ID: 881372
Sample Name: Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe
Cookbook: default.jbs
Time: 11:26:07
Date: 04/06/2023
Version: 37.1.0 Beryl

Table of Contents

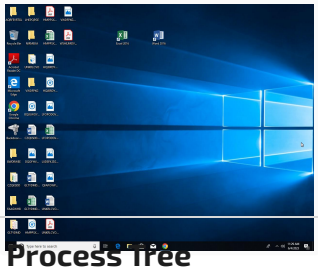
Windows Analysis Report

Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe

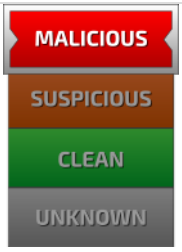
Overview

General Information

Sample Name:	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe
Analysis ID:	881372
MD5:	d2c96c075741…
SHA1:	09667b1bef10f…
SHA256:	d2a573edc893…
Tags:	exe NanoCore RAT
Infos:	



Detection



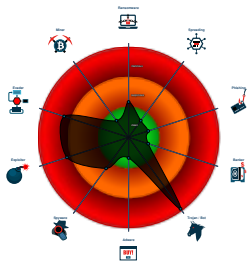
Nanocore

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Antivirus / Scanner detection for sub…
- Sigma detected: Scheduled temp fil…
- Antivirus detection for dropped file
- Sigma detected: Drops script at sta…
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic

Classification



Process Tree

- **System is w10x64**
- Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe (PID: 7044 cmdline: C:\Users\user\Desktop\Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe MD5: D2C96C075741CCD8BED558E39838A59D)
  - MSBuild.exe (PID: 5980 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe MD5: 88BBB7610152B48C2B3879473B17857E)
    - schtasks.exe (PID: 5916 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp9A5C.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 3676 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - MSBuild.exe (PID: 5744 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe 0 MD5: 88BBB7610152B48C2B3879473B17857E)
    - conhost.exe (PID: 3100 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - znytpstdcrwsisx.exe (PID: 5292 cmdline: "C:\Users\user\AppData\Roaming\hdoydskbdx\znytpstdcrwsisx.exe" MD5: A360B0402DD16AE837F59D09E1BF3B3C)
    - MSBuild.exe (PID: 5944 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe MD5: 88BBB7610152B48C2B3879473B17857E)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Nanocore RAT, NanoCore	Nanocore is a Remote Access Tool used to steal credentials and to spy on cameras. It as been used for a while by numerous criminal actors as well as by nation state threat actors.	• APT33 • The Gorgon Group	http://https://assets.virustotal.com/reports/2021trends.pdfhttps://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/https://blog.360totalsecurity.com/en/vendetta-new-threat-actor-from-europe/https://blog.checkpoint.com/security/march-2023s-most-wanted-malware-new-emotet-campaign-bypasses-microsoft-blocks-to-distribute-malicious-onenote-files/https://blog.morphisec.com/syk-crypter-discord	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.nanocore

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "2ad4e32f-c687-4329-b5e5-302ef0e0",
  "Group": "Default",
  "Domain1": "nickdns22.duckdns.org",
  "Domain2": "127.0.0.1",
  "Port": 1896,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Disable",
  "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

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\znytpstdcrwsisx.fr.url	Methodology_Suspicious_Shortcut_Local_URL	Detects local script usage for .URL persistence	@itsreallynick (Nick Carr), @QW5kcmV3 (Andrew Thompson)	• 0x14:$file: URL=file:/// • 0x71:$file: URL=file:/// • 0x0:$url_explicit: [InternetShortcut] • 0x5d:$url_explicit: [InternetShortcut]

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000003.407208526.000000000175C000.00000004.00000020.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xfd9d:$x1: NanoCore.ClientPluginHost • 0xfdda:$x2: IClientNetworkHost • 0x1390d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000006.00000003.407208526.000000000175C000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000003.407208526.000000000175C000.00000004.00000020.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfb05:$a: NanoCore • 0xfb15:$a: NanoCore • 0xfd49:$a: NanoCore • 0xfd5d:$a: NanoCore • 0xfd9d:$a: NanoCore • 0xfb64:$b: ClientPlugin • 0xfd66:$b: ClientPlugin • 0xfda6:$b: ClientPlugin • 0xfc8b:$c: ProjectData • 0x10692:$d: DESCrypto • 0x1805e:$e: KeepAlive • 0x1604c:$g: LogClientMessage • 0x12247:$i: get_Connected • 0x109c8:$j: #=q • 0x109f8:$j: #=q • 0x10a14:$j: #=q • 0x10a44:$j: #=q • 0x10a60:$j: #=q • 0x10a7c:$j: #=q • 0x10aac:$j: #=q • 0x10ac8:$j: #=q
00000006.00000003.407208526.000000000175C000.00000004.00000020.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xfd9d:$a1: NanoCore.ClientPluginHost • 0xfd5d:$a2: NanoCore.ClientPlugin • 0x11cb6:$b1: get_BuilderSettings • 0xfbb9:$b2: ClientLoaderForm.resources • 0x113d6:$b3: PluginCommand • 0xfd8e:$b4: IClientAppHost • 0x1a20e:$b5: GetBlockHash • 0x1230e:$b6: AddHostEntry • 0x16001:$b7: LogClientException • 0x1227b:$b8: PipeExists • 0xfdc7:$b9: IClientLoggingHost
00000006.00000003.409346361.0000000001431000.00000004.00000020.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x35a4d:$x1: NanoCore.ClientPluginHost • 0x35a8a:$x2: IClientNetworkHost • 0x395bd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 150 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.MSBuild.exe.31e3c74.1.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
7.2.MSBuild.exe.31e3c74.1.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
7.2.MSBuild.exe.31e3c74.1.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xe38:$x2: NanoCore.ClientPlugin • 0xe75:$x3: NanoCore.ClientPluginHost • 0xe5a:$i1: IClientApp • 0xe4e:$i2: IClientData • 0xe29:$i3: IClientNetwork • 0xec3:$i4: IClientAppHost • 0xe65:$i5: IClientDataHost • 0xeb0:$i6: IClientLoggingHost • 0xe8f:$i7: IClientNetworkHost • 0xea2:$i8: IClientUIHost • 0xed2:$i9: IClientNameObjectCollection • 0xef7:$i10: IClientReadOnlyNameObjectCollection • 0xe41:$s1: ClientPlugin • 0x177c:$s1: ClientPlugin • 0x1789:$s1: ClientPlugin • 0x11f9:$s6: get_ClientSettings • 0x1249:$s7: get_Connected
7.2.MSBuild.exe.31e3c74.1.raw.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xe75:$a1: NanoCore.ClientPluginHost • 0xe38:$a2: NanoCore.ClientPlugin • 0x120c:$b1: get_BuilderSettings • 0xec3:$b4: IClientAppHost • 0x127d:$b6: AddHostEntry • 0x12ec:$b7: LogClientException • 0x1261:$b8: PipeExists • 0xeb0:$b9: IClientLoggingHost
6.3.znytpstdcrwsisx.exe.16ec7f8.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 190 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Data Obfuscation

Sigma detected: Drops script at startup location

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: 192.168.2.3 - Destination IP: 192.169.69.26

Timestamp:	192.168.2.3192.169.69.264971118962025019 06/04/23-11:28:18.475887
SID:	2025019
Source Port:	49711
Destination Port:	1896
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26

Timestamp:	192.168.2.3192.169.69.264971718962025019 06/04/23-11:28:50.523433
SID:	2025019
Source Port:	49717
Destination Port:	1896
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26

Timestamp:	192.168.2.3192.169.69.264970718962025019 06/04/23-11:27:57.173727
SID:	2025019
Source Port:	49707
Destination Port:	1896
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26

Timestamp:	192.168.2.3192.169.69.264971218962025019 06/04/23-11:28:23.420896
SID:	2025019
Source Port:	49712

Destination Port:	1896
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26	
Timestamp:	192.168.2.3192.169.69.264971318962025019 06/04/23-11:28:28.432846
SID:	2025019
Source Port:	49713
Destination Port:	1896
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26	
Timestamp:	192.168.2.3192.169.69.264971918962025019 06/04/23-11:29:00.977409
SID:	2025019
Source Port:	49719
Destination Port:	1896
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26	
Timestamp:	192.168.2.3192.169.69.264971818962025019 06/04/23-11:28:55.916794
SID:	2025019
Source Port:	49718
Destination Port:	1896
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26	
Timestamp:	192.168.2.3192.169.69.264970518962025019 06/04/23-11:27:45.907549
SID:	2025019
Source Port:	49705
Destination Port:	1896
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26	
Timestamp:	192.168.2.3192.169.69.264969918962025019 06/04/23-11:27:14.981963
SID:	2025019
Source Port:	49699
Destination Port:	1896
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26	
Timestamp:	192.168.2.3192.169.69.264970618962025019 06/04/23-11:27:50.915043
SID:	2025019
Source Port:	49706
Destination Port:	1896
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26	
Timestamp:	192.168.2.3192.169.69.264970118962025019 06/04/23-11:27:25.413836
SID:	2025019
Source Port:	49701
Destination Port:	1896
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26	
Timestamp:	192.168.2.3192.169.69.264970018962025019 06/04/23-11:27:20.405611
SID:	2025019
Source Port:	49700
Destination Port:	1896
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Found malware configuration
- 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

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)
- Binary is likely a compiled AutoIt script file

Data Obfuscation

- .NET source code contains potential unpacker

Boot Survival

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

Malware Analysis System Evasion

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

HIPS / PFW / Operating System Protection Evasion

- Writes to foreign memory regions
- Allocates memory in foreign processes
- Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

