (PID: 5292 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe 0 MD5: 88BBB7610152B48C2B3879473B17857E)
  - conhost.exe (PID: 1968 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 5972 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 88BBB7610152B48C2B3879473B17857E)
  - conhost.exe (PID: 2792 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 5588 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 88BBB7610152B48C2B3879473B17857E)
  - conhost.exe (PID: 5860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
00000000.00000002.220940423.000000000032A000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x15bdd:$x1: NanoCore.ClientPluginHost • 0x15c1a:$x2: IClientNetworkHost • 0x1974d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.220940423.000000000032A000.00000004.00020000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.220940423.000000000032A000.00000004.00020000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x15945:$a: NanoCore • 0x15955:$a: NanoCore • 0x15b89:$a: NanoCore • 0x15b9d:$a: NanoCore • 0x15bdd:$a: NanoCore • 0x159a4:$b: ClientPlugin • 0x15ba6:$b: ClientPlugin • 0x15be6:$b: ClientPlugin • 0x15acb:$c: ProjectData • 0x164d2:$d: DESCrypto • 0x1de9e:$e: KeepAlive • 0x1be8c:$g: LogClientMessage • 0x18087:$i: get_Connected • 0x16808:$j: #=q • 0x16838:$j: #=q • 0x16854:$j: #=q • 0x16884:$j: #=q • 0x168a0:$j: #=q • 0x168bc:$j: #=q • 0x168ec:$j: #=q • 0x16908:$j: #=q
00000003.00000003.228783921.000000000448 1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x1312:$a: NanoCore • 0x1337:$a: NanoCore • 0x1390:$a: NanoCore • 0x1152d:$a: NanoCore • 0x11553:$a: NanoCore • 0x115af:$a: NanoCore • 0x1e404:$a: NanoCore • 0x1e45d:$a: NanoCore • 0x1e490:$a: NanoCore • 0x1e6bc:$a: NanoCore • 0x1e738:$a: NanoCore • 0x1ed51:$a: NanoCore • 0x1ee9a:$a: NanoCore • 0x1f36e:$a: NanoCore • 0x1f655:$a: NanoCore • 0x1f66c:$a: NanoCore • 0x229f5:$a: NanoCore • 0x23daf:$a: NanoCore • 0x23df9:$a: NanoCore • 0x24a53:$a: NanoCore • 0x2a038:$a: NanoCore
Process Memory Space: SecuriteInfo.com.Trojan.DownLoader36.7233.23906.exe PID: 2440	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x10df52:$x1: NanoCore.ClientPluginHost • 0x10dfb3:$x2: IClientNetworkHost • 0x1133b8:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x12132a:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 3 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.SecuriteInfo.com.Trojan.DownLoader36.7233.23906.exe.320000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1e5dd:$x1: NanoCore.ClientPluginHost • 0x1e61a:$x2: IClientNetworkHost • 0x2214d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.SecuriteInfo.com.Trojan.DownLoader36.7233.23906.exe.320000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1e355:$x1: NanoCore Client.exe • 0x1e5dd:$x2: NanoCore.ClientPluginHost • 0x1fc16:$s1: PluginCommand • 0x1fc0a:$s2: FileCommand • 0x20abb:$s3: PipeExists • 0x26872:$s4: PipeCreated • 0x1e607:$s5: IClientLoggingHost
0.2.SecuriteInfo.com.Trojan.DownLoader36.7233.23906.exe.320000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
0.2.SecuriteInfo.com.Trojan.DownLoader36.7233.23906.exe.320000.0.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x1e345:$a: NanoCore • 0x1e355:$a: NanoCore • 0x1e589:$a: NanoCore • 0x1e59d:$a: NanoCore • 0x1e5dd:$a: NanoCore • 0x1e3a4:$b: ClientPlugin • 0x1e5a6:$b: ClientPlugin • 0x1e5e6:$b: ClientPlugin • 0x1e4cb:$c: ProjectData • 0x1eed2:$d: DESCrypto • 0x2689e:$e: KeepAlive • 0x2488c:$g: LogClientMessage • 0x20a87:$i: get_Connected • 0x1f208:$j: #=q • 0x1f238:$j: #=q • 0x1f254:$j: #=q • 0x1f284:$j: #=q • 0x1f2a0:$j: #=q • 0x1f2bc:$j: #=q • 0x1f2ec:$j: #=q • 0x1f308:$j: #=q

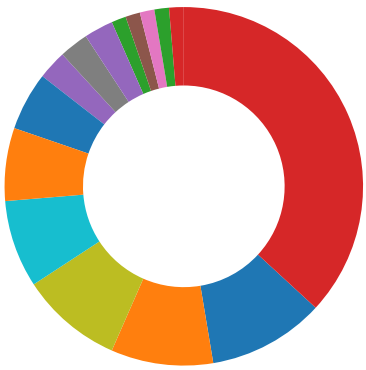
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

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)

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

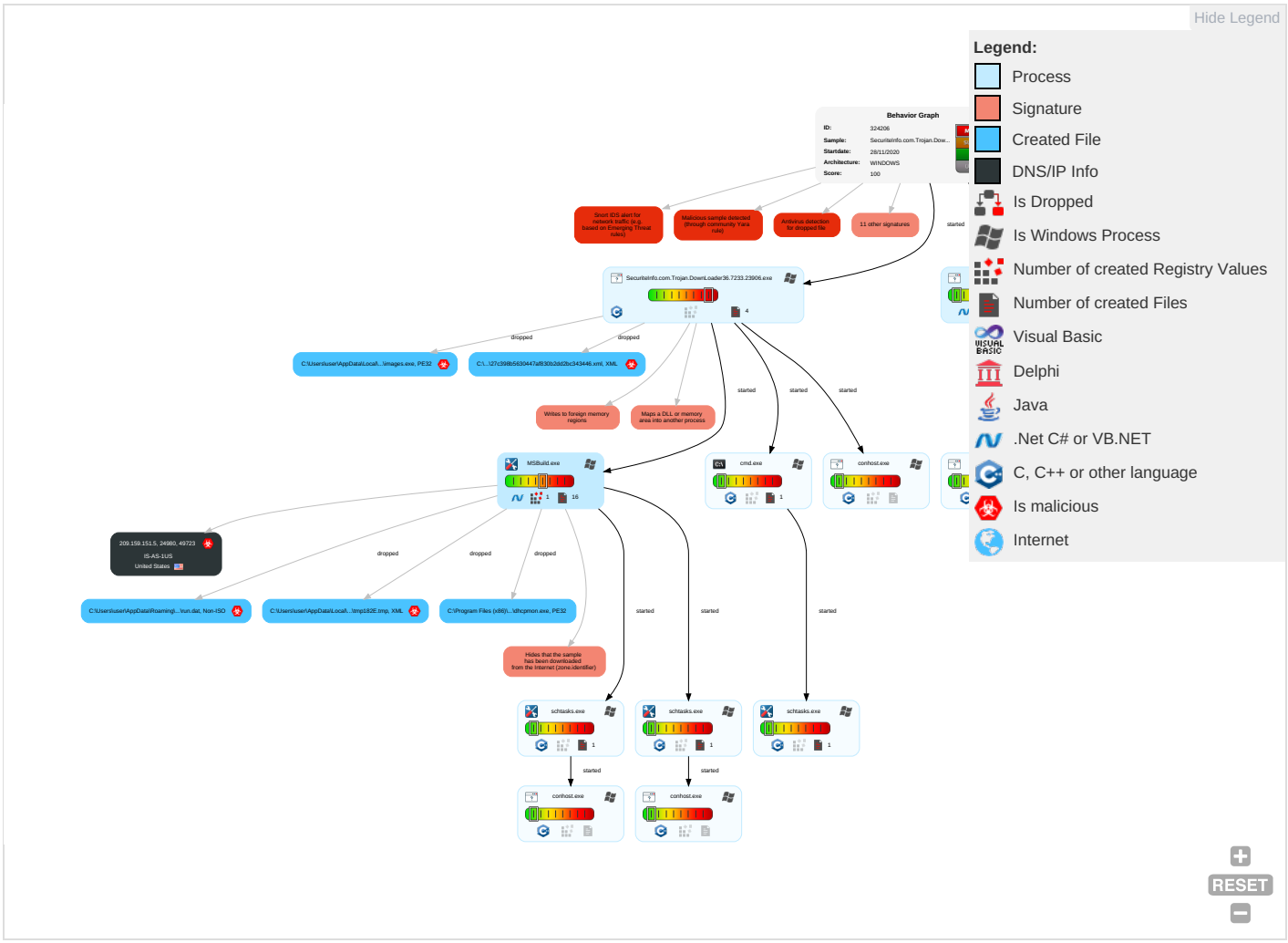
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 2 1 2	Masquerading 2	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eave Insec Netw Comr
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 2	LSASS Memory	Security Software Discovery 1 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Explo Redir Calls/
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Explo Track Locat
Local Accounts	Native API 1	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1	SIM (Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	Account Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamn Denia Servi