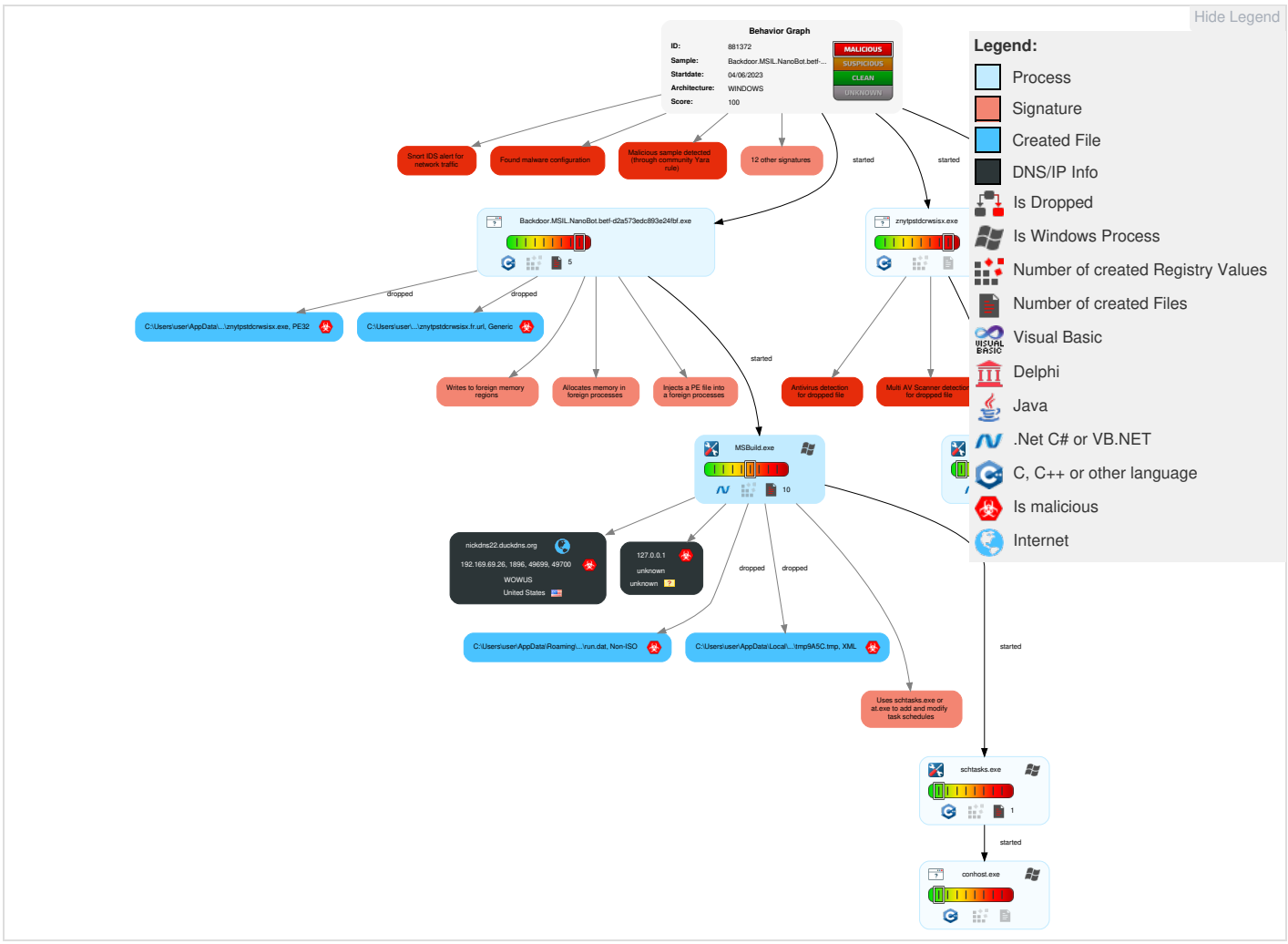
Detected Nanocore Rat

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	2 Command and Scripting Interpreter	1 Scheduled Task/Job	1 Access Token Manipulation	1 Masquerading	1 1 Input Capture	1 System Time Discovery	Remote Services	1 1 Input Capture	Exfiltration Over Other Network Medium	1 2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	2 Registry Run Keys / Startup Folder	3 1 2 Process Injection	1 Disable or Modify Tools	LSASS Memory	2 1 Security Software Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Remote Access Software	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 1 Virtualization/Sandbox Evasion	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	2 Registry Run Keys / Startup Folder	1 Access Token Manipulation	NTDS	2 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	3 1 2 Process Injection	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	2 2 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Deobfuscate/Decode Files or Information	Cached Domain Credentials	1 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Obfuscated Files or Information	DCSync	Network Sniffing	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 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

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
Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe	70%	ReversingLabs	Win32.Trojan.Nymeria	
Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe	65%	Virustotal		Browse
Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe	100%	Avira	DR/AutoIt.Gen8	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\hdoydskbdx\znytpstdcrwsisx.exe	100%	Avira	DR/AutoIt.Gen8	
C:\Users\user\AppData\Roaming\hdoydskbdx\znytpstdcrwsisx.exe	81%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
nickdns22.duckdns.org	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.sysinternals.comopenThe	0%	URL Reputation	safe	
nickdns22.duckdns.org	0%	Avira URL Cloud	safe	
nickdns22.duckdns.org	2%	Virustotal		Browse
http://www.sysinternals.comFileVersionLegalCopyrightLISTBOXDEL:AllUsersuserComputerscomputerGroupsgr	0%	Avira URL Cloud	safe	
http://https://rrchnm.org/	0%	Virustotal		Browse
http://https://rrchnm.org/	0%	Avira URL Cloud	safe	
http://www.sysinternals.comopenConnection	0%	Avira URL Cloud	safe	
http://www.sysinternals.comWindowPositionSOFTWARE	0%	Avira URL Cloud	safe	
http://https://www.virustotal.comPOST4e3202fdbe953d628f650229af5b3eb49cd46b2d3bfe5546ae3c5fa48b554e0capikey	0%	Avira URL Cloud	safe	
http://https://www.sysinternals.comntdllRtlInitUnicodeStringNtOpenDirectoryObjectNtQuerySectionNtQueryDirec	0%	Avira URL Cloud	safe	
http://www.sysinternals.comFileVersionLegalCopyright	0%	Avira URL Cloud	safe	
127.0.0.1	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
nickdns22.duckdns.org	192.169.69.26	true	true	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
nickdns22.duckdns.org	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
127.0.0.1	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

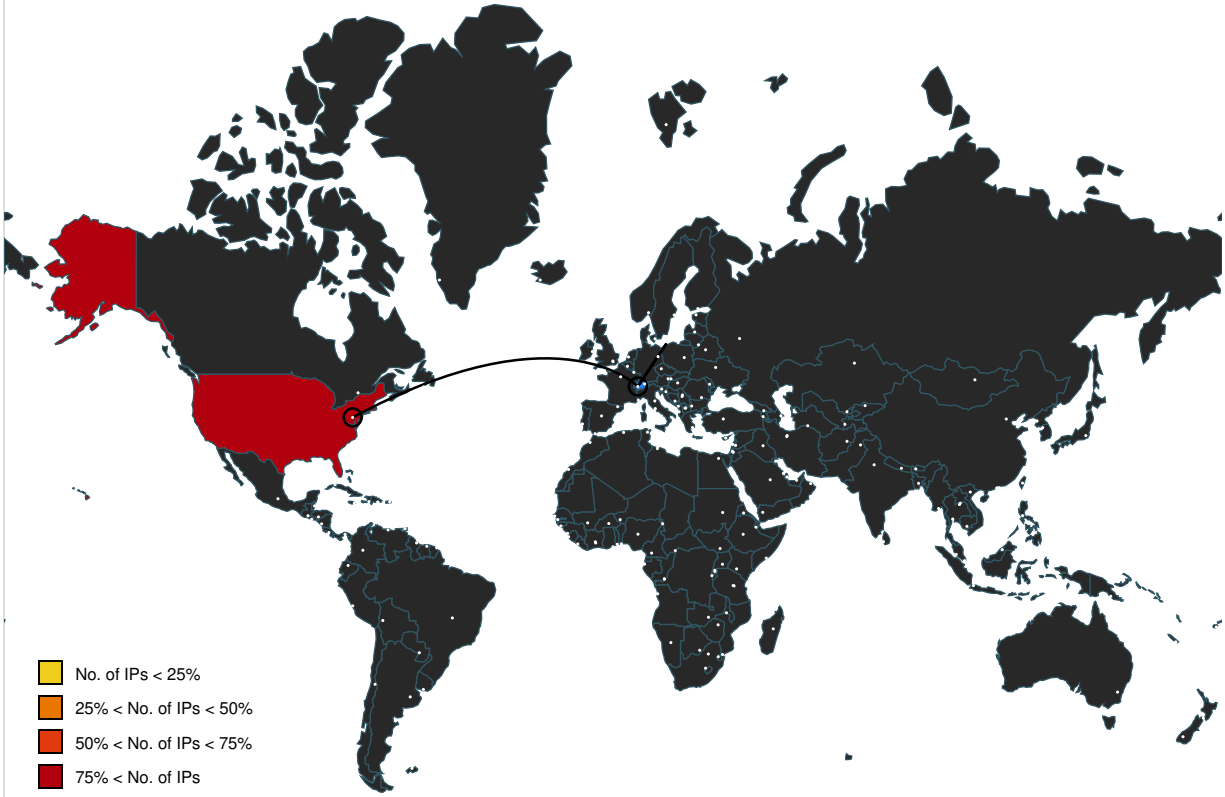
Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.zotero.org/	znytpstdcrwsisx.exe.0.dr	false		high
http://https://ims-prod06.adobelogin.com	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.378236827.000000005691000.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.368183823.0000000004C32000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://crashpad.chromium.org/	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, znytpstdcrwsisx.exe.0.dr	false		high
http://https://ims-na1-stg1.adobelogin.com	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.378236827.000000005691000.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.368183823.0000000004C32000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.mendeley.com?dgcid=Mendeley_Desktop_Help-menu-website	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, znytpstdcrwsisx.exe.0.dr	false		high
http://https://service.elsevier.com/app/home/supporthub/mendeley/?dgcid=Mendeley_Desktop_Help-menu-FAQ	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, znytpstdcrwsisx.exe.0.dr	false		high
http://https://crashpad.chromium.org/bug/new	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, znytpstdcrwsisx.exe.0.dr	false		high
http://https://www.gmu.edu/	znytpstdcrwsisx.exe.0.dr	false		high
http://https://csl.mendeley.com	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, znytpstdcrwsisx.exe.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sysinternals.com	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.378236827.000000005691000.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.365309489.0000000004823000.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.368183823.0000000004C32000.00000004.00000020.00020000.00000000.sdmp	false		high
http://support.mendeley.com/customer/portal/articles/227955	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, znytpstdcrwsisx.exe.0.dr	false		high
http://https://www.elsevier.com/legal/privacy-policy	znytpstdcrwsisx.exe.0.dr	false		high
http://https://www.virustotal.com/about/terms-of-service%s	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.369979852.000000005DF0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.sysinternals.comopenThe	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.378236827.000000005691000.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.366011372.0000000005469000.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.365309489.0000000004823000.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.372536607.0000000004A39000.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.374414583.00000000053CA000.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.368183823.0000000004C32000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://crashpad.chromium.org/https://crashpad.chromium.org/bug/new	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, znytpstdcrwsisx.exe.0.dr	false		high
http://https://rrchnm.org/	znytpstdcrwsisx.exe.0.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://creativecommons.org/licenses/by-sa/3.0/	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, znytpstdcrwsisx.exe.0.dr	false		high
http://www.sysinternals.comFileVersionLegalCopyrightLISTBOXDEL:AllUsersuserComputerscomputerGroupsgr	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, znytpstdcrwsisx.exe.0.dr	false	• Avira URL Cloud: safe	low
http://https://service.elsevier.com/app/answers/detail/a_id/19611/kw/duplicates/supporthub/mendeley/Yes	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, znytpstdcrwsisx.exe.0.dr	false		high
http://https://www.elsevier.com/legal/elsevier-website-terms-and-conditions	znytpstdcrwsisx.exe.0.dr	false		high
http://https://www.mendeley.com/guides?dgcid=Mendeley_Desktop_Help-menu-Help-guides	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, znytpstdcrwsisx.exe.0.dr	false		high
http://https://clients2.google.com/service/update2/crxupdate_urlBrowser	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.369979852.000000005DF0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://p.yusukekamiyamane.com/	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, znytpstdcrwsisx.exe.0.dr	false		high
http://https://github.com/Juris-M/citeproc-js	znytpstdcrwsisx.exe.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sysinternals.comWindowPositionSOFTWARE	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.378236827.0000000005691000.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.366011372.0000000005469000.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.365309489.0000000004823000.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.372536607.0000000004A39000.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.374414583.00000000053CA000.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.364770823.0000000004CB8000.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.368183823.0000000004C32000.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.369979852.0000000005DF0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://service.elsevier.com/app/contact/supporthub/mendeley?dgcid=Mendeley_Desktop_Help-menu-Contac	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, znytpstdcrwsisx.exe.0.dr	false		high
http://https://plasma.kde.org	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, znytpstdcrwsisx.exe.0.dr	false		high
http://https://www.mendeley.com/library	znytpstdcrwsisx.exe.0.dr	false		high
http://https://www.virustotal.com/en/about/terms-of-service/	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.369979852.0000000005DF0000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://www.mendeley.com/guides?dgcid=Mendeley_Desktop_Help-menu-Help-guideshttps://www.mendeley.com	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, znytpstdcrwsisx.exe.0.dr	false		high
http://citationstyles.org/	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, znytpstdcrwsisx.exe.0.dr	false		high
http://www.sysinternals.comopenConnection	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.378236827.0000000005691000.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.366011372.0000000005469000.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.365309489.0000000004823000.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.372536607.0000000004A39000.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.374414583.00000000053CA000.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.368183823.0000000004C32000.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.369979852.0000000005DF0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://github.com/citation-style-language/styles	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, znytpstdcrwsisx.exe.0.dr	false		high
http://https://www.virustotal.comPOST4e3202fdbe953d628f650229af5b3eb49cd46b2d3bfe5546ae3c5fa48b554e0capikey	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.369979852.0000000005DF0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.sysinternals.comntdllRtlInitUnicodeStringNtOpenDirectoryObjectNtQuerySectionNtQueryDirec	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, znytpstdcrwsisx.exe.0.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sysinternals.comFileVersionLegalCopyright	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.378236827.000000005691000.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.366011372.0000000005469000.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.365309489.000000000482300.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.372536607.0000000004A39000.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.374414583.00000000053CA000.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.368183823.0000000004C32000.00000004.00000020.00020000.00000000.sdmp, Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, 00000000.00000003.369979852.0000000005DF0000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://citationstyles.org	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe, znytpstdcrwsisx.exe.0.dr	false		high
http://https://service.elsevier.com/app/answers/detail/a_id/22094/kw/migrate/supporthub/mendeley/	znytpstdcrwsisx.exe.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.169.69.26	nickdns22.duckdns.org	United States		23033	WOWUS	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	881372
Start date and time:	2023-06-04 11:26:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 56s
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:	12
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:	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe
Detection:	MAL
Classification:	mal100.troj.expl.evad.winEXE@11/9@12/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 20% (good quality ratio 20%) • Quality average: 95.5% • Quality standard deviation: 4.5%
HCA Information:	Failed
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe
- TCP Packets have been reduced to 100
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:27:12	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\znytpstdcrwsisx.fr.url
11:27:13	API Interceptor	834x Sleep call for process: MSBuild.exe modified
11:27:15	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe" s>$(Arg0)