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1	DCSync	System Owner/User Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 2 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dowr Insec Proto

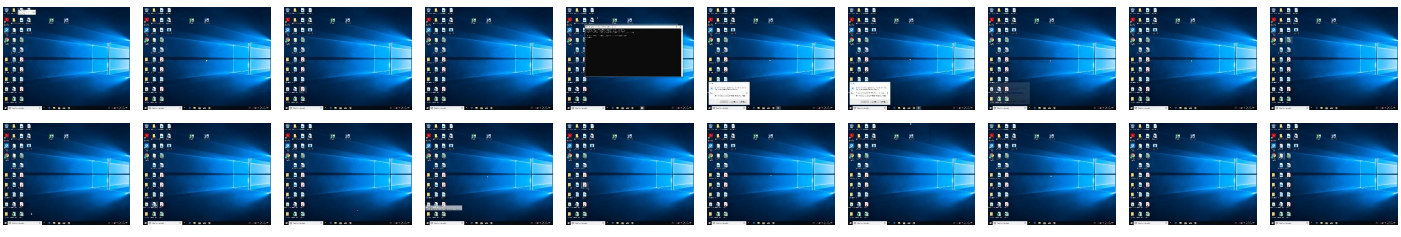
Behavior Graph



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
SecuriteInfo.com.Trojan.DownLoader36.7233.23906.exe	24%	Metadefender		Browse
SecuriteInfo.com.Trojan.DownLoader36.7233.23906.exe	75%	ReversingLabs	Win32.Exploit.CVE-2017-11882	
SecuriteInfo.com.Trojan.DownLoader36.7233.23906.exe	100%	Avira	TR/ATRAPS.Gen	
SecuriteInfo.com.Trojan.DownLoader36.7233.23906.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Temp\images.exe	100%	Avira	TR/ATRAPS.Gen	
C:\Users\user\AppData\Local\Temp\Temp\images.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\Temp\images.exe	79%	ReversingLabs	Win32.Backdoor.NanoCore	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.SecuriteInfo.com.Trojan.DownLoader36.7233.23906.exe.320000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
0.0.SecuriteInfo.com.Trojan.DownLoader36.7233.23906.exe.320000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File

Domains

No Antivirus matches

URLs

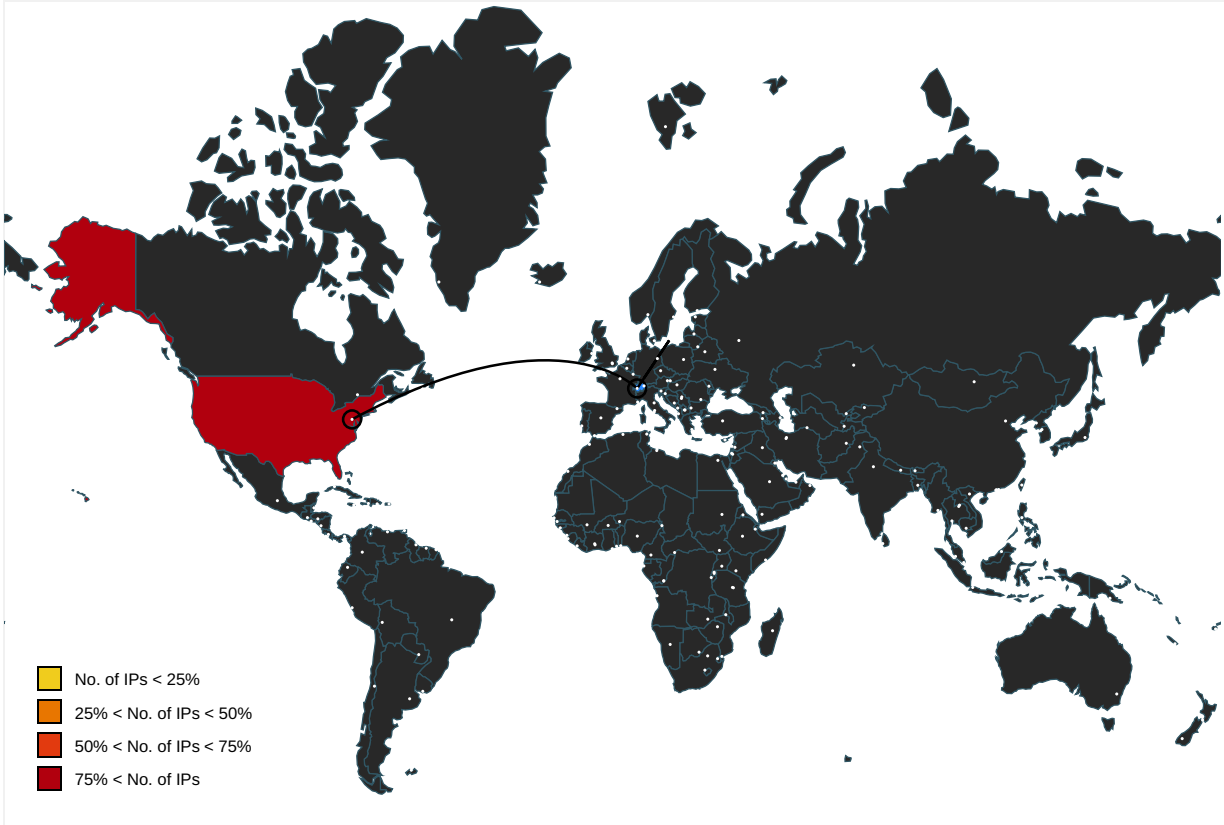
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
209.159.151.5	unknown	United States		19318	IS-AS-1US	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	324206
Start date:	28.11.2020

Start time:	17:48:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Trojan.DownLoader36.7233.23906.21829 (renamed file extension from 21829 to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	36
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@20/15@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 42.5% (good quality ratio 38.5%) • Quality average: 78.8% • Quality standard deviation: 31%
HCA Information:	• Successful, ratio: 88% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 52.147.198.201, 104.43.193.48, 51.104.139.180, 92.122.144.200, 20.54.26.129, 93.184.221.240, 92.122.213.194, 92.122.213.247, 51.11.168.160 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs.microsoft.com, wu.ec.azureedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net • Report size exceeded maximum capacity and may have missing behavior information. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/324206/sample/SecuriteInfo.com.Trojan.DownLoader36.7233.23906.exe

Simulations

Behavior and APIs

Time	Type	Description
17:49:16	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe" s>$(Arg0)
17:49:16	API Interceptor	956x Sleep call for process: MSBuild.exe modified
17:49:17	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
17:49:18	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
209.159.151.5	Package_details.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
IS-AS-1US	Package_details.exe	Get hash	malicious	Browse	• 209.159.151.5
	http://https://bakrisoil.com/wp-content/cd.php?e=gjeffries@hughesellard.com	Get hash	malicious	Browse	• 104.218.51.229
	baf6b9fcec491619b45c1dd7db56ad3d.exe	Get hash	malicious	Browse	• 66.45.248.130
	http://https://encrypt.poweradz.net/	Get hash	malicious	Browse	• 209.159.158.130
	http://encrypt.poweradz.net	Get hash	malicious	Browse	• 209.159.158.130
	eLaaw7SqMi.exe	Get hash	malicious	Browse	• 104.37.188.231
	p8LV1eVFyO.exe	Get hash	malicious	Browse	• 66.45.248.130
	Invoice_334654_168522_from_Inc.xlsm	Get hash	malicious	Browse	• 216.219.81.3
	Invoice_403372_917428_from_Inc.xlsm	Get hash	malicious	Browse	• 216.219.81.3
	IQtvZjIdhN.exe	Get hash	malicious	Browse	• 66.45.248.130
	Req-87086782-8575.htm	Get hash	malicious	Browse	• 66.45.228.57
	148wWoi8vI.exe	Get hash	malicious	Browse	• 66.45.248.130
	wZ6ARBLKPj.exe	Get hash	malicious	Browse	• 69.10.42.234
	Attachments_240369 475265.doc	Get hash	malicious	Browse	• 216.219.81.50
	AGENT APPOINTMENT.xlsm	Get hash	malicious	Browse	• 216.158.225.211
	isb777amx.exe	Get hash	malicious	Browse	• 66.23.227.135
	http://https://venushome-my.sharepoint.com/:b:/g/personal/nsh_venushomeappliances_com/EX5FneZcfnZMndmJcDSa_toBsLtKOV-PlkwfYKs_6Hf8sA?e=I7myHO	Get hash	malicious	Browse	• 206.72.203.52
	test9.exe	Get hash	malicious	Browse	• 66.45.228.160
	http://https://firebasestorage.googleapis.com/v0/b/iouyfgjkgh.appspot.com/o/WEBMAIL.html?alt=media&token=f21ff97e-0c97-456a-9a4b-10962301f5d2#salim.mamlouk@holding-kamph.com	Get hash	malicious	Browse	• 64.20.38.219
	http://https://firebasestorage.googleapis.com/v0/b/nnajnr.appspot.com/o/WEBMAIL.html?alt=media&token=de90d2b5-b8b1-4623-87f1-c5411b10395b#asegura@talgo.com	Get hash	malicious	Browse	• 64.20.38.219

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Purchase Order PDF pdf.exe	Get hash	malicious	Browse	
	Orden CW62125Q, pdf.exe	Get hash	malicious	Browse	
	7444478441.js	Get hash	malicious	Browse	
	7444478441.js	Get hash	malicious	Browse	
	7444478441.js	Get hash	malicious	Browse	
	5HuSdWXs4n.exe	Get hash	malicious	Browse	
	ABU.exe	Get hash	malicious	Browse	
	LI-TAK P0 TVOP CK-20-08-30 203008,pdf.exe	Get hash	malicious	Browse	
	ppp.exe	Get hash	malicious	Browse	
	787774778.js	Get hash	malicious	Browse	
	12477123690.js	Get hash	malicious	Browse	
	12477123690.js	Get hash	malicious	Browse	
	order pdf.exe	Get hash	malicious	Browse	
	Documents RF V23665.exe	Get hash	malicious	Browse	
	78547744787.js	Get hash	malicious	Browse	
	58669333.js	Get hash	malicious	Browse	
	58669333.js	Get hash	malicious	Browse	
	78547744787.js	Get hash	malicious	Browse	
	78547744787.js	Get hash	malicious	Browse	
	order.exe	Get hash	malicious	Browse	

Created / dropped Files

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

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	69632
Entropy (8bit):	5.20894581699571
Encrypted:	false
SSDEEP:	768:NElGiBcBuiyFjUwF0wdP9/rJMDnRFRJfStGpwV3e3qtAcy:ilGBu7jjP9/tMDn9Jt+VO3GO
MD5:	88BBB7610152B48C2B3879473B17857E
SHA1:	0F6CF8DD66AA58CE31DA4E8AC0631600EF055636
SHA-256:	2C7ACC16D19D076D67E9F1F37984935899B79536C9AC6EEC8850C44D20F87616
SHA-512:	5BACDF6C190A76C2C6A9A3519936E08E898AC8A2B1384D60429DF850BE778860435BF9E5EB316517D2345A5AAE201F369863F7A242134253978BCB5B2179CA58
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: Purchase Order PDF pdf.exe, Detection: malicious, Browse • Filename: Orden CW62125Q, pdf.exe, Detection: malicious, Browse • Filename: 7444478441.js, Detection: malicious, Browse • Filename: 7444478441.js, Detection: malicious, Browse • Filename: 7444478441.js, Detection: malicious, Browse • Filename: 5HuSdWXs4n.exe, Detection: malicious, Browse • Filename: ABU.exe, Detection: malicious, Browse • Filename: LI-TAK P0 TVOP CK-20-08-30 203008,pdf.exe, Detection: malicious, Browse • Filename: ppp.exe, Detection: malicious, Browse • Filename: 787774778.js, Detection: malicious, Browse • Filename: 12477123690.js, Detection: malicious, Browse • Filename: 12477123690.js, Detection: malicious, Browse • Filename: order pdf.exe, Detection: malicious, Browse • Filename: Documents RF V23665.exe, Detection: malicious, Browse • Filename: 78547744787.js, Detection: malicious, Browse • Filename: 58669333.js, Detection: malicious, Browse • Filename: 58669333.js, Detection: malicious, Browse • Filename: 78547744787.js, Detection: malicious, Browse • Filename: 78547744787.js, Detection: malicious, Browse • Filename: order.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....{Z.....@..... .....@.. .....@.....99.. ..@.....S.....`/..... ..... ..... ..H.....text..... ..... ..`.rsrc...`/.....0.....@..@.reloc..... . .....@..B..... .....