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

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
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
Reputation:	moderate, very likely benign file
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\Temp\aut8DF8.tmp

Process:	C:\Users\user\Desktop\Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe
File Type:	data
Category:	dropped
Size (bytes):	207872
Entropy (8bit):	**7.999050560075495**
Encrypted:	**true**
SSDEEP:	6144:yfHioBK/DQ0vgnZ92J6yN8n59mrjuydK/znla5oC:yfOjvgb2JpNeorjOznA5oC
MD5:	D63A88D1A1B8198E665C1094E96488BC
SHA1:	427EA9EB92C1C20B647CECD78C6085B509BCC326
SHA-256:	68B951C18FA6D7FDD30A5EB01609BAB36677D1414A6EC2D5A25C327A7D7CB9B0
SHA-512:	9C79A3F8E506447F6B5D24E27CED80E4EE449245D3483741EBD27E89656423B0ABDE9AE8ADBEAB430566999E86E3E70A8FECB6FE7F515F327066FF42E7A9E236
Malicious:	false
Preview:	z.(+...l.....;.N.....E.....q..B....5.UTtw.Sf..aE.j.Ix.Tq....9..8w.PxA...*.-...xA&..'..mX.....9.My..M-.2V0....,...M..q.....v...._..T67b5.Jb.S..Q!QQ..(ni....J..Y&..z..gj5...jH..G......s.7...0...u.AL.....$....Y...S...i.....WJ.t.=.....R..@...O2..sf.XQ.....3.z....NQl.h....X .....:d.O.....1N...i6..EU..J8.....V.{.c.F.....A..C[....m...E..N..PZ.....{H..e~..l.....7..%..o .M+.B..~..../\Y=s..JX@.....*f..s&..3..1Y..._:...c/.....Tc.../A..>n.F.../.Z.U.i.....}...+..i4\....Z#.....&.JD.."O.?.ou(u4%b..O..Tm.y.n...{.....t.~w?.0.3.Bx..)....e.-.][. ...QeH.n.. ...vM.....m...RE..../(N.....H.up}.....v..l..ey.o.((O..#s.l.LX...j..9)...X.h..$%Vk.....ta_.~.....2V..X.@o..R.....`[.T...,.O..Q.H.....s.C...J.w.....q.....wr...N.'W.r.;."jo.Z....?....z.....b.w.D..b|...@.....N;....^L....2..nx..-...~.+@....C.....A./6GJ.t..g.s.MA.R...rh.....1..*4.B..).....V.HM..AB....zJ.`|`...g....iwOd..Q..B..F.s.7.WS.-.@...6...l...j.a]U..-"!".!.

C:\Users\user\AppData\Local\Temp\cbmfpeiu

Process:	C:\Users\user\Desktop\Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe
File Type:	data
Category:	dropped
Size (bytes):	207872
Entropy (8bit):	**7.999050560075495**

Encrypted:	**true**
SSDEEP:	6144:yfHioBK/DQ0vgnZ92J6yN8n59mrjuydK/znla5oC:yfOjvgb2JpNeorjOznA5oC
MD5:	D63A88D1A1B8198E665C1094E96488BC
SHA1:	427EA9EB92C1C20B647CECD78C6085B509BCC326
SHA-256:	68B951C18FA6D7FDD30A5EB01609BAB36677D1414A6EC2D5A25C327A7D7CB9B0
SHA-512:	9C79A3F8E506447F6B5D24E27CED80E4EE449245D3483741EBD27E89656423B0ABDE9AE8ADBEAB430566999E86E3E70A8FECB6FE7F515F327066FF42E7A9E23 6
Malicious:	false
Preview:	z.(+...!.....;.N.....E.....q..B....5.UTtw.Sf..aE.j.lx.Tq....9..8w.PxA...*.-...xA&..'..mX.....9.My..M-.2V0....,...M..q.....v...._..T67b5.Jb.S..Q!QQ..(ni....J..Y&..z..gj5...jH.. G.....s.7...0...u.AL.....$....Y...S...i.....WJ.t.=.....R..@...O2..sf.XQ.....3.z....NQl.h....X .....:d.O.....1N...i6..EU..J8.....V.{.c.F.....A..C[....m...E..N..PZ.....{H..e~..l.....7.. %..o .M+.B..~..../\Y=s..JX@.....*f..s&..3..1Y..._:...c/.....Tc.../A..>n.F.../.Z.U.i.....}...+..i4\....Z#.....&.JD.."O.?.ou(u4%b..O..Tm.y.n...{.....t.~w?.0.3.Bx..)....e.-.][. ...QeH.n.. ...vM.....m...RE..../(N.....H.up}.....v..l..ey.o.((O..#s.l.LX...j..9)...X.h..$%Vk.....ta_.~.....2V..X.@o..R.....`[.T...,.O..Q.H.....s.C...J.w.....q.....wr...N.'W.r.;."jo.Z....?....z.....b.w. D..b|...@.....N;....^L....2..nx..-...~.+@....C.....A./6GJ.t..g.s.MA.R...rh.....1..*4.B..).....V.HM..AB....zJ.`|`...g....iwOd..Q..B..F.s.7.WS.-.@...6...l...j.a]U..-"!".!.

C:\Users\user\AppData\Local\Temp\tmp9A5C.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:	E530DA4A5D4336FC37838D0E93B5EB3804B9C489C71F6954A47FC81A4C655BB72EC493E109CF96E6E3617D7623AC80697AD3BBD5FFC6281BAFC8B34DCA5E65 67
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>.. </Princi pals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoing OnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyI fNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunO nlyIfIdle>.. <Wak

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
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:a0Qn:/Qn
MD5:	0E18C253EB33804FAEB60D95384CE28F
SHA1:	5265FBE488A3AAB00CE74A325B5D6CA465A55142
SHA-256:	ADDCC29B2ABC88AC2C25A4F28879604E2F1CF0104A7A1CF6E0B16528FB50183F
SHA-512:	00D7DEE5D4A845629844DE6A41E373247524C8E187CF05C2B7AE3570C1DA2BC4E9E1892C90EE6F52399858406D6202C0929CBD3F35AC9A855EB7D84EE3FD65 3
Malicious:	**true**
Preview:	..)Q)e.H

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
MD5:	A35128E4E28B27328F70E4E8FF482443
SHA1:	B89066B2F8DB34299AABFD7ABEE402D5444DD079
SHA-256:	88AEA00733DC4B570A29D56A423CC5BF163E5ACE7AF349972EB0BBA8D9AD06E1

SHA-512:	F098E844B5373B34642B49B6E0F2E15CFDAA1A8B6CABC2196CEC0F3765289E5B1FD4AB588DD65F97C8E51FA9A81077621E9A06946859F296904C646906A70F33
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\znytpstdcrwsisx.fr.url

Process:	C:\Users\user\Desktop\Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe
File Type:	Generic INItialization configuration [InternetShortcut]
Category:	modified
Size (bytes):	186
Entropy (8bit):	4.970025311868907
Encrypted:	false
SSDEEP:	3:HRAbABGQYm5uOWXp5cViEaKC5D9c6AQI6ABGQYm5uOWXp5cViEaKC5D9c6AQA:HRYFVmwOWXp+NaZ5D+1YFVmwOWXp+Nay
MD5:	AC58C72B816D89CF6D82C181DF3FCD1C
SHA1:	ED37DDAD70163D899BF6DD12DBE4B839E147AE0A
SHA-256:	2B28DEC4AEE449EF1FD1FEC9E7C9CB29D967868CCFBD41E9CB1939DA8A202A7F
SHA-512:	0DD626181E2074E41D1FD55FF153DBD843D06B992B2CABB2B8ADB4DBDE0C993C915F2CDB45A362E5BC90751B015045E27725D09707D54DBEF344189954B4500
Malicious:	**true**
Yara Hits:	• Rule: Methodology_Suspicious_Shortcut_Local_URL, Description: Detects local script usage for .URL persistence, Source: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\znytpstdcrwsisx.fr.url, Author: @itsreallynick (Nick Carr), @QW5kcmV3 (Andrew Thompson)
Preview:	[InternetShortcut]..URL=file:///C:\Users\user\AppData\Roaming\hdoydskbdx\znytpstdcrwsisx.exe[InternetShortcut]..URL=file:///C:\Users\user\AppData\Roaming\hdoydskbdx\znytpstdcrwsisx.exe

C:\Users\user\AppData\Roaming\hdoydskbdx\znytpstdcrwsisx.exe

Process:	C:\Users\user\Desktop\Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4967954
Entropy (8bit):	5.837705465010447
Encrypted:	false
SSDEEP:	49152:RVg5tQ7aoFsGabuKxN5GmoZgZh8Jjf1SXAEaYD:fg56ddKPo2
MD5:	A360B0402DD16AE837F59D09E1BF3B3C
SHA1:	F62C60788659D8EAD3AAB08A752C02F270CF8CCD
SHA-256:	490AD4D568CF15F2B6BAFE80BEC8857CFD0680DD7FB65F352D6CC9DF9DCF5342
SHA-512:	2FA747F6AE259AF35521C0DAAD99059C3C0A726064C030579B3736C017A64C11CA015AACA2B5BBB68873418598338 31D71DDB54A402099E7FA3B8EB24A6BC56F
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 81%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d.....'.a....H.k....H.h.....H.i....}%....}5.....~.....k.....o.... .1.....j....Rich.....PE..L.H..2.[.....".....&.....t_.....@.....M.....[.....@...@.....@.....p..|....@...O.....Ll..... .....0'..@.....`.....text...O.....|..... ..`.rdata..B.....2.....@..@.data...T.....b.....@....rsrc....O...@...P...b.....@..@.relo c..t.....@..BeSkkNGPG.y...@...z...X.....PTcLNQBR^.....uhxZiqpZ.w...p...x.....bMgQsjaV.....GBMbimfi..... .....DgfAMsww.n.....p.....rSvCgsmi.....YskjstAT