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

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\MSBuild.exe.log	
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	325
Entropy (8bit):	5.334380084018418
Encrypted:	false
SSDEEP:	6:Q3LadLCR22IAQykdL1tZbLsbFLIP12MUAvvro6ysGMFLIP12MUAvvrs:Q3LaJU20NaL1tZbgbe4MqJsGMe4M6
MD5:	65CE98936A67552310EFE2F0FF5BDF88
SHA1:	8133653A6B9A169C7496ADE315CED322CFC3613A
SHA-256:	682F7C55B1B6E189D17755F74959CD08762F91373203B3B982ACFFCADE2E871A
SHA-512:	2D00AC024267EC384720A400F6D0B4F7EDDF49FAF8AB3C9E6CBFBBAE90ECADACA9022B33E3E8EC92E4F57C7FC830299C8643235EB4AA7D8A6AFE9DD1775F57C3
Malicious:	false
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..2,"Microsoft.Build.Engine, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.Build.Framework, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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:	modified
Size (bytes):	441
Entropy (8bit):	5.388715099859351
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U2+gYhD5itZbgbe4MqJsGMe4M6:MLF20NaL32+g2OH4xvn4j
MD5:	88F0104DB9A3F9BC4F0FC3805F571B0D
SHA1:	CDD4F34385792F0CCE0A844F4ABB447C25AB4E73
SHA-256:	F6C11D3D078ED73F2640DA510E68DEEAA5F14F79CAE2E23A254B4E37C7D0230F
SHA-512:	04B977F63CAB8DE20EA7EFA9D4299C2E625D92FA6D54CA03EECD9F322E978326B353824F23BEC0E712083BDE0DBC5CC4EE90922137106B096050CA46A166DFE
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.Xml\527c933194f3a99a816d83c619a3e1d3\System.Xml.ni.dll",0..2,"Microsoft.Build.Engine, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.Build.Framework, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\27c398b5630447af830b2dd2bc343446.xml	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.DownLoader36.7233.23906.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1287
Entropy (8bit):	5.229307073850279
Encrypted:	false
SSDEEP:	24:2do4+S8Tcqd2r6gFwvbIrovlgU3ODOiIQRvh7hwZgvw43aVdyZEiTbn:c+XB2mbIrovl33ODOiLdKZgfoIt/
MD5:	17923A8153452A388A2DBDB5AA8118BE
SHA1:	B2BAE36FAF1E841516B3B122704C5D3CDE82D4DA
SHA-256:	66CC1714F3E1AC319A5FCB027577AFD9E4CEF6E9B03C945D73B7781D030A7D30
SHA-512:	6EA5A088FAA554EB447DFDC04CF004278F3578CE66E2E05CA5F0B50A545EC8E7FB9F365446F0867C1D400D8546F55A098A0C5437D24A9FD5FDB3031C9EEEEE59
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>2015-09-27T14:27:44.8929027</Date > .<Author>899552\user</Author>.</RegistrationInfo>.<Triggers>.<LogonTrigger>.<Enabled>true</Enabled>.<UserId>899552\user</UserId>.</LogonTrigger>.<RegistrationTrigger>.<Enabled>false</Enabled>.</RegistrationTrigger>.</Triggers>.<Principals>.<Principal id="Author">.<UserId>899552\user</UserId>.<LogonType>InteractiveToken</LogonType>.<RunLevel>LeastPrivilege</RunLevel>.</Principal>.</Principals>.<Settings>.<MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.<AllowHardTerminate>false</AllowHardTerminate>.<StartWhenAvailable>true</StartWhenAvailable>.<RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.<IdleSettings>.<StopOnIdleEnd>true</StopOnIdleEnd>.<RestartOnIdle>false</RestartOnIdle>.</IdleSettings>.<AllowStartOnDemand>true</AllowStartOnDemand>.<Enabled>true</Enabled>.<Hidden>fals

C:\Users\user\AppData\Local\Temp\Temp\images.exe	
Process:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.DownLoader36.7233.23906.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	271370
Entropy (8bit):	7.8736012263539585
Encrypted:	false
SSDEEP:	6144:Nqh+mUvToYfwuCiXri8Z/0jdKOs1dcxjc15ONu:NcUvTtwVqFZ2Dxjc3y
MD5:	0B77D13126DDB4FE1012DEF81EA16914
SHA1:	EFC2ABFBA1A703C8F069727CEFC48AA3DF6D0F95

C:\Users\user\AppData\Local\Temp\Temp\images.exe	
SHA-256:	415839939DCFD7D536A5F2BA9BBFFE95B33E6196B8168BAAB617813FF9A75FC9
SHA-512:	C5C76E17E5509E6D59885468ED9AEE3920BBEFBF3612DEA63B96649C1424B21E731391CA50A37345F13F0846926AFC069F7AC68535BE351D6555AB0E0A26C8BA
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 79%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Zo..4<..4<..4<.<..4<.<..4<.<..4<..O<..4<..5<..4<.<..4<.<..4<.<..4<Rich..4<.....PE..L....._.....f.....~.....@.....`.....@.....L.....@.....P.....P.. .@.....text...td.....f..... ..`.rdata..... ...j.....@..@.data.....@....rsrc.....@.....@..@.reloc.....P..... .....@..B.....

C:\Users\user\AppData\Local\Temp\tmp182E.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	5.136963558289723
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mnc2xtn:cbk4oL600QydbQxIYODOLedq3ZLj
MD5:	AE766004C0D8792953BAFFFE8F6A2E3B
SHA1:	14B12F27543A401E2FE0AF8052E116CAB0032426
SHA-256:	1ABDD9B6A6B84E4BA1AF1282DC84CE276C59BA253F4C4AF05FEA498A4FD99540
SHA-512:	E530DA4A5D4336FC37838D0E93B5EB3804B9C489C71F6954A47FC81A4C655BB72EC493E109CF96E6E3617D7623AC80697AD3BBD5FFC6281BAFC8B34DCA5E657
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <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\tmp1B1D.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	3:XrURGizD7cnRNGbgCFKRNX/pBK0jCV83ne+VdWPiKgmR7kkmefoeLBizbCuVkqYM:X4LDAnybgCFcps0OafmCYDlizZr/i/Oh
MD5:	9E7D0351E4DF94A9B0BADCEB6A9DB963
SHA1:	76C6A69B1C31CEA2014D1FD1E222A3DD1E433005
SHA-256:	AAFC7B40C5FE680A2BB549C3B90AABAAC63163F74FFFC0B00277C6BBFF88B757
SHA-512:	93CCF7E046A3C403ECF8BC4F1A8850BA0180FE18926C98B297C5214EB77BC212C8FBCC58412D0307840CF2715B63BE68BACDA95AA98E82835C5C53F17EF3851

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?...A.K...J.=8x!....+.2e'..E?.G.....[.&

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators, with overstriking
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:zrDP:fDP
MD5:	06FC58F9927778A61F43FE9613879AF5
SHA1:	5AB2C91B11AB018ADE2B61CE0AB5C87800FA0046
SHA-256:	19C6998695CA227D07148CEDF0DE018EDD4FB5F99B46AABAC9964B30483EA378
SHA-512:	DE1AA02C219A2583FCBEB941CBEB4230D3E4E3EAB985BE0AFDF06E3D5BCC45CE0A8921DD71852C07F8CA0F353BBD90A0C2100B58B5EA255CEE759F2836F4C41A
Malicious:	**true**
Preview:	.k.....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671BCB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	426832
Entropy (8bit):	**7.999527918131335**
Encrypted:	**true**
SSDEEP:	6144:zKfHbamD8WN+JQYrjM7Ei2CsFJjyh9zvgPonV5HqZcPVT4Eb+Z6no3QSzjeMsdF/:zKf137EiDsTjevgArYcPVLoTQS+0iv
MD5:	653DDDCB6C89F6EC51F3DDC0053C5914
SHA1:	4CF7E7D42495CE01C261E4C5C4B8BF6CD76CCEE5
SHA-256:	83B9CAE66800C768887FB270728F6806CBEBDEAD9946FA730F01723847F17FF9
SHA-512:	27A467F2364C21CD1C6C34EF1CA5FFB09B4C3180FC9C025E293374EB807E4382108617BB4B97F8EBBC27581CD6E5988BB5E21276B3CB829C1C0E49A6FC9463A
Malicious:	false
Preview:	..g&jo...IPg...GM....R>i...o...I.>.&.r{....8...}...E....v.!7.u3e.. .....db...}.....".t(.xC9.cp.B....7...'.....%.....w.^.._.....B.W%.<..i.0.{9.xS...5...)..w..$..C..?`F..u.5.T.X.w'Si..z.n{...Y!m...RA...xg....[7...z..9@.K.-...T..+.ACe....R....enO.....AoNMT.\^....}H&..4I...B.:..@..J...v..rI5..kP.....2j....B..B.~.T..>.c..emW;Rn<9..[.r.o....R[....@=...:....L.g<.....I..%4[.G^.~.I'.....v.p&.....+..S...9d/.{..H.`@.1.....f.\s...X.a.].<.h*...J4*...k.x....%3.....3.c..?%....>.!.}..)(.{...H...3..`].Q.[sN..JX(.%pH....+.....(...v.....H...3..8.a_..J..?4...y.N(..D.*h..g.jD..I...44Q?..N.....oX.A.....I...n?./.....$.!..;.^9"H.....*...OkF....v.m_.e.v..f...."..bq{.....O.-....%R+...-.P.i..t5....2Z# ...#...,L..{..j..heT -=Z.P;...g.m)<owJ].J..../.p..8.u8.&..#.m9...j%..g&....g.x.I,....u.[....>./W.....*X...b*Z...ex.0..x.}.....Tb...[..H_M._.^N.d&...g._."@4N.pDs].GbT.....&p.....Nw...%$=.....{..J.1....2....<E{..<!G..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.85263908467479
Encrypted:	false
SSDEEP:	3:oMty8WbSI1u:oMLWuI1u

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
MD5:	A35128E4E28B27328F70E4E8FF482443
SHA1:	B89066B2F8DB34299AABFD7ABEE402D5444DD079
SHA-256:	88AEA00733DC4B570A29D56A423CC5BF163E5ACE7AF349972EB0BBA8D9AD06E1
SHA-512:	F098E844B5373B34642B49B6E0F2E15CFDAA1A8B6CABC2196CEC0F3765289E5B1FD4AB588DD65F97C8E51FA9A81077621E9A06946859F296904C646906A70F33
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	306
Entropy (8bit):	4.969261552825097
Encrypted:	false
SSDEEP:	6:zx3M1tlAX8bSWR30qysGMQbSVRRZBXVRbJ0fFdCsq2UTiMdH8stCal+n:zK1XnV30ZsGMIG9BFRbQdCT2UftCM+
MD5:	F227448515085A647910907084E6728E
SHA1:	5FA1A8E28B084DA25A1BBC51A2D75810CEF57E2C
SHA-256:	662BA47D628FE8EBE95DD47B4482110A10B49AED09387BC0E028BB66E68E20BD
SHA-512:	6F6E5DFFF7B17C304FB19B0BA5466AF84EF98A5C2EFA573AF72CFD3ED6964E9FD7F8E4B79FCFFBEF87CE545418C69D4984F4DD60BBF457D0A3640950F8FC5AF0
Malicious:	false
Preview:	Microsoft (R) Build Engine Version 2.0.50727.8922..[Microsoft .NET Framework, Version 2.0.50727.8922]..Copyright (C) Microsoft Corporation 2005. All rights reserved.....MSBUILD : error MSB1003: Specify a project or solution file. The current working directory does not contain a project or solution file...

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	7.873728502504083
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.Trojan.DownLoader36.7233.23906.exe
File size:	271360
MD5:	ee4555ac614048e36aae067b6a032951
SHA1:	c7559fe7c094d4643ea3ab09c071fa0ac8ec18a4
SHA256:	3a2278374596d368ec773c10d54ec91f69445144248769abb155de58215d8c2c
SHA512:	620f7a6440caa0d16dc3e466b4078850d76e05c292d92225046d1ba1672a4ff550f601418344637554ab046ed1c96864c00702c75e6f5fb3b42454985ebcc03d
SSDEEP:	6144:Nqh+mUvToYfwuCiXri8Z/0jdKOs1dcxjc15ONu:NcUvTtwVqFZ2Dxjc3y
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Zo..4<...4<..4<...<..4<...<..4<...<..4<..O<..4<..5<..4<...<..4<...<..4<...<..4<Rich..4<.....PE..L....._...

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40147e

General

Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FBBD6F3 [Mon Nov 23 15:36:19 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	b0701deda97f8f775ded6a80cfec3216

Entrypoint Preview

Instruction
call 00007F9360F8323Eh
jmp 00007F9360F81A49h
mov edi, edi
push ebp
mov ebp, esp
sub esp, 00000328h
mov dword ptr [00442778h], eax
mov dword ptr [00442774h], ecx
mov dword ptr [00442770h], edx
mov dword ptr [0044276Ch], ebx
mov dword ptr [00442768h], esi
mov dword ptr [00442764h], edi
mov word ptr [00442790h], ss
mov word ptr [00442784h], cs
mov word ptr [00442760h], ds
mov word ptr [0044275Ch], es
mov word ptr [00442758h], fs
mov word ptr [00442754h], gs
pushfd
pop dword ptr [00442788h]
mov eax, dword ptr [ebp+00h]
mov dword ptr [0044277Ch], eax
mov eax, dword ptr [ebp+04h]
mov dword ptr [00442780h], eax
lea eax, dword ptr [ebp+08h]
mov dword ptr [0044278Ch], eax
mov eax, dword ptr [ebp-00000320h]
mov dword ptr [004426C8h], 00010001h
mov eax, dword ptr [00442780h]
mov dword ptr [0044267Ch], eax
mov dword ptr [00442670h], C0000409h
mov dword ptr [00442674h], 00000001h
mov eax, dword ptr [0040A004h]
mov dword ptr [ebp-00000328h], eax
mov eax, dword ptr [0040A008h]
mov dword ptr [ebp-00000324h], eax
call dword ptr [00000090h]

Rich Headers

Programming Language:	• [C] VS2008 build 21022 • [LNK] VS2008 build 21022 • [ASM] VS2008 build 21022 • [IMP] VS2005 build 50727 • [RES] VS2008 build 21022 • [C++] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x964c	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x44000	0x10	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x45000	0x70c	.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	0x9350	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x198	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6474	0x6600	False	0.612132352941	data	6.57687344022	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1fc0	0x2000	False	0.36865234375	data	5.50028935513	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x391fc	0x38800	False	0.983156457412	data	7.98418937184	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x44000	0x10	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x45000	0xeda	0x1000	False	0.39306640625	data	3.79564261107	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Imports

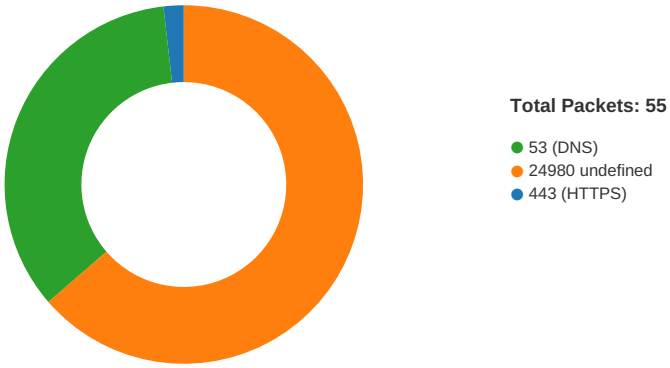
DLL	Import
KERNEL32.dll	GetConsoleWindow, GetProcAddress, LoadLibraryA, CloseHandle, GetStringTypeW, GetStringTypeA, LCMapStringW, MultiByteToWideChar, LCMapStringA, GetLocaleInfoA, HeapSize, RtlUnwind, HeapReAlloc, VirtualAlloc, HeapAlloc, IsValidCodePage, GetOEMCP, GetACP, GetCPInfo, InitializeCriticalSectionAndSpinCount, EnterCriticalSection, LeaveCriticalSection, GetSystemTimeAsFileTime, GetCurrentProcessId, GetTickCount, QueryPerformanceCounter, HeapFree, VirtualFree, HeapCreate, InterlockedDecrement, GetCurrentThreadId, GetCommandLineA, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, GetModuleHandleW, Sleep, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameA, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, WideCharToMultiByte, GetLastError, GetEnvironmentStringsW, SetHandleCount, GetFileType, GetStartupInfoA, DeleteCriticalSection, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, SetLastError
MSACM32.dll	acmMetrics, acmStreamReset, acmFilterChooseW, acmDriverOpen, acmDriverDetailsW
RPCRT4.dll	I_RpcNsBindingSetEntryNameW, NdrComplexArrayBufferSize, I_RpcIfInqTransferSyntaxes, RpcBindingServerFromClient, NDRSContextMarshall, RpcRevertToSelfEx
OLEAUT32.dll	VarCyFromUI4, VarDecFromDate, LPSAFEARRAY_UserUnmarshal, OleLoadPictureEx, VarR4FromBool
WINMM.dll	mmioDescend, mixerGetLineInfoA, mmioInstallIOProcA, midiInGetErrorTextA, mmTaskCreate, waveInGetErrorTextA, waveOutGetPosition, mmioAdvance
MPR.dll	WNetCancelConnection2A, WNetCancelConnectionA, WNetGetResourceParentA, WNetConnectionDialog1A, WNetGetResourceParentW, WNetDisconnectDialog1W, WNetUseConnectionA, WNetConnectionDialog, WNetGetUniversalNameA, WNetGetProviderNameA
USER32.dll	ShowWindow, CallWindowProcW