\Device\ConDrv

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.107306146099542
Encrypted:	false
SSDEEP:	6:zx3M1tlAX8bSWR30qysGMQbSVRRZBXVRbJ0fFPRAgRYan:zK1XnV30ZsGMIG9BFRbQ5AUYan
MD5:	67DDD8252A246E7B14649B0063E351C0
SHA1:	AAE1C6839D1CC4A626D0FB2D4773823AD209FA17
SHA-256:	24C8283BA3F7FCA2E4CEF6F141263DD1E8A36E5A5CD96A97BFE83525D7663116
SHA-512:	326A5E0A440F60D4808C91499F1F3616C496B67DC053B4A2A40B0FE09002074AE5365018781F8746E98E7E3CFCD35F1310D17FB7C2138A8157318E6791987025
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 MSB1009: Project file does not exist...Switch: 0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.837703338237122
TrID:	• Win32 Executable (generic) a (10002005/4) 96.49% • DirectShow filter (201580/2) 1.94% • Windows ActiveX control (116523/4) 1.12% • Win32 EXE PECompact compressed (generic) (41571/9) 0.40% • Generic Win/DOS Executable (2004/3) 0.02%
File name:	Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe
File size:	4967948
MD5:	d2c96c075741ccd8bed558e39838a59d
SHA1:	09667b1bef10f69697d997a26d9d963dfe4bdeb3
SHA256:	d2a573edc893e24fbf245c4f8f918ec3b4f04fab928f073a24da3cb741d18388
SHA512:	cd882b512f98c72793b46a160feab5a7efa432a180a29f05fceabd6677d7791e9f64fa43246acd774a37439845203d0113ec1737a8e8118c9ed1ee35fb40d323
SSDEEP:	49152:RVg5tQ7aoFsGabuKxN5GmoZgZh8Jjf1SXAEaY7:fg56ddKPo2
TLSH:	5636051273F90556F2F36B31ADB191555F3ABDA99AF2D62E3240024E0976A40FE31B33
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d.....'.a.....H.k.....H.h.....H.i.....}%.....}5.....~.....k.....o.....1.....j.....Rich.....

File Icon

Icon Hash:	3f894c353f383a38

Static PE Info

General

Entrypoint:	0x425f74
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, TERMINAL_SERVER_AWARE
Time Stamp:	0x5BAE3218 [Fri Sep 28 13:52:24 2018 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	3d95adbf13bbe79dc24dccb401c12091

Entrypoint Preview

Instruction
call 00007F11D5288ACFh
jmp 00007F11D527BAE4h
int3
int3
push edi
push esi
mov esi, dword ptr [esp+10h]
mov ecx, dword ptr [esp+14h]
mov edi, dword ptr [esp+0Ch]

Instruction
mov eax, ecx
mov edx, ecx
add eax, esi
cmp edi, esi
jbe 00007F11D527BC6Ah
cmp edi, eax
jc 00007F11D527BFCEh
bt dword ptr [004C0158h], 01h
jnc 00007F11D527BC69h
rep movsb
jmp 00007F11D527BF7Ch
cmp ecx, 00000080h
jc 00007F11D527BE34h
mov eax, edi
xor eax, esi
test eax, 0000000Fh
jne 00007F11D527BC70h
bt dword ptr [004BA370h], 01h
jc 00007F11D527C140h
bt dword ptr [004C0158h], 00000000h
jnc 00007F11D527BE0Dh
test edi, 00000003h
jne 00007F11D527BE1Eh
test esi, 00000003h
jne 00007F11D527BDFDh
bt edi, 02h
jnc 00007F11D527BC6Fh
mov eax, dword ptr [esi]
sub ecx, 04h
lea esi, dword ptr [esi+04h]
mov dword ptr [edi], eax
lea edi, dword ptr [edi+04h]
bt edi, 03h
jnc 00007F11D527BC73h
movq xmm1, qword ptr [esi]
sub ecx, 08h
lea esi, dword ptr [esi+08h]
movq qword ptr [edi], xmm1
lea edi, dword ptr [edi+08h]
test esi, 00000007h
je 00007F11D527BCC5h
bt esi, 03h
jnc 00007F11D527BD18h
movdqa xmm1, dqword ptr [esi+00h]

Rich Headers

Programming Language:	• [C] VS2008 SP1 build 30729 • [IMP] VS2008 SP1 build 30729 • [ASM] VS2012 UPD4 build 61030 • [RES] VS2012 UPD4 build 61030 • [LNK] VS2012 UPD4 build 61030

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb7004	0x17c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc4000	0x54f80	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x119000	0x6c4c	.reloc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_DEBUG	0x8d8d0	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xb2730	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8d000	0x860	.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	0x8b54f	0x8b600	False	0.5699499019058296	data	6.680413749210956	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8d000	0x2cc42	0x2ce00	False	0.330464397632312	data	5.770192333189168	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xba000	0x9d54	0x6200	False	0.16402264030612246	data	2.002691099965349	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0xc4000	0x54f80	0x55000	False	0.9236299402573529	data	7.805489545240979	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x119000	0xa474	0xa600	False	0.5017884036144579	data	5.245426654116355	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
eSkkNGPG	0x124000	0x79ad	0x7a00	False	0.35098616803278687	data	4.535518130136907	
PTcLNQBR	0x12c000	0xaf5e	0xb000	False	0.43363813920454547	data	5.356692905431131	
uhxZiqpZ	0x137000	0x778b	0x7800	False	0.3194986979166667	data	4.3334565362895985	
bMgQsjaV	0x13f000	0x3fc8f	0x3fe00	False	0.24984711350293543	data	4.05145736763233	
GBMbimfi	0x17f000	0xa719	0xa800	False	0.4670293898809524	data	5.242631553298864	
DgfAMsww	0x18a000	0x16e17	0x17000	False	0.29977284307065216	data	4.933275518369312	
rSvCgsmi	0x1a1000	0xec4	0x1000	False	0.44287109375	data	5.224668348563421	
YskjstAT	0x1a2000	0xc35e	0xc400	False	0.4137436224489796	data	4.976696158252635	
LoVCKuYF	0x1af000	0x13567	0x13600	False	0.3956023185483871	data	4.838724782349081	
WVocwQqb	0x1c3000	0x2da88	0x2dc00	False	0.26286074112021857	data	4.978337116946978	
oSCGvaQZ	0x1f1000	0x1a95	0x1c00	False	0.22140066964285715	data	2.893264792435353	
yZjSVOZX	0x1f3000	0xeaa	0x1000	False	0.4404296875	data	5.471251398155905	
QXbsjhZl	0x1f4000	0x56ab	0x5800	False	0.3450372869318182	data	4.563138313410933	
yyMCijkk	0x1fa000	0x240a	0x2600	False	0.3959703947368421	data	5.108896911843352	
mpFeMMWO	0x1fd000	0x3983	0x3a00	False	0.20480872844827586	SysEx File -	4.340130743432657	
lykrKTJc	0x201000	0x6364	0x6400	False	0.2933984375	data	4.674033826538105	
uiehlGyj	0x208000	0x27a	0x400	False	0.310546875	data	2.456558757278845	
zVFOZMAw	0x209000	0x601d5	0x60200	False	0.29784521293888166	data	5.856604686192216	
YlpJAimU	0x26a000	0x5ab5	0x5c00	False	0.35597826086956524	data	5.271103031571286	
JwzqdXdu	0x270000	0x14bf0	0x14c00	False	0.3460913968373494	data	4.477563975249695	
UGiiFcPP	0x285000	0x7aa4	0x7c00	False	0.3504284274193548	data	4.508458694566567	
WQbVwRsn	0x28d000	0x14b8e	0x14c00	False	0.16732163027108435	data	3.70717026919471	
tPcESPxm	0x2a2000	0xadc5	0xae00	False	0.38873922413793105	data	4.905327698141381	
aJkBpZiD	0x2ad000	0x6b65	0x6c00	False	0.3318504050925926	data	4.392601916452199	
oVRlQlUl	0x2b4000	0x6fc2	0x7000	False	0.33461216517857145	data	4.387432855547406	
kJDrTOOv	0x2bb000	0x83ee	0x8400	False	0.32359730113636365	data	4.337865742001504	
dPNhZlJs	0x2c4000	0x5564	0x5600	False	0.32980559593023256	data	4.4462925278137835	
tpgvdaSU	0x2ca000	0xaa2d	0xac00	False	0.395008175872093	data	5.184872625976529	
stGTwKsk	0x2d5000	0x1a5	0x200	False	0.46484375	data	3.5685468265164313	
NWtntEHY	0x2d6000	0x3b29	0x3c00	False	0.3858723958333333	data	4.867479033195617	
SeCKBtus	0x2da000	0x3549	0x3600	False	0.5189525462962963	data	5.681334906237916	

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
YLnRofwZ	0x2de000	0x1d076	0x1d200	False	0.33267670332618027	data	4.731011954937073	
ITINviCX	0x2fc000	0x1fd3	0x2000	False	0.414794921875	data	5.360679897144668	
xXKSfIFI	0x2fe000	0xa5fb	0xa600	False	0.39780214608433734	data	5.050269524194634	
rzHoctSy	0x309000	0x1010	0x1200	False	0.4262152777777778	data	5.038816754642175	
tqGkaUrY	0x30b000	0x618f	0x6200	False	0.32067123724489793	DIY-Thermocam raw data (Lepton 2.x), scale 25973-29230, spot sensor temperature 44652775269962177880321 59318016.000000, unit celsius, color scheme 0, calibration: offset 144115188075855872.000000, slope 17884532710627128377344.000000	4.335120538803027	
XUULAqjj	0x312000	0x37ff	0x3800	False	0.4321986607142857	data	5.362762787611382	
OJKanVIF	0x316000	0x21634	0x21800	False	0.30387855643656714	data	4.277314480562102	
XOKAQdyM	0x338000	0x1864d	0x18800	False	0.3765345982142857	data	5.080509846456985	
bvHwouBZ	0x351000	0xa2b0	0xa400	False	0.2437595274390244	data	4.199028080121188	
emfUrPdE	0x35c000	0xe7e3	0xe800	False	0.40808526400862066	data	5.094889583938427	
wDjKtsMK	0x36b000	0x35eaa	0x36000	False	0.19294795283564814	data	3.3645037945584124	
mVRJZCIE	0x3a1000	0xecf3	0xee00	False	0.40045627626050423	data	4.849352362005015	
tOofDbnU	0x3b0000	0xa892	0xaa00	False	0.4192325367647059	data	4.961370398375378	
jMZzwYXU	0x3bb000	0x4cf7	0x4e00	False	0.49368990384615385	data	5.31897065544915	
nBeILfXx	0x3c0000	0x9372	0x9400	False	0.3332717483108108	data	4.3261187170092255	
vXOljvTV	0x3ca000	0x35cb	0x3600	False	0.6312210648148148	data	6.633589844178363	
HdeHlMsv	0x3ce000	0x89bc	0x8a00	False	0.3580446105072464	data	4.550960204952043	
INgZfirH	0x3d7000	0xe593	0xe600	False	0.32138247282608695	data	4.937237493219116	
kDTxXhPW	0x3e6000	0x143	0x200	False	0.388671875	data	2.309414250359407	
WGoHkNIX	0x3e7000	0xf27	0x1000	False	0.4541015625	data	5.223482856241876	
KQZwnOJl	0x3e8000	0xd7fc	0xd800	False	0.46073857060185186	DIY-Thermocam raw data (Lepton 3.x), scale 11520-12544, spot sensor temperature 0.000000, unit celsius, color scheme 0, calibration: offset 1475739525896764129280.000000, slope 97044631222971209141452 80.000000	5.127740862936039	
TIucAObT	0x3f6000	0x6cd5	0x6e00	False	0.4237926136363636	data	5.240262688404368	
LbFXKCFw	0x3fd000	0xc78b	0xc800	False	0.37185546875	data	4.6714439388315085	
zVPYqkoM	0x40a000	0xb156	0xb200	False	0.39786692415730335	data	5.027793035702181	
FueMosXg	0x416000	0x4c2a	0x4e00	False	0.3350360576923077	data	4.519752982476082	
iRDivbUE	0x41b000	0xc1e	0xe00	False	0.4263392857142857	data	5.114047767058862	
qqDFgVrq	0x41c000	0x56ee	0x5800	False	0.21666370738636365	data	3.357912782144656	
NoZwckKd	0x422000	0xb466	0xb600	False	0.35561899038461536	data	4.609491392908207	
xegiIWpk	0x42e000	0x3b1	0x400	False	0.466796875	data	3.5123040032137434	
lFLuySNA	0x42f000	0x9c9c	0x9e00	False	0.41836431962025317	data	4.809466543354873	
yfUTtHPf	0x439000	0x7dc	0x800	False	0.39599609375	data	4.148816820068358	
HFrlIBYb	0x43a000	0x11bd	0x1200	False	0.4587673611111111	data	5.275938366031744	
NCFRXIWT	0x43c000	0x2038	0x2200	False	0.30652573529411764	data	3.70753335612539	
DOngBUEn	0x43f000	0x921b4	0x92200	False	0.28899734014114625	data	5.578060697455509	
XkEBteUo	0x4d2000	0x511e	0x5200	False	0.3346512957317073	data	4.507233992378509	
JfnpBUQQ	0x4d8000	0x1677	0x1800	False	0.3590494791666667	data	3.8394132116328463	

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xc4590	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 192	English	Great Britain
RT_ICON	0xc46b8	0x668	Device independent bitmap graphic, 48 x 96 x 4, image size 1152	English	Great Britain
RT_ICON	0xc4d20	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 512	English	Great Britain
RT_ICON	0xc5008	0x1e8	Device independent bitmap graphic, 24 x 48 x 4, image size 288	English	Great Britain

Name	RVA	Size	Type	Language	Country
RT_ICON	0xc51f0	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 128	English	Great Britain
RT_ICON	0xc5318	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	English	Great Britain
RT_ICON	0xc61c0	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	English	Great Britain
RT_ICON	0xc6a68	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 576, 256 important colors	English	Great Britain
RT_ICON	0xc7130	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	English	Great Britain
RT_ICON	0xc7698	0xabb6	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	Great Britain
RT_ICON	0xd2250	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	Great Britain
RT_ICON	0xd47f8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	Great Britain
RT_ICON	0xd58a0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400	English	Great Britain
RT_ICON	0xd6228	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	Great Britain
RT_STRING	0xd6690	0x594	data	English	Great Britain
RT_STRING	0xd6c24	0x68a	data	English	Great Britain
RT_STRING	0xd72b0	0x490	data	English	Great Britain
RT_STRING	0xd7740	0x5fc	data	English	Great Britain
RT_STRING	0xd7d3c	0x65c	data	English	Great Britain
RT_STRING	0xd8398	0x466	data	English	Great Britain
RT_STRING	0xd8800	0x158	Matlab v4 mat-file (little endian) n, numeric, rows 0, columns 0	English	Great Britain
RT_RCDATA	0xd8958	0x400cb	data		
RT_GROUP_ICON	0x118a24	0xbc	data	English	Great Britain
RT_GROUP_ICON	0x118ae0	0x14	data	English	Great Britain
RT_VERSION	0x118af4	0xdc	data	English	Great Britain
RT_MANIFEST	0x118bd0	0x3b0	ASCII text, with CRLF line terminators	English	Great Britain

Imports

DLL	Import
WSOCK32.dll	__WSAFDIsSet, recv, send, setsockopt, ntohs, recvfrom, select, WSAStartup, htons, accept, listen, bind, closesocket, connect, WSACleanup, ioctlsocket, sendto, WSAGetLastError, inet_addr, gethostbyname, gethostname, socket
VERSION.dll	GetFileVersionInfoW, VerQueryValueW, GetFileVersionInfoSizeW
WINMM.dll	timeGetTime, waveOutSetVolume, mciSendStringW
COMCTL32.dll	ImageList_Destroy, ImageList_Remove, ImageList_SetDragCursorImage, ImageList_BeginDrag, ImageList_DragEnter, ImageList_DragLeave, ImageList_EndDrag, ImageList_DragMove, ImageList_Create, InitCommonControlsEx, ImageList_ReplaceIcon
MPR.dll	WNetUseConnectionW, WNetCancelConnection2W, WNetGetConnectionW, WNetAddConnection2W
WININET.dll	InternetReadFile, InternetCloseHandle, InternetOpenW, InternetSetOptionW, InternetCrackUrlW, HttpQueryInfoW, InternetQueryOptionW, HttpOpenRequestW, HttpSendRequestW, FtpOpenFileW, FtpGetFileSize, InternetOpenUrlW, InternetConnectW, InternetQueryDataAvailable
PSAPI.DLL	GetProcessMemoryInfo
IPHLPAPI.DLL	IcmpCreateFile, IcmpCloseHandle, IcmpSendEcho
USERENV.dll	UnloadUserProfile, DestroyEnvironmentBlock, CreateEnvironmentBlock, LoadUserProfileW
UxTheme.dll	IsThemeActive

DLL	Import
KERNEL32.dll	HeapAlloc, GetProcessHeap, HeapFree, Sleep, GetCurrentThreadId, MultiByteToWideChar, MulDiv, GetVersionExW, GetSystemInfo, FreeLibrary, LoadLibraryA, GetProcAddress, SetErrorMode, GetModuleFileNameW, WideCharToMultiByte, lstrcpyW, lstrlenW, GetModuleHandleW, QueryPerformanceCounter, VirtualFreeEx, OpenProcess, VirtualAllocEx, WriteProcessMemory, ReadProcessMemory, CreateFileW, SetFilePointerEx, ReadFile, WriteFile, FlushFileBuffers, TerminateProcess, CreateToolhelp32Snapshot, Process32FirstW, Process32NextW, SetFileTime, GetFileAttributesW, FindFirstFileW, FindClose, GetLongPathNameW, GetCurrentThread, FindNextFileW, MoveFileW, CopyFileW, CreateDirectoryW, RemoveDirectoryW, SetSystemPowerState, QueryPerformanceFrequency, FindResourceW, LoadResource, LockResource, SizeofResource, EnumResourceNamesW, OutputDebugStringW, GetTempPathW, GetTempFileNameW, DeviceIoControl, GetLocalTime, CompareStringW, DeleteCriticalSection, WaitForSingleObject, LeaveCriticalSection, GetStdHandle, CreatePipe, InterlockedExchange, TerminateThread, LoadLibraryExW, FindResourceExW, VirtualFree, FormatMessageW, GetExitCodeProcess, GetPrivateProfileStringW, WritePrivateProfileStringW, GetPrivateProfileSectionW, WritePrivateProfileSectionW, GetPrivateProfileSectionNamesW, FileTimeToLocalFileTime, FileTimeToSystemTime, SystemTimeToFileTime, LocalFileTimeToFileTime, GetDriveTypeW, GetDiskFreeSpaceExW, GetDiskFreeSpaceW, GetVolumeInformationW, SetVolumeLabelW, CreateHardLinkW, SetFileAttributesW, GetShortPathNameW, CreateEventW, SetEvent, GetEnvironmentVariableW, SetEnvironmentVariableW, GlobalLock, GlobalUnlock, GlobalAlloc, GetFileSize, GlobalFree, GlobalMemoryStatusEx, Beep, GetSystemDirectoryW, GetComputerNameW, GetWindowsDirectoryW, GetCurrentProcessId, GetProcessIoCounters, CreateProcessW, SetPriorityClass, LoadLibraryW, VirtualAlloc, CloseHandle, GetLastError, GetFullPathNameW, SetCurrentDirectoryW, IsDebuggerPresent, GetCurrentDirectoryW, lstrcmpiW, RaiseException, InitializeCriticalSectionAndSpinCount, InterlockedDecrement, InterlockedIncrement, CreateThread, DuplicateHandle, EnterCriticalSection, GetCurrentProcess, ExitProcess, GetModuleHandleExW, ExitThread, GetSystemTimeAsFileTime, ResumeThread, GetCommandLineW, IsProcessorFeaturePresent, HeapSize, IsValidCodePage, GetACP, GetOEMCP, GetCPInfo, SetLastError, UnhandledExceptionFilter, SetUnhandledExceptionFilter, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, GetStartupInfoW, GetStringTypeW, SetStdHandle, GetFileType, GetConsoleCP, GetConsoleMode, RtlUnwind, ReadConsoleW, SetFilePointer, GetTimeZoneInformation, GetDateFormatW, GetTimeFormatW, LCMapStringW, GetEnvironmentStringsW, FreeEnvironmentStringsW, HeapReAlloc, WriteConsoleW, SetEndOfFile, DeleteFileW, SetEnvironmentVariableA
USER32.dll	SetWindowPos, GetCursorInfo, RegisterHotKey, ClientToScreen, GetKeyboardLayoutNameW, IsCharAlphaW, IsCharAlphaNumericW, IsCharLowerW, IsCharUpperW, GetMenuStringW, GetSubMenu, GetCaretPos, IsZoomed, MonitorFromPoint, GetMonitorInfoW, SetWindowLongW, SetLayeredWindowAttributes, FlashWindow, GetClassLongW, TranslateAcceleratorW, IsDialogMessageW, GetSysColor, InflateRect, DrawFocusRect, DrawTextW, FrameRect, DrawFrameControl, FillRect, PtInRect, DestroyAcceleratorTable, CreateAcceleratorTableW, SetCursor, GetWindowDC, GetSystemMetrics, DrawMenuBar, GetActiveWindow, CharNextW, wsprintfW, RedrawWindow, DestroyMenu, SetMenu, GetWindowTextLengthW, CreateMenu, IsDlgButtonChecked, DefDlgProcW, CallWindowProcW, ReleaseCapture, SetCapture, MonitorFromRect, LoadImageW, CreateIconFromResourceEx, mouse_event, ExitWindowsEx, SetActiveWindow, FindWindowExW, EnumThreadWindows, SetMenuDefaultItem, InsertMenuItemW, IsMenu, TrackPopupMenuEx, GetCursorPos, CopyImage, CheckMenuRadioItem, GetMenuItemID, GetMenuItemCount, SetMenuItemInfoW, GetMenuItemInfoW, SetForegroundWindow, IsIconic, FindWindowW, UnregisterHotKey, keybd_event, SendInput, GetAsyncKeyState, SetKeyboardState, GetKeyboardState, GetKeyState, VkKeyScanW, LoadStringW, DialogBoxParamW, MessageBeep, EndDialog, SendDlgItemMessageW, GetDlgItem, SetWindowTextW, CopyRect, ReleaseDC, GetDC, EndPaint, BeginPaint, GetClientRect, GetMenu, DestroyWindow, EnumWindows, GetDesktopWindow, IsWindow, IsWindowEnabled, IsWindowVisible, EnableWindow, InvalidateRect, GetWindowLongW, GetWindowThreadProcessId, AttachThreadInput, GetFocus, ScreenToClient, SendMessageTimeoutW, EnumChildWindows, CharUpperBuffW, GetClassNameW, GetParent, GetDlgCtrlID, SendMessageW, MapVirtualKeyW, PostMessageW, GetWindowRect, SetUserObjectSecurity, CloseDesktop, CloseWindowStation, OpenDesktopW, SetProcessWindowStation, GetProcessWindowStation, OpenWindowStationW, GetUserObjectSecurity, AdjustWindowRectEx, SetRect, SetClipboardData, EmptyClipboard, CountClipboardFormats, CloseClipboard, GetClipboardData, IsClipboardFormatAvailable, OpenClipboard, BlockInput, GetMessageW, LockWindowUpdate, DispatchMessageW, TranslateMessage, DeleteMenu, PeekMessageW, MessageBoxW, DefWindowProcW, MoveWindow, SetFocus, PostQuitMessage, KillTimer, CreatePopupMenu, RegisterWindowMessageW, SetTimer, ShowWindow, CreateWindowExW, RegisterClassExW, LoadIconW, LoadCursorW, GetSysColorBrush, GetForegroundWindow, MessageBoxA, DestroyIcon, SystemParametersInfoW, CharLowerBuffW, GetWindowTextW
GDI32.dll	SetPixel, DeleteObject, GetTextExtentPoint32W, ExtCreatePen, StrokeAndFillPath, StrokePath, GetDeviceCaps, CloseFigure, LineTo, AngleArc, CreateCompatibleBitmap, CreateCompatibleDC, MoveToEx, Ellipse, PolyDraw, BeginPath, SelectObject, StretchBlt, GetDIBits, DeleteDC, GetPixel, CreateDCW, GetStockObject, Rectangle, SetViewportOrgEx, GetObjectW, SetBkMode, RoundRect, SetBkColor, CreatePen, CreateSolidBrush, SetTextColor, CreateFontW, GetTextFaceW, EndPath
COMDLG32.dll	GetSaveFileNameW, GetOpenFileNameW
ADVAPI32.dll	GetAclInformation, RegEnumValueW, RegDeleteValueW, RegDeleteKeyW, RegEnumKeyExW, RegSetValueExW, RegCreateKeyExW, GetUserNameW, RegOpenKeyExW, RegCloseKey, RegQueryValueExW, RegConnectRegistryW, InitializeSecurityDescriptor, InitializeAcl, AdjustTokenPrivileges, OpenThreadToken, OpenProcessToken, LookupPrivilegeValueW, DuplicateTokenEx, CreateProcessAsUserW, CreateProcessWithLogonW, GetLengthSid, CopySid, InitiateSystemShutdownExW, LogonUserW, AllocateAndInitializeSid, CheckTokenMembership, FreeSid, GetTokenInformation, GetSecurityDescriptorDacl, SetSecurityDescriptorDacl, AddAce, GetAce
SHELL32.dll	DragQueryPoint, ShellExecuteExW, DragQueryFileW, SHEmptyRecycleBinW, SHGetPathFromIDListW, SHBrowseForFolderW, SHCreateShellItem, SHGetDesktopFolder, SHGetSpecialFolderLocation, SHGetFolderPathW, SHFileOperationW, ExtractIconExW, Shell_NotifyIconW, ShellExecuteW, DragFinish
ole32.dll	CoTaskMemAlloc, CoTaskMemFree, CLSIDFromString, ProgIDFromCLSID, CLSIDFromProgID, OleSetMenuDescriptor, MkParseDisplayName, OleSetContainedObject, CoCreateInstance, IIDFromString, StringFromGUID2, CreateStreamOnHGlobal, CoInitialize, CoUninitialize, GetRunningObjectTable, CoGetInstanceFromFile, CoGetObject, CoInitializeSecurity, CoCreateInstanceEx, CoSetProxyBlanket
OLEAUT32.dll	RegisterTypeLib, LoadTypeLibEx, VariantCopyInd, SysReAllocString, SysFreeString, SafeArrayDestroyDescriptor, SafeArrayDestroyData, SafeArrayUnaccessData, SafeArrayAccessData, SafeArrayAllocData, UnRegisterTypeLib, SafeArrayCreateVector, SysAllocString, SysStringLen, VariantTimeToSystemTime, VarR8FromDec, SafeArrayGetVartype, OleLoadPicture, QueryPathOfRegTypeLib, VariantCopy, VariantClear, CreateDispTypeInfo, CreateStdDispatch, DispCallFunc, VariantChangeType, SafeArrayAllocDescriptorEx, VariantInit