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/28/20-17:49:17.283033	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49723	24980	192.168.2.3	209.159.151.5

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 17:49:01.251102924 CET	443	49690	204.79.197.200	192.168.2.3
Nov 28, 2020 17:49:01.251230001 CET	49690	443	192.168.2.3	204.79.197.200
Nov 28, 2020 17:49:17.149760962 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:17.253833055 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.253953934 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:17.283032894 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:17.404994011 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.405109882 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:17.563344955 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.563474894 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:17.667670965 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.714481115 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:17.721899033 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:17.875973940 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.892357111 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.892399073 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.892425060 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.892448902 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.892474890 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.892473936 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:17.892501116 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.892508030 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:17.892524004 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.892549992 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.892570972 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:17.892574072 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.892599106 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.892611027 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:17.892659903 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:17.996613026 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.996649981 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.996675014 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.996706009 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.996733904 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.996757030 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.996783018 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.996788025 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:17.996809959 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.996814966 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:17.996834993 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.996848106 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:17.996860981 CET	24980	49723	209.159.151.5	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 17:49:17.996865988 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:17.996889114 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.996913910 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:17.996916056 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.996942043 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.996967077 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.996968985 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:17.996990919 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.997015953 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.997015953 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:17.997066021 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:17.997108936 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.997133970 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.997165918 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.997184992 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:17.997190952 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:17.997246027 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:18.101255894 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101305962 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101335049 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101358891 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101376057 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:18.101414919 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101430893 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:18.101443052 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101464987 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101485968 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101509094 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:18.101511002 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101536989 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101547956 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:18.101561069 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101583958 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101591110 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:18.101610899 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101635933 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101649046 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:18.101659060 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101684093 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101696014 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:18.101702929 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101728916 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101733923 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:18.101752996 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101775885 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101792097 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:18.101802111 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101830959 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101836920 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:18.101855993 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101882935 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101887941 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:18.101910114 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101938963 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101943970 CET	49723	24980	192.168.2.3	209.159.151.5
Nov 28, 2020 17:49:18.101964951 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101989985 CET	24980	49723	209.159.151.5	192.168.2.3
Nov 28, 2020 17:49:18.101989985 CET	49723	24980	192.168.2.3	209.159.151.5

UDP Packets

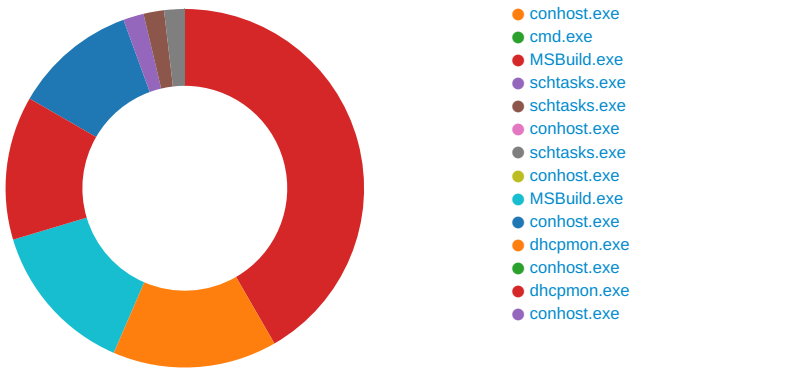
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 17:49:01.365673065 CET	60831	53	192.168.2.3	8.8.8.8
Nov 28, 2020 17:49:01.392847061 CET	53	60831	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2020 17:49:02.188767910 CET	60100	53	192.168.2.3	8.8.8.8
Nov 28, 2020 17:49:02.215718985 CET	53	60100	8.8.8.8	192.168.2.3
Nov 28, 2020 17:49:02.833033085 CET	53195	53	192.168.2.3	8.8.8.8
Nov 28, 2020 17:49:02.860352039 CET	53	53195	8.8.8.8	192.168.2.3
Nov 28, 2020 17:49:03.668102026 CET	50141	53	192.168.2.3	8.8.8.8
Nov 28, 2020 17:49:03.695293903 CET	53	50141	8.8.8.8	192.168.2.3
Nov 28, 2020 17:49:04.472825050 CET	53023	53	192.168.2.3	8.8.8.8
Nov 28, 2020 17:49:04.499989986 CET	53	53023	8.8.8.8	192.168.2.3
Nov 28, 2020 17:49:05.205583096 CET	49563	53	192.168.2.3	8.8.8.8
Nov 28, 2020 17:49:05.245820999 CET	53	49563	8.8.8.8	192.168.2.3
Nov 28, 2020 17:49:06.089550972 CET	51352	53	192.168.2.3	8.8.8.8
Nov 28, 2020 17:49:06.116694927 CET	53	51352	8.8.8.8	192.168.2.3
Nov 28, 2020 17:49:06.884823084 CET	59349	53	192.168.2.3	8.8.8.8
Nov 28, 2020 17:49:06.912450075 CET	53	59349	8.8.8.8	192.168.2.3
Nov 28, 2020 17:49:07.798429012 CET	57084	53	192.168.2.3	8.8.8.8
Nov 28, 2020 17:49:07.825588942 CET	53	57084	8.8.8.8	192.168.2.3
Nov 28, 2020 17:49:08.470161915 CET	58823	53	192.168.2.3	8.8.8.8
Nov 28, 2020 17:49:08.497859955 CET	53	58823	8.8.8.8	192.168.2.3
Nov 28, 2020 17:49:09.148407936 CET	57568	53	192.168.2.3	8.8.8.8
Nov 28, 2020 17:49:09.175578117 CET	53	57568	8.8.8.8	192.168.2.3
Nov 28, 2020 17:49:28.395394087 CET	50540	53	192.168.2.3	8.8.8.8
Nov 28, 2020 17:49:28.422703981 CET	53	50540	8.8.8.8	192.168.2.3
Nov 28, 2020 17:49:35.464407921 CET	54366	53	192.168.2.3	8.8.8.8
Nov 28, 2020 17:49:35.504997015 CET	53	54366	8.8.8.8	192.168.2.3
Nov 28, 2020 17:49:47.695863008 CET	53034	53	192.168.2.3	8.8.8.8
Nov 28, 2020 17:49:47.739499092 CET	53	53034	8.8.8.8	192.168.2.3
Nov 28, 2020 17:49:50.130630016 CET	57762	53	192.168.2.3	8.8.8.8
Nov 28, 2020 17:49:50.167737007 CET	53	57762	8.8.8.8	192.168.2.3
Nov 28, 2020 17:50:02.806616068 CET	55435	53	192.168.2.3	8.8.8.8
Nov 28, 2020 17:50:02.833656073 CET	53	55435	8.8.8.8	192.168.2.3
Nov 28, 2020 17:50:07.385375977 CET	50713	53	192.168.2.3	8.8.8.8
Nov 28, 2020 17:50:07.412429094 CET	53	50713	8.8.8.8	192.168.2.3
Nov 28, 2020 17:50:37.652371883 CET	56132	53	192.168.2.3	8.8.8.8
Nov 28, 2020 17:50:37.679497957 CET	53	56132	8.8.8.8	192.168.2.3
Nov 28, 2020 17:50:39.390965939 CET	58987	53	192.168.2.3	8.8.8.8
Nov 28, 2020 17:50:39.426575899 CET	53	58987	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: SecuriteInfo.com.Trojan.DownLoader36.7233.23906.exe PID: 2440
Parent PID: 5572