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	Great Britain	

Network Behavior

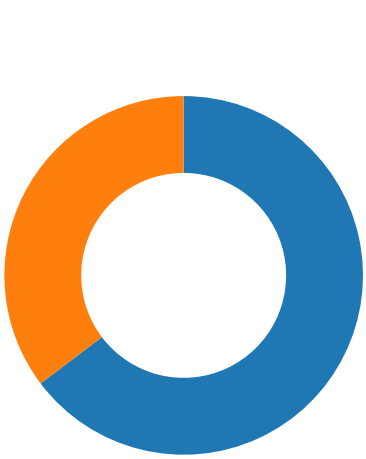
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3192.169.69.26 4971118962025019 06/04/23-11:28:18.475887	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49711	1896	192.168.2.3	192.169.69.26
192.168.2.3192.169.69.26 4971718962025019 06/04/23-11:28:50.523433	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49717	1896	192.168.2.3	192.169.69.26
192.168.2.3192.169.69.26 4970718962025019 06/04/23-11:27:57.173727	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49707	1896	192.168.2.3	192.169.69.26
192.168.2.3192.169.69.26 4971218962025019 06/04/23-11:28:23.420896	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49712	1896	192.168.2.3	192.169.69.26
192.168.2.3192.169.69.26 4971318962025019 06/04/23-11:28:28.432846	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49713	1896	192.168.2.3	192.169.69.26
192.168.2.3192.169.69.26 4971918962025019 06/04/23-11:29:00.977409	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49719	1896	192.168.2.3	192.169.69.26
192.168.2.3192.169.69.26 4971818962025019 06/04/23-11:28:55.916794	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49718	1896	192.168.2.3	192.169.69.26
192.168.2.3192.169.69.26 4970518962025019 06/04/23-11:27:45.907549	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49705	1896	192.168.2.3	192.169.69.26
192.168.2.3192.169.69.26 4969918962025019 06/04/23-11:27:14.981963	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49699	1896	192.168.2.3	192.169.69.26
192.168.2.3192.169.69.26 4970618962025019 06/04/23-11:27:50.915043	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49706	1896	192.168.2.3	192.169.69.26
192.168.2.3192.169.69.26 4970118962025019 06/04/23-11:27:25.413836	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49701	1896	192.168.2.3	192.169.69.26
192.168.2.3192.169.69.26 4970018962025019 06/04/23-11:27:20.405611	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49700	1896	192.168.2.3	192.169.69.26

Network Port Distribution

Total Packets: 34

- 53 (DNS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 4, 2023 11:27:00.324069023 CEST	49693	443	192.168.2.3	23.0.174.88
Jun 4, 2023 11:27:00.324297905 CEST	49693	443	192.168.2.3	23.0.174.88
Jun 4, 2023 11:27:00.324374914 CEST	49693	443	192.168.2.3	23.0.174.88
Jun 4, 2023 11:27:00.324446917 CEST	49693	443	192.168.2.3	23.0.174.88
Jun 4, 2023 11:27:00.324493885 CEST	49693	443	192.168.2.3	23.0.174.88
Jun 4, 2023 11:27:00.324533939 CEST	49693	443	192.168.2.3	23.0.174.88
Jun 4, 2023 11:27:00.335150003 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.335196972 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.335339069 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.335508108 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.335681915 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.335861921 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.336209059 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.336437941 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.336488008 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.336636066 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.336671114 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.336865902 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.336981058 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.337177038 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.337305069 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.337481022 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.337692976 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.337846041 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.337924004 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.338171959 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.338228941 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.338363886 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.338484049 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.338557005 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.338663101 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.338768005 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.351888895 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.351933956 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.351989031 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.352036953 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.352076054 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.352104902 CEST	49693	443	192.168.2.3	23.0.174.88
Jun 4, 2023 11:27:00.352109909 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.352188110 CEST	49693	443	192.168.2.3	23.0.174.88
Jun 4, 2023 11:27:00.352188110 CEST	49693	443	192.168.2.3	23.0.174.88

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 4, 2023 11:27:00.352353096 CEST	49693	443	192.168.2.3	23.0.174.88
Jun 4, 2023 11:27:00.352416039 CEST	49693	443	192.168.2.3	23.0.174.88
Jun 4, 2023 11:27:00.352447987 CEST	49693	443	192.168.2.3	23.0.174.88
Jun 4, 2023 11:27:00.363018990 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.363064051 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.363219023 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.363254070 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.363403082 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.363518000 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.363564968 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.363723993 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.363903999 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.363944054 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.363975048 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.364007950 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.364041090 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.364073992 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.364099979 CEST	49693	443	192.168.2.3	23.0.174.88
Jun 4, 2023 11:27:00.364104986 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.364187002 CEST	49693	443	192.168.2.3	23.0.174.88
Jun 4, 2023 11:27:00.364187002 CEST	49693	443	192.168.2.3	23.0.174.88
Jun 4, 2023 11:27:00.461503029 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.461559057 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:00.461791992 CEST	49693	443	192.168.2.3	23.0.174.88
Jun 4, 2023 11:27:14.639772892 CEST	49699	1896	192.168.2.3	192.169.69.26
Jun 4, 2023 11:27:14.913640022 CEST	1896	49699	192.169.69.26	192.168.2.3
Jun 4, 2023 11:27:14.914050102 CEST	49699	1896	192.168.2.3	192.169.69.26
Jun 4, 2023 11:27:14.981962919 CEST	49699	1896	192.168.2.3	192.169.69.26
Jun 4, 2023 11:27:15.416867018 CEST	1896	49699	192.169.69.26	192.168.2.3
Jun 4, 2023 11:27:19.842092991 CEST	49700	1896	192.168.2.3	192.169.69.26
Jun 4, 2023 11:27:20.402514935 CEST	49693	443	192.168.2.3	23.0.174.88
Jun 4, 2023 11:27:20.402683020 CEST	49693	443	192.168.2.3	23.0.174.88
Jun 4, 2023 11:27:20.402740002 CEST	49693	443	192.168.2.3	23.0.174.88
Jun 4, 2023 11:27:20.402806044 CEST	49693	443	192.168.2.3	23.0.174.88
Jun 4, 2023 11:27:20.402849913 CEST	49693	443	192.168.2.3	23.0.174.88
Jun 4, 2023 11:27:20.402873993 CEST	49693	443	192.168.2.3	23.0.174.88
Jun 4, 2023 11:27:20.405004978 CEST	1896	49700	192.169.69.26	192.168.2.3
Jun 4, 2023 11:27:20.405138016 CEST	49700	1896	192.168.2.3	192.169.69.26
Jun 4, 2023 11:27:20.405611038 CEST	49700	1896	192.168.2.3	192.169.69.26
Jun 4, 2023 11:27:20.413551092 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:20.413616896 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:20.413661957 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:20.413703918 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:20.413747072 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:20.413851976 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:20.413966894 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:20.414011955 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:20.414129019 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:20.414172888 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:20.414285898 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:20.414411068 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:20.414608955 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:20.414654016 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:20.414855957 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:20.414886951 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:20.414913893 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:20.415009022 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:20.415081024 CEST	443	49693	23.0.174.88	192.168.2.3
Jun 4, 2023 11:27:20.415213108 CEST	443	49693	23.0.174.88	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jun 4, 2023 11:27:14.502774954 CEST	52387	53	192.168.2.3	8.8.8.8
Jun 4, 2023 11:27:14.624871969 CEST	53	52387	8.8.8.8	192.168.2.3
Jun 4, 2023 11:27:19.818093061 CEST	56924	53	192.168.2.3	8.8.8.8
Jun 4, 2023 11:27:19.838557959 CEST	53	56924	8.8.8.8	192.168.2.3
Jun 4, 2023 11:27:24.938667059 CEST	60625	53	192.168.2.3	8.8.8.8
Jun 4, 2023 11:27:25.060234070 CEST	53	60625	8.8.8.8	192.168.2.3
Jun 4, 2023 11:27:45.224785089 CEST	49302	53	192.168.2.3	8.8.8.8
Jun 4, 2023 11:27:45.338428020 CEST	53	49302	8.8.8.8	192.168.2.3
Jun 4, 2023 11:27:50.444329977 CEST	53975	53	192.168.2.3	8.8.8.8
Jun 4, 2023 11:27:50.467924118 CEST	53	53975	8.8.8.8	192.168.2.3
Jun 4, 2023 11:27:55.807750940 CEST	51139	53	192.168.2.3	8.8.8.8
Jun 4, 2023 11:27:55.828227997 CEST	53	51139	8.8.8.8	192.168.2.3
Jun 4, 2023 11:28:17.666209936 CEST	52955	53	192.168.2.3	8.8.8.8
Jun 4, 2023 11:28:17.780860901 CEST	53	52955	8.8.8.8	192.168.2.3
Jun 4, 2023 11:28:22.939152956 CEST	60582	53	192.168.2.3	8.8.8.8
Jun 4, 2023 11:28:23.062289953 CEST	53	60582	8.8.8.8	192.168.2.3
Jun 4, 2023 11:28:27.976121902 CEST	57134	53	192.168.2.3	8.8.8.8
Jun 4, 2023 11:28:28.098058939 CEST	53	57134	8.8.8.8	192.168.2.3
Jun 4, 2023 11:28:49.655924082 CEST	62050	53	192.168.2.3	8.8.8.8
Jun 4, 2023 11:28:49.769670963 CEST	53	62050	8.8.8.8	192.168.2.3
Jun 4, 2023 11:28:55.252490044 CEST	56042	53	192.168.2.3	8.8.8.8
Jun 4, 2023 11:28:55.282026052 CEST	53	56042	8.8.8.8	192.168.2.3
Jun 4, 2023 11:29:00.458888054 CEST	59636	53	192.168.2.3	8.8.8.8
Jun 4, 2023 11:29:00.487466097 CEST	53	59636	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Jun 4, 2023 11:27:14.502774954 CEST	192.168.2.3	8.8.8.8	0x32de	Standard query (0)	nickdns22.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 11:27:19.818093061 CEST	192.168.2.3	8.8.8.8	0xa211	Standard query (0)	nickdns22.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 11:27:24.938667059 CEST	192.168.2.3	8.8.8.8	0xcb5	Standard query (0)	nickdns22.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 11:27:45.224785089 CEST	192.168.2.3	8.8.8.8	0x72a6	Standard query (0)	nickdns22.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 11:27:50.444329977 CEST	192.168.2.3	8.8.8.8	0x722d	Standard query (0)	nickdns22.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 11:27:55.807750940 CEST	192.168.2.3	8.8.8.8	0xc7c8	Standard query (0)	nickdns22.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 11:28:17.666209936 CEST	192.168.2.3	8.8.8.8	0x325a	Standard query (0)	nickdns22.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 11:28:22.939152956 CEST	192.168.2.3	8.8.8.8	0x6307	Standard query (0)	nickdns22.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 11:28:27.976121902 CEST	192.168.2.3	8.8.8.8	0x5504	Standard query (0)	nickdns22.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 11:28:49.655924082 CEST	192.168.2.3	8.8.8.8	0xedcf	Standard query (0)	nickdns22.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 11:28:55.252490044 CEST	192.168.2.3	8.8.8.8	0x59b1	Standard query (0)	nickdns22.duckdns.org	A (IP address)	IN (0x0001)	false
Jun 4, 2023 11:29:00.458888054 CEST	192.168.2.3	8.8.8.8	0x63f6	Standard query (0)	nickdns22.duckdns.org	A (IP address)	IN (0x0001)	false