General

Start time:	17:49:06
Start date:	28/11/2020
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Trojan.DownLoader36.7233.23906.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Trojan.DownLoader36.7233.23906.exe'
Imagebase:	0x320000
File size:	271360 bytes
MD5 hash:	EE4555AC614048E36AAE067B6A032951
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.220940423.000000000032A000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.220940423.000000000032A000.00000004.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.220940423.000000000032A000.00000004.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	AB24C1	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Temp\images.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	AB2407	CreateFileW
C:\Users\user\AppData\Local\Temp\27c398b5630447af830b2dd2bc343446.xml	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	AB4978	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Temp\images.exe	unknown	271370	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 ab b1 5a 6f ef d0 34 3c ef d0 34 3c ef d0 34 3c f1 82 b0 3c f5 d0 34 3c f1 82 a1 3c ff d0 34 3c f1 82 b7 3c a7 d0 34 3c c8 16 4f 3c e0 d0 34 3c ef d0 35 3c 80 d0 34 3c f1 82 be 3c ee d0 34 3c f1 82 a0 3c ee d0 34 3c f1 82 a5 3c ee d0 34 3c 52 69 63 68 ef d0 34 3c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 f3 d6 bb 5f 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.........Zo..4<..4<..4<...<.. 4<...<..4<... <..4<..O<..4<..5<..4<... <..4<...<..4<...<..4<Ri ch..4<........................ PE..L......_...	success or wait	1	AB2420	WriteFile
C:\Users\user\AppData\Local\Te mp\27c398b5630447af830b2dd2bc343446.xml	unknown	1287	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 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 20 3d 20 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 0a 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 3c 44 61 74 65 3e 32 30 31 35 2d 30 39 2d 32 37 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 20 3e 20 0a 3c 41 75 74 68 6f 72 3e 38 39 39 35 35 32 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0a 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 3c 54 72 69 67 67 65 72 73 3e 0a 3c 4c 6f 67 6f 6e 54	<?xml version="1.0" encoding="UTF-16"?>. <Task version = "1.2" xmlns="http://schemas.mic ros oft.com/windows/2004/02/ mit/task">. <RegistrationInfo>.<Date> 2015-09- 27T14:27:44.8929027</D ate > . <Author>899552\user</Au thor>.</RegistrationInfo>. <Triggers>.<LogonT	success or wait	1	AB49A7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.Trojan.DownLoader36.7233.23906.exe	unknown	271360	success or wait	1	AB23CD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	AB085E	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	AB085E	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	AB085E	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	AB085E	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	AB085E	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	AB085E	ReadFile

Analysis Process: conhost.exe PID: 5092 Parent PID: 2440

General

Start time:	17:49:07
Start date:	28/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: cmd.exe PID: 5316 Parent PID: 2440

General

Start time:	17:49:12
Start date:	28/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c schtasks /Create /TN images /XML 'C:\Users\user\AppData\Local\Temp\27c398b5630447af830b2dd2bc343446.xml'
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: MSBuild.exe PID: 2152 Parent PID: 2440

General

Start time:	17:49:12
Start date:	28/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Imagebase:	0x8e0000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: NanoCore, Description: unknown, Source: 00000003.00000003.228783921.0000000004481000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	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	72FB60AC	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	53407A1	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	534089B	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	53407A1	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	5340B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp182E.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5340D1C	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	534089B	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp1B1D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	5340D1C	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	53407A1	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	53407A1	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	72FB60AC	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	72FB60AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	534089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	534089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	534089B	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp182E.tmp	success or wait	1	131BF0E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp1B1D.tmp	success or wait	1	131BF0E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	ed 6b 2e fa 08 94 d8 48	.k.....H	success or wait	1	5340A53	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	69632	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 a9 d1 7b 5a 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 08 00 00 c0 00 00 00 40 00 00 00 00 00 00 de d2 00 00 00 20 00 00 00 e0 00 00 00 00 40 00 00 20 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 01 00 00 10 00 00 39 39 01 00 03 00 40 05 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......PE..L..... {Z.....................@........... ....@.. ....@ ......99....@................	success or wait	1	5340B20	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp182E.tmp	unknown	1320	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	5340A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	57	43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 5c 76 32 2e 30 2e 35 30 37 32 37 5c 4d 53 42 75 69 6c 64 2e 65 78 65	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe	success or wait	1	5340A53	WriteFile
C:\Users\user\AppData\Local\Temp\tmp1B1D.tmp	unknown	1310	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	5340A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc bb 8e f9 04 20 53 f0 bc 12 1c d2 7d 46 46 d4 32 d7 fe a4 68 e2 b4 4d 2b cf cc b9 c1 ec 4c bb 23 8c 58 cb ee 2b 8b b7 cd 01 a9 c0 2a c7 f9 1e d1 7e 66 1e 47 30 5e c3 a9 dd 96 3b b4 2e 95 a2 57 32 c2 3d 10 b3 ce 4b ca 7e c7 4c cc 9f 15 26 66 8d bb 2e 70 c8 04 1b f8 b7 c2 0f e9 ff e7 0b 10 3a 37 72 48 7d bd be f1 88 0d 2f 48 16 b2 87 06 17 96 4c 8c b6 04 3f b5 f3 04 41 08 4b 07 d1 e5 84 4a 17 3d 38 78 21 19 a1 e1 e4 2b fa 32 65 27 d7 1f 45 3f d9 47 11 9e a7 e7 a8 01 f0 5b 00 26	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i..... S.....}FF.2.. .h..M+.....L.#.X..+.....*.... ~f.G0^....;....W2.=...K.~.L... &f...p.....:7rH}...../H .....L...?...A.K....J.=8x!... .+.2e'..E?.G.....[.&	success or wait	1	5340A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	426832	c1 e9 67 26 6a 6f 1f 01 d5 49 50 67 08 81 cd a2 47 4d d1 a4 d4 0d a7 52 3e 69 e1 fc 09 6f 8c b1 04 49 e1 3e e3 bb b0 26 9f 72 7b d6 fa a5 93 38 a9 d3 a5 93 7d ff da 89 8a 45 03 7f ea e6 96 76 cf 21 37 95 75 33 65 bc fc 20 fb c0 05 b7 f7 64 62 bd 90 15 7d b2 c7 1d 02 02 ab e8 22 c2 74 28 06 78 43 39 b8 63 70 15 42 e6 e0 91 e1 37 82 0f 1b 27 bd 93 ad a1 d3 7f c2 25 bd 09 b2 06 eb c7 77 86 5e ac c1 5f 13 c4 d2 02 d8 9d d4 b4 f1 42 b7 57 25 fd 3c ce a6 d9 a4 69 e1 30 d1 7b 39 bb 78 53 fc ab fb 35 c5 d8 c7 29 05 ef 77 ca 0f 24 14 92 43 87 80 3f 60 46 d7 8f da 75 a8 35 db 92 54 b6 58 ab 77 27 53 69 f4 f0 7a b2 6e 7b 8f ef b9 ea 9f 84 59 21 6d d8 d3 1c 52 41 f8 b9 e3 78 67 d3 d0 ba 03 e9 5b 37 8a 18 89 7a b7 9f 39 40 02 4b ca 2d 9a fe 88 54 95 8d 2b d8 41 43 65	..g&jo...IPg....GM.....R>i...o ...I.>...&.r{....8....}....E.. ...v.!7.u3e.. .....db...}..... ..".t(.xC9.cp.B....7...'..... .%.....w.^._.....B.W%.<. ...i.0.{9.xS...5...)..w..$..C..? `F...u.5..T.X.w'Si..z.n{.... ..Y!m...RA...xg..... [7...z..9@.K.-...T..+.ACe	success or wait	1	5340A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 7e 61 d3 f8 a3 01 06 96 0c a9 7e ba 7e 86 90 d9 e5 05 8d ca 33 e7 55 0b	9iH....}Z..4..f.~a.....~.~. .....3.U.	success or wait	1	5340A53	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	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	72FE5544	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5340A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4096	success or wait	1	5340A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4096	end of file	1	5340A53	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	5340C12	RegSetValueExW