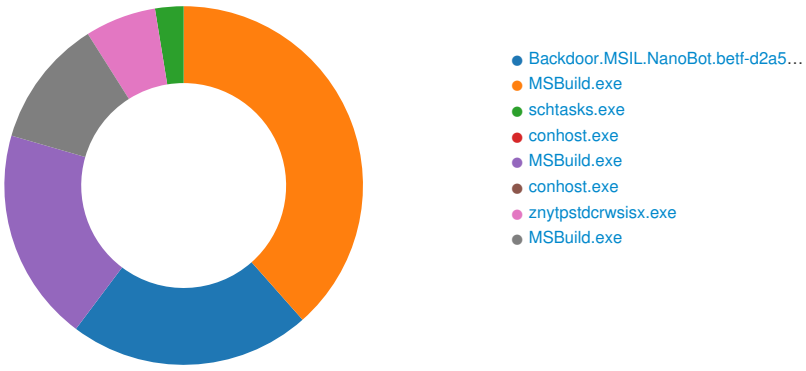
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 4, 2023 11:27:14.624871969 CEST	8.8.8.8	192.168.2.3	0x32de	No error (0)	nickdns22.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 11:27:19.838557959 CEST	8.8.8.8	192.168.2.3	0xa211	No error (0)	nickdns22.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Jun 4, 2023 11:27:25.060234070 CEST	8.8.8.8	192.168.2.3	0xcb5	No error (0)	nickdns22.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 11:27:45.338428020 CEST	8.8.8.8	192.168.2.3	0x72a6	No error (0)	nickdns22.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 11:27:50.467924118 CEST	8.8.8.8	192.168.2.3	0x722d	No error (0)	nickdns22.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 11:27:55.828227997 CEST	8.8.8.8	192.168.2.3	0xc7c8	No error (0)	nickdns22.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 11:28:17.780860901 CEST	8.8.8.8	192.168.2.3	0x325a	No error (0)	nickdns22.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 11:28:23.062289953 CEST	8.8.8.8	192.168.2.3	0x6307	No error (0)	nickdns22.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 11:28:28.098058939 CEST	8.8.8.8	192.168.2.3	0x5504	No error (0)	nickdns22.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 11:28:49.769670963 CEST	8.8.8.8	192.168.2.3	0xedcf	No error (0)	nickdns22.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 11:28:55.282026052 CEST	8.8.8.8	192.168.2.3	0x59b1	No error (0)	nickdns22.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
Jun 4, 2023 11:29:00.487466097 CEST	8.8.8.8	192.168.2.3	0x63f6	No error (0)	nickdns22.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe PID: 7044, Parent PID: 3452

General

Target ID:	0
Start time:	11:27:01
Start date:	04/06/2023
Path:	C:\Users\user\Desktop\Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe

Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe
Imagebase:	0x2d0000
File size:	4967948 bytes
MD5 hash:	D2C96C075741CCD8BED558E39838A59D
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: 00000000.00000003.383770715.00000000013B3000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.383770715.00000000013B3000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.383770715.00000000013B3000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000003.383770715.00000000013B3000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.384143061.0000000001195000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.384143061.0000000001195000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.384143061.0000000001195000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000003.384143061.0000000001195000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.382325169.0000000001197000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.382325169.0000000001197000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.382325169.0000000001197000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000003.382325169.0000000001197000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.383002021.00000000014E4000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.383002021.00000000014E4000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.383002021.00000000014E4000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000003.383002021.00000000014E4000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.382620539.0000000001428000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.382620539.0000000001428000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.382620539.0000000001428000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000003.382620539.0000000001428000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.382379627.0000000001429000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.382379627.0000000001429000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.382379627.0000000001429000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000003.382379627.0000000001429000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.383032344.0000000004FF1000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.383032344.0000000004FF1000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.383032344.0000000004FF1000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000003.383032344.0000000004FF1000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.382518683.0000000001197000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.382518683.0000000001197000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.382518683.0000000001197000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000003.382518683.0000000001197000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.387268383.0000000001196000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.387268383.0000000001196000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.387268383.0000000001196000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000003.387268383.0000000001196000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.383592412.0000000001419000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.383592412.0000000001419000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.383592412.0000000001419000.00000004.00000020.00020000.00000000.sdmp,

	Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000003.383592412.0000000001419000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.382557238.00000000013C2000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.382557238.00000000013C2000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.382557238.00000000013C2000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000003.382557238.00000000013C2000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.383733827.00000000013E6000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.383733827.00000000013E6000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.383733827.00000000013E6000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000003.383733827.00000000013E6000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.382477117.000000000145C000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.382477117.000000000145C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.382477117.000000000145C000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000003.382477117.000000000145C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.383509738.000000000144C000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.383509738.000000000144C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.383509738.000000000144C000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000003.383509738.000000000144C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\hdoydskbdx	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	31638E	CreateDirectoryW
C:\Users\user\AppData\Roaming\hdoydskbdx\znytpstdcrwsisx.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	34408F	CreateFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\znytpstdcrwsisx.fr.url	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	34408F	CreateFileW
C:\Users\user\AppData\Local\Temp\aut8DF8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	31C74C	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\cbmfpeiu	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	31C354	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\aut8DF8.tmp	success or wait	1	31C377	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\hdoydskbdx\znytpstdcrwsisx.exe	0	4967954	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 01 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 fd 64 1e fd 05 fd 79 05 fd 79 05 fd fd 27 fd 61 78 05 fd fd 48 fd 6b 4a 05 fd fd 48 fd 68 fd 17 05 fd fd 48 fd 69 4b 05 fd 70 7d 25 70 05 fd 70 7d 35 5c 05 fd 79 05 fd 6d 07 fd fd fd fd 7e fd fd 05 fd fd fd fd 6b 7b 05 fd fd fd fd 6f 78 05 fd 79 05 31 78 05 fd fd fd fd 6a 78 05 fd fd 52 69 63 68 fd 05 fd fd 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$d'aHkHhHi}%}5~ko1jRich	success or wait	1	315DFE	WriteFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\znytpstdcrwsisx.fr.url	0	93	5b 49 6e 74 65 72 6e 65 74 53 68 6f 72 74 63 75 74 5d 0d 0a 55 52 4c 3d 66 69 6c 65 3a 2f 2f 2f 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 68 64 6f 79 64 73 6b 62 64 78 5c 7a 6e 79 74 70 73 74 64 63 72 77 73 69 73 78 2e 65 78 65	[InternetShortcut]URL=file:///C:\Users\user\AppData\Roaming\hdoydskbdx\znytpstdcrwsisx.exe	success or wait	1	315DFE	WriteFile
C:\Users\user\AppData\Local\Temp\aut8DF8.tmp	0	65536	7a fd 28 2b 79 fd f4 21 fd 19 fd fd c1 fd 7f fd 3b 04 4e fd 11 fd fd 1b fd 0c 45 01 fd fd fd 17 fd fd 0a fd fd fd 1c 71 fd fd 42 fd 06 fd fd 35 fd 55 54 74 77 fd 53 66 fd fd 61 45 14 6a 11 49 78 0e 54 71 fd fd fd fd 39 fd 18 38 77 fd 50 78 41 1d fd fd 2a 18 2d 17 fd fd 78 41 26 fd 7f 27 12 fd 6d 58 fd 17 fd fd 0e fd fd fd 39 fd 4d 79 fd 1e 4d 2d fd 32 56 30 12 03 fd 05 2c 15 fd 19 4d fd fd 71 07 fd 04 fd 08 76 fd 2e fd fd 5f fd fd 54 36 37 62 35 dd 4a 62 fd 53 fd fd 51 21 51 51 05 7f 28 6e 69 fd 96 fd fd 4a fd fd 59 26 fd fd 7a 74 fd 67 6a 35 fd fd 0b 6a 48 1e db 47 fd fd 0b fd fd fd 73 00 37 17 cf 0c 30 fd fd 08 75 fd 41 4c fd fd 19 17 fd fd 24 07 fd fd 1a 59 fd fd fd 53 fd fd 13 69 fd fd 01 fd fd 57 4a 15 74 fd 3d fd	z(+!;NEqB5UTtwSfaEjlxTq98wPxA*-xA&'mX9MyM-2V0,Mqv._T67b5JbSQ!QQ(niJY&zgj5jHGs70uAL$YSiWJt=	success or wait	4	2FB7D3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\aut8DF8.tmp	204800	3072	44 fd 50 fd fd fd 39 fd fd fd fd 40 04 30 6a fd 73 1f 0a 5a 6b fd 54 3e 29 7f 20 fd fd fd fd 27 1f fd 66 fd fd fd 09 fd 42 75 fd fd fd fd fd 59 38 fd 23 10 fd 25 fd fd 4e 42 fd 5a 21 2d fd 4d 0b 33 50 0a fd 38 fd fd fd fd fd 6d fd 57 fd 0f fd fd 23 3b 09 fd 1e 16 2e fd fd fd fd fd 36 fd fd 2b fd 73 5a 3b 5f 12 1f 0f fd 3d 1a 5b 04 fd 7a fd 26 fd 16 1c fd 2b 7b 04 fd 4a 73 9b 32 b6 0a fd 40 21 fd 61 79 fd fd 6b 39 15 2b 6b 00 fd 79 68 4b fd 46 64 04 fd 3e 0d 74 fd 06 fd fd fd fd 11 fd fd fd 6a fd 8f fd fd 3b fd fd 4d 09 fd 31 fd 3f 1c fd 39 42 50 6c fd fd 21 fd 7b fd fd 0f 77 fd fd 6f 06 fd fd 56 36 12 08 fd 06 7c 75 fd fd fd fd fd 56 1b fd 4e fd 66 05 fd fd 11 fd 00 fd 40 fd 7e 4f 13 6f fd fd fd 6c 64 70 fd 38 2e fd fd	DP9@0jsZkT>) 'fBuY8#%NBZ!-M3P8 mW#;.6+sZ;_=z&+ {Js2@!ayk9+kyhK Fd>tj;M1?9BP! {woV6|uVN@~Ooldp8.	success or wait	1	2FB7D3	WriteFile
C:\Users\user\AppData\Local\Temp\cbmfpeiu	0	131072	7a fd 28 2b 79 fd f4 21 fd 19 fd fd c1 fd 7f fd 3b 04 4e fd 11 fd fd 1b fd 0c 45 01 fd fd fd 17 fd fd 0a fd fd fd 1c 71 fd fd 42 fd 06 fd fd 35 fd 55 54 74 77 fd 53 66 fd fd 61 45 14 6a 11 49 78 0e 54 71 fd fd fd fd 39 fd 18 38 77 fd 50 78 41 1d fd fd 2a 18 2d 17 fd fd 78 41 26 fd 7f 27 12 fd 6d 58 fd 17 fd fd 0e fd fd fd 39 fd 4d 79 fd 1e 4d 2d fd 32 56 30 12 03 fd 05 2c 15 fd 19 4d fd fd 71 07 fd 04 fd 08 76 fd 2e fd fd 5f fd fd 54 36 37 62 35 dd 4a 62 fd 53 fd fd 51 21 51 51 05 7f 28 6e 69 fd 96 fd fd 4a fd fd 59 26 fd fd 7a 74 fd 67 6a 35 fd fd 0b 6a 48 1e db 47 fd fd 0b fd fd fd 73 00 37 17 cf 0c 30 fd fd 08 75 fd 41 4c fd fd 19 17 fd fd 24 07 fd fd 1a 59 fd fd fd 53 fd fd 13 69 fd fd 01 fd fd 57 4a 15 74 fd 3d fd	z(+!;NEqB5UTtwSfaEjlxTq98wPxA*- xA&'mX9MyM- 2V0,Mqv._T67b5JbSQ !QQ(niJY&zgj5jHGs70uAL$YSiWJt=	success or wait	2	31C354	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe	unknown	65536	success or wait	1	2DC33D	ReadFile
C:\Users\user\Desktop\Backdoor.MSIL.NanoBot.betf-d2a573edc893e24fbf.exe	unknown	65536	success or wait	76	2DC33D	ReadFile
C:\Users\user\AppData\Roaming\hdoydskbdx\znytpstdcrwsisx.exe	unknown	65536	end of file	1	2DC33D	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\znytpstdcrwsisx.fr.url	unknown	65536	end of file	1	2DC33D	ReadFile
C:\Users\user\AppData\Local\Temp\cbmfpeiu	unknown	65536	success or wait	1	2DC33D	ReadFile
C:\Users\user\AppData\Local\Temp\cbmfpeiu	unknown	65536	success or wait	4	2DC33D	ReadFile

Analysis Process: MSBuild.exe PID: **5980**, Parent PID: **7044**

General

Target ID:	1
Start time:	11:27:11
Start date:	04/06/2023
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:	0x720000
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: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.630789913.0000000002DC1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.634788699.00000000059F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.634788699.00000000059F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.634788699.00000000059F0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.634788699.00000000059F0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.634788699.00000000059F0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.634649068.0000000005640000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.634649068.0000000005640000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000001.00000002.634649068.0000000005640000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000001.00000002.634649068.0000000005640000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
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	6C7E60AC	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	6C7E60AC	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	5020D15	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	5020E0F	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp9A5C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	50210E0	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	5020E0F	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	5020D15	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	5020D15	CreateDirectoryW

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	6C7E60AC	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	6C7E60AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp9A5C.tmp	success or wait	1	E0BF0E	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	0	8	fd fd 29 51 29 65 fd 48	)Q)eH	success or wait	1	5020FC7	WriteFile
C:\Users\user\AppData\Local\Temp\tmp9A5C.tmp	0	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	5020FC7	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	0	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	5020FC7	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	6C815544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6C815544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	6C815544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	6C815544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	6C818738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	6C818738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C818738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe	unknown	4096	success or wait	1	6C8BBF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe	unknown	512	success or wait	1	6C8BBF06	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	6C815544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	6C815544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C815544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	6C815544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5020FC7	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4096	success or wait	1	5020FC7	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4096	end of file	1	5020FC7	ReadFile

Analysis Process: schtasks.exe PID: **5916**, Parent PID: **5980**

General

Target ID:	2
Start time:	11:27:13
Start date:	04/06/2023
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\tmp9A5C.tmp
Imagebase:	0x3f0000
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\tmp9A5C.tmp	unknown	2	success or wait	1	3FAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp9A5C.tmp	unknown	1321	success or wait	1	3FABD9	ReadFile

Analysis Process: conhost.exe PID: **3676**, Parent PID: **5916**

General

Target ID:	3
Start time:	11:27:13
Start date:	04/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: MSBuild.exe PID: **5744**, Parent PID: **1080**

General	
Target ID:	4
Start time:	11:27:15
Start date:	04/06/2023
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:	0xd50000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.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	6C7E60AC	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	6C7E60AC	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	6C7D34A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	2F2A7A3	WriteFile
\Device\ConDrv	169	169	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	2F2A7A3	WriteFile
\Device\ConDrv	235	66	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	2F2A7A3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\MSBuild.exe.log	0	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",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",02,"Microsoft.Build.Engine, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",02,"Microsoft.Build.Framework,	success or wait	1	6CABA33A	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	6C815544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6C815544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	6C815544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	6C815544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	6C818738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	6C818738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C818738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.rsp	unknown	4096	success or wait	1	2F2A7A3	ReadFile

Analysis Process: conhost.exe PID: **3100**, Parent PID: **5744**

General

Target ID:	5
Start time:	11:27:15
Start date:	04/06/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: znytpstdcrwsisx.exe PID: **5292**, Parent PID: **3452**

General

Target ID:	6
Start time:	11:27:20
Start date:	04/06/2023
Path:	C:\Users\user\AppData\Roaming\hdoydskbdx\znytpstdcrwsisx.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\hdoydskbdx\znytpstdcrwsisx.exe"
Imagebase:	0xdf0000
File size:	4967954 bytes
MD5 hash:	A360B0402DD16AE837F59D09E1BF3B3C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000003.407208526.000000000175C000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000003.407208526.000000000175C000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000003.407208526.000000000175C000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000003.407208526.000000000175C000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000003.409346361.0000000001431000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000003.409346361.0000000001431000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000003.409346361.0000000001431000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000003.409346361.0000000001431000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000003.407143398.000000000178F000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000003.407143398.000000000178F000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000003.407143398.000000000178F000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000003.407143398.000000000178F000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000003.407063143.0000000004541000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000003.407063143.0000000004541000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000003.407063143.0000000004541000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000003.407063143.0000000004541000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000003.405134959.00000000016ED000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000003.405134959.00000000016ED000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000003.405134959.00000000016ED000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000003.405134959.00000000016ED000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000003.409265675.0000000001431000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000003.409265675.0000000001431000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000003.409265675.0000000001431000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000003.409265675.0000000001431000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000003.407268539.0000000001729000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000003.407268539.0000000001729000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000003.407268539.0000000001729000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000003.407268539.0000000001729000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000003.405268351.000000000172A000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000003.405268351.000000000172A000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000003.405268351.000000000172A000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000003.405268351.000000000172A000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000003.405858359.00000000016BA000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000003.405858359.00000000016BA000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000003.405858359.00000000016BA000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source:

	00000006.00000003.405858359.00000000016BA000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000003.405433292.00000000016EC000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000003.405433292.00000000016EC000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000003.405433292.00000000016EC000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000003.405433292.00000000016EC000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000003.409440308.0000000001457000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000003.409440308.0000000001457000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000003.409440308.0000000001457000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000003.409440308.0000000001457000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000003.409174074.0000000001431000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000003.409174074.0000000001431000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000003.409174074.0000000001431000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000003.409174074.0000000001431000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000003.406996996.0000000001687000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000003.406996996.0000000001687000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000003.406996996.0000000001687000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000003.406996996.0000000001687000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000003.405084980.0000000001457000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000003.405084980.0000000001457000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000003.405084980.0000000001457000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000003.405084980.0000000001457000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000003.409044743.0000000001431000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000003.409044743.0000000001431000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000003.409044743.0000000001431000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000003.409044743.0000000001431000.00000004.00000020.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000003.405355044.0000000001687000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000003.405355044.0000000001687000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000003.405355044.0000000001687000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000003.405355044.0000000001687000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 81%, ReversingLabs
Reputation:	low

File Activities

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\znytpstdcrwsisx.fr.url	93	93	5b 49 6e 74 65 72 6e 65 74 53 68 6f 72 74 63 75 74 5d 0d 0a 55 52 4c 3d 66 69 6c 65 3a 2f 2f 2f 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 68 64 6f 79 64 73 6b 62 64 78 5c 7a 6e 79 74 70 73 74 64 63 72 77 73 69 73 78 2e 65 78 65	[InternetShortcut]URL=file:///C:\Users\user\AppData\Roaming\hdoydskbdx\znytpstdcrwsisx.exe	success or wait	1	E35DFE	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\znytpstdcrwsisx.fr.url	unknown	65536	success or wait	1	DFC33D	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\znytpstdcrwsisx.fr.url	unknown	65536	end of file	1	DFC33D	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\cbmfpeiu	unknown	65536	success or wait	1	DFC33D	ReadFile
C:\Users\user\AppData\Local\Temp\cbmfpeiu	unknown	65536	success or wait	4	DFC33D	ReadFile

Analysis Process: MSBuild.exe PID: **5944**, Parent PID: **5292**

General

Target ID:	7
Start time:	11:27:22
Start date:	04/06/2023
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:	0xac0000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
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: 00000007.00000002.421398026.00000000031C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.421398026.00000000031C1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000002.421398026.00000000031C1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.420789152.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.420789152.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.420789152.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000002.420789152.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.421501770.00000000041C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.421501770.00000000041C1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000002.421501770.00000000041C1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
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	6C7E60AC	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	6C7E60AC	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	6C815544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6C815544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	6C815544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	6C815544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	4095	success or wait	1	6C818738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\msbuild.exe.config	unknown	8173	end of file	1	6C818738	ReadFile

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	6C818738	ReadFile

Disassembly

No disassembly