Analysis Process: schtasks.exe PID: 4928 Parent PID: 5316

General

Start time:	17:49:13
Start date:	28/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /Create /TN images /XML 'C:\Users\user\AppData\Local\Temp\27c398b5630447af830b2dd2bc343446.xml'
Imagebase:	0xb40000
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\27c398b5630447af830b2dd2bc343446.xml	unknown	2	success or wait	1	B4AB22	ReadFile
C:\Users\user\AppData\Local\Temp\27c398b5630447af830b2dd2bc343446.xml	unknown	1288	success or wait	1	B4ABD9	ReadFile

Analysis Process: schtasks.exe PID: 5920 Parent PID: 2152

General

Start time:	17:49:15
Start date:	28/11/2020

Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp182E.tmp'
Imagebase:	0xb40000
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\tmp182E.tmp	unknown	2	success or wait	1	B4AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp182E.tmp	unknown	1321	success or wait	1	B4ABD9	ReadFile

Analysis Process: conhost.exe PID: 5948 Parent PID: 5920

General

Start time:	17:49:15
Start date:	28/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 2168 Parent PID: 2152

General

Start time:	17:49:15
Start date:	28/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp1B1D.tmp'
Imagebase:	0xb40000
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\tmp1B1D.tmp	unknown	2	success or wait	1	B4AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp1B1D.tmp	unknown	1311	success or wait	1	B4ABD9	ReadFile

Analysis Process: conhost.exe PID: 4120 Parent PID: 2168

General

Start time:	17:49:16
Start date:	28/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: MSBuild.exe PID: 5292 Parent PID: 528

General

Start time:	17:49:16
Start date:	28/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe 0
Imagebase:	0x9d0000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

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	72FB60AC	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	72FB60AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\MSBuild.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	7266DCB3	unknown
\Device\ConDrv	unknown	169	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 42 75 69 6c 64 20 45 6e 67 69 6e 65 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 0d 0a 5b 4d 69 63 72 6f 73 6f 66 74 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 2c 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 5d 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 20 32 30 30 35 2e 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) Build Engine Version 2.0.50727.8922.. [Microsoft .NET Framework, Version 2.0. 50727.8922]..Copyright (C) Microsoft Corporation 2005. All rights reserved.....	success or wait	1	7266DFAB	unknown
\Device\ConDrv	unknown	66	4d 53 42 55 49 4c 44 20 3a 20 65 72 72 6f 72 20 4d 53 42 31 30 30 39 3a 20 50 72 6f 6a 65 63 74 20 66 69 6c 65 20 64 6f 65 73 20 6e 6f 74 20 65 78 69 73 74 2e 0d 0a 53 77 69 74 63 68 3a 20 30 0d 0a	MSBUILD : error MSB1009: Project file does not exist...Switch: 0..	success or wait	1	7266DFAB	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\MSBuild.exe.log	unknown	325	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 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 42 75 69 6c 64 2e 45 6e 67 69 6e 65 2c 20 56 65 72 73 69 6f 6e 3d 32 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 42 75 69 6c 64 2e 46 72 61 6d 65 77 6f 72 6b 2c 20	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..2,"Microsoft.Build.Engine, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.Build.Framework,	success or wait	1	7328A33A	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	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	72FE8738	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.rsp	unknown	4096	success or wait	1	7266C1B7	unknown

Analysis Process: conhost.exe PID: 1968 Parent PID: 5292

General

Start time:	17:49:17
Start date:	28/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: 5972 Parent PID: 528

General

Start time:	17:49:17
Start date:	28/11/2020
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x4c0000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, 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	72FB60AC	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	72FB60AC	unknown
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	72FB60AC	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	72FB60AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	7266DCB3	unknown
\Device\ConDrv	unknown	169	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 42 75 69 6c 64 20 45 6e 67 69 6e 65 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 0d 0a 5b 4d 69 63 72 6f 73 6f 66 74 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 2c 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 5d 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 20 32 30 30 35 2e 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) Build Engine Version 2.0.50727.8922..[Microsoft .NET Framework, Version 2.0.50727.8922]..Copyright (C) Microsoft Corporation 2005. All rights reserved.....	success or wait	1	7266DFAB	unknown
\Device\ConDrv	unknown	66	4d 53 42 55 49 4c 44 20 3a 20 65 72 72 6f 72 20 4d 53 42 31 30 30 39 3a 20 50 72 6f 6a 65 63 74 20 66 69 6c 65 20 64 6f 65 73 20 6e 6f 74 20 65 78 69 73 74 2e 0d 0a 53 77 69 74 63 68 3a 20 30 0d 0a	MSBUILD : error MSB1009: Project file does not exist...Switch: 0..	success or wait	1	7266DFAB	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	unknown	441	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 58 6d 6c 5c 35 32 37 63 39 33 33 31 39 34 66 33 61 39 39 61 38 31 36 64 38 33 63 36 31 39 61 33 65 31 64 33 5c 53 79 73 74 65 6d 2e 58 6d 6c 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66	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.Xml\527c933194f3a99a816d83c619a3e1d3\System.Xml.ni.dll",0..2,"Microsof	success or wait	1	7328A33A	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	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7266C1B7	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7266C1B7	unknown

Analysis Process: conhost.exe PID: 2792 Parent PID: 5972

General

Start time:	17:49:17
Start date:	28/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: 5588 Parent PID: 3388

General

Start time:	17:49:27
Start date:	28/11/2020
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x890000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

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	72FB60AC	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	72FB60AC	unknown
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	72FB60AC	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	72FB60AC	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	118A897	WriteFile
\Device\ConDrv	unknown	169	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 42 75 69 6c 64 20 45 6e 67 69 6e 65 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 0d 0a 5b 4d 69 63 72 6f 73 6f 66 74 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 2c 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 5d 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 20 32 30 30 35 2e 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) Build Engine Version 2.0.50727.8922.. [Microsoft .NET Framework, Version 2.0. 50727.8922]..Copyright (C) Microsoft Corporation 2005. All rights reserved.....	success or wait	1	118A897	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	137	4d 53 42 55 49 4c 44 20 3a 20 65 72 72 6f 72 20 4d 53 42 31 30 30 33 3a 20 53 70 65 63 69 66 79 20 61 20 70 72 6f 6a 65 63 74 20 6f 72 20 73 6f 6c 75 74 69 6f 6e 20 66 69 6c 65 2e 20 54 68 65 20 63 75 72 72 65 6e 74 20 77 6f 72 6b 69 6e 67 20 64 69 72 65 63 74 6f 72 79 20 64 6f 65 73 20 6e 6f 74 20 63 6f 6e 74 61 69 6e 20 61 20 70 72 6f 6a 65 63 74 20 6f 72 20 73 6f 6c 75 74 69 6f 6e 20 66 69 6c 65 2e 0d 0a	MSBUILD : error MSB1003: Specify a project or solution file. The current working directory does not contain a project or solution file...	success or wait	1	118A897	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	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	118A897	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	118A897	ReadFile

Analysis Process: conhost.exe PID: 5860 Parent PID: 5588

General

Start time:	17:49:27
Start date:	28/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis