ID: 796775
Sample Name: 3yIxxU5Wko.exe
Cookbook: default.jbs
Time: 08:00:16
Date: 02/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

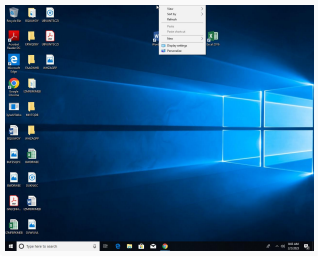
Windows Analysis Report

3yIxxU5Wko.exe

Overview

General Information

Sample Name:	3yIxxU5Wko.exe
Analysis ID:	796775
MD5:	6df2c2caaccc7…
SHA1:	419ab96d1452…
SHA256:	8ecc4898d03b…
Tags:	exe NanoCore RAT
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

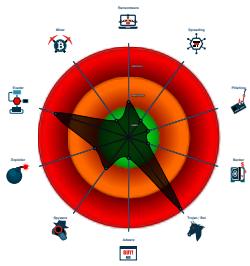
Nanocore

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Sigma detected: Scheduled temp fil…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- 3yIxxU5Wko.exe (PID: 5192 cmdline: C:\Users\user\Desktop\3yIxxU5Wko.exe MD5: 6DF2C2CAACCC7947F8439F248CDD386F)
  - 3yIxxU5Wko.exe (PID: 3232 cmdline: C:\Users\user\Desktop\3yIxxU5Wko.exe MD5: 6DF2C2CAACCC7947F8439F248CDD386F)
  - 3yIxxU5Wko.exe (PID: 5480 cmdline: C:\Users\user\Desktop\3yIxxU5Wko.exe MD5: 6DF2C2CAACCC7947F8439F248CDD386F)
    - schtasks.exe (PID: 320 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmpFB74.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 3108 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5348 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmpFD98.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 3732 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - conhost.exe (PID: 5348 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- 3yIxxU5Wko.exe (PID: 4748 cmdline: C:\Users\user\Desktop\3yIxxU5Wko.exe 0 MD5: 6DF2C2CAACCC7947F8439F248CDD386F)
  - 3yIxxU5Wko.exe (PID: 5868 cmdline: C:\Users\user\Desktop\3yIxxU5Wko.exe MD5: 6DF2C2CAACCC7947F8439F248CDD386F)
  - 3yIxxU5Wko.exe (PID: 2376 cmdline: C:\Users\user\Desktop\3yIxxU5Wko.exe MD5: 6DF2C2CAACCC7947F8439F248CDD386F)
- dhcpmon.exe (PID: 4976 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: 6DF2C2CAACCC7947F8439F248CDD386F)
  - dhcpmon.exe (PID: 1748 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 6DF2C2CAACCC7947F8439F248CDD386F)
  - dhcpmon.exe (PID: 4500 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 6DF2C2CAACCC7947F8439F248CDD386F)
- dhcpmon.exe (PID: 3424 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 6DF2C2CAACCC7947F8439F248CDD386F)
  - dhcpmon.exe (PID: 5884 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 6DF2C2CAACCC7947F8439F248CDD386F)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "be28fce4-4930-4ffe-96ed-0110cf99",
  "Group": "SecureKMT",
  "Domain1": "tzitziklishop.ddns.net",
  "Domain2": "127.0.0.1",
  "Port": 1665,
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.536518016.0000000007410000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x59eb:$x1: NanoCore.ClientPluginHost • 0x5b48:$x2: IClientNetworkHost
00000002.00000002.536518016.0000000007410000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0x59eb:$x2: NanoCore.ClientPluginHost • 0x6941:$s3: PipeExists • 0x5be1:$s4: PipeCreated • 0x5a05:$s5: IClientLoggingHost
00000002.00000002.536518016.0000000007410000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x5ad5:$x2: NanoCore.ClientPlugin • 0x59eb:$x3: NanoCore.ClientPluginHost • 0x5aeb:$i3: IClientNetwork • 0x5a24:$i5: IClientDataHost • 0x5a05:$i6: IClientLoggingHost • 0x5b48:$i7: IClientNetworkHost • 0x5a43:$i8: IClientUIHost • 0x6955:$i9: IClientNameObjectCollection • 0x54fc:$s1: ClientPlugin • 0x5ade:$s1: ClientPlugin • 0x6971:$s6: get_ClientSettings
00000002.00000002.536518016.0000000007410000.00000004.08000000.00040000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x59eb:$a1: NanoCore.ClientPluginHost • 0x5ad5:$a2: NanoCore.ClientPlugin • 0x732e:$b7: LogClientException • 0x6941:$b8: PipeExists • 0x5a05:$b9: IClientLoggingHost
00000002.00000002.532206387.00000000055F0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
Click to see the 102 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.3ylxxU5Wko.exe.73f0000.25.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x605:$x1: NanoCore.ClientPluginHost • 0x63e:$x2: IClientNetworkHost

Source	Rule	Description	Author	Strings
2.2.3yIxxU5Wko.exe.73f0000.25.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0x605:$x2: NanoCore.ClientPluginHost • 0x720:$s4: PipeCreated • 0x61f:$s5: IClientLoggingHost
2.2.3yIxxU5Wko.exe.73f0000.25.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x67f:$x2: NanoCore.ClientPlugin • 0x605:$x3: NanoCore.ClientPluginHost • 0x695:$i3: IClientNetwork • 0x61f:$i6: IClientLoggingHost • 0x63e:$i7: IClientNetworkHost • 0x688:$s1: ClientPlugin
2.2.3yIxxU5Wko.exe.73f0000.25.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x605:$a1: NanoCore.ClientPluginHost • 0x67f:$a2: NanoCore.ClientPlugin • 0xda0:$b7: LogClientException • 0x61f:$b9: IClientLoggingHost
2.2.3yIxxU5Wko.exe.76b0000.29.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x3d99:$x1: NanoCore.ClientPluginHost • 0x3db3:$x2: IClientNetworkHost
Click to see the 288 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

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

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.6 - Destination IP: 45.12.253.26 −

Timestamp:	192.168.2.645.12.253.264971816652816766 02/02/23-08:01:58.369947
SID:	2816766
Source Port:	49718
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.12.253.26 - Destination IP: 192.168.2.6 −

Timestamp:	45.12.253.26192.168.2.61665497152841753 02/02/23-08:01:51.077424
SID:	2841753
Source Port:	1665
Destination Port:	49715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.6 - Destination IP: 45.12.253.26	
Timestamp:	192.168.2.645.12.253.264971316652816766 02/02/23-08:01:29.730882
SID:	2816766
Source Port:	49713
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.6 - Destination IP: 45.12.253.26	
Timestamp:	192.168.2.645.12.253.264971416652816766 02/02/23-08:01:39.744017
SID:	2816766
Source Port:	49714
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.6 - Destination IP: 45.12.253.26	
Timestamp:	192.168.2.645.12.253.264971516652816766 02/02/23-08:01:51.165371
SID:	2816766
Source Port:	49715
Destination Port:	1665
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 45.12.253.26 - Destination IP: 192.168.2.6	
Timestamp:	45.12.253.26192.168.2.61665497182810290 02/02/23-08:01:58.690998
SID:	2810290
Source Port:	1665
Destination Port:	49718
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.12.253.26 - Destination IP: 192.168.2.6	
Timestamp:	45.12.253.26192.168.2.61665497182841753 02/02/23-08:01:58.903710
SID:	2841753
Source Port:	1665
Destination Port:	49718
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

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

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

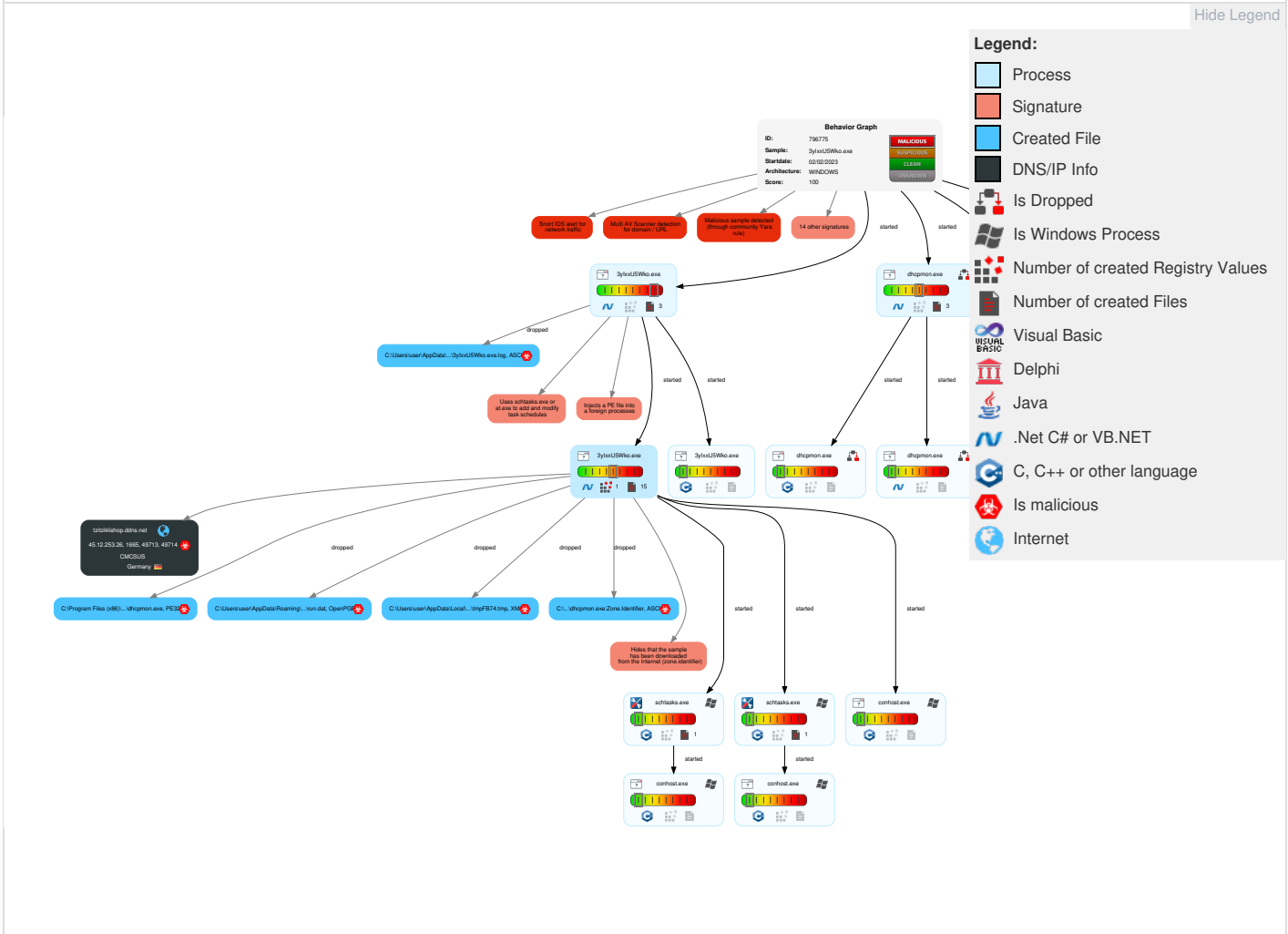
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	1 Scheduled Task/Job	1 1 2 Process Injection	2 Masquerading	1 1 Input Capture	2 1 1 Security Software Discovery	Remote Services	1 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 2 Process Injection	NTDS	1 Application Window Discovery	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	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 2 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	2 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	System Owner/User 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	3 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 3 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

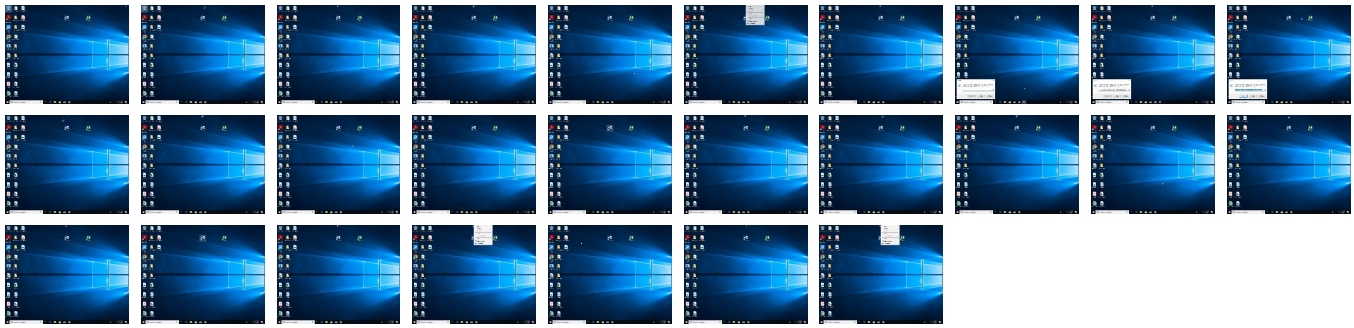
Behavior Graph



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
3ylxxU5Wko.exe	28%	ReversingLabs	Win32.Trojan.Pwsx	

Source	Detection	Scanner	Label	Link
3yIxxU5Wko.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	28%	ReversingLabs	Win32.Trojan.Pwsx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.3yIxxU5Wko.exe.64a0000.20.unpack	100%	Avira	TR/NanoCore.fadte		Download File
18.2.3yIxxU5Wko.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
tzitziklishop.ddns.net	12%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/L	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.tiro.comB	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/8	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/5	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/5	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/c	0%	URL Reputation	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.fontbureau.comldv	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.coma	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.comR.TTF	0%	URL Reputation	safe	
http://www.fontbureau.comalsd	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Q	0%	URL Reputation	safe	
tzitziklishop.ddns.net	100%	Avira URL Cloud	malware	
http://www.sajatypeworks.comeY	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.comd5	0%	Avira URL Cloud	safe	
http://www.fontbureau.comFG	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/y/	0%	Avira URL Cloud	safe	
http://www.tiro.comT=	0%	Avira URL Cloud	safe	
tzitziklishop.ddns.net	12%	Virustotal		Browse
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.tiro.coml	0%	URL Reputation	safe	
http://www.fontbureau.comac	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htme	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/keb	0%	Avira URL Cloud	safe	
127.0.0.1	0%	Avira URL Cloud	safe	
http://www.fontbureau.comttodh	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y00	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
tzitziklishop.ddns.net	45.12.253.26	true	true	• 12%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
tzitziklishop.ddns.net	true	• 12%, Virustotal, Browse • Avira URL Cloud: malware	unknown
127.0.0.1	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comd5	3yIxxU5Wko.exe, 00000000.00000003.248154930.000000000610B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	3yIxxU5Wko.exe, 00000000.00000002.280901191.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	3yIxxU5Wko.exe, 00000000.00000002.280901191.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	3yIxxU5Wko.exe, 00000000.00000002.280901191.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	3yIxxU5Wko.exe, 00000000.00000002.280901191.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/L	3ylxxU5Wko.exe, 00000000.00000003.247230845.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246594659.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.247301851.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.247048926.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.247202053.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246548104.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246957227.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246297960.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246881598.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.247102368.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246931816.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.247027959.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246804982.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.247272353.000000000610B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comFG	3ylxxU5Wko.exe, 00000000.00000003.248154930.000000000610B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	3ylxxU5Wko.exe, 00000000.00000002.280901191.0000000007302000.00000004.00000800.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.244999013.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.245035032.000000000610B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	3ylxxU5Wko.exe, 00000000.00000002.280901191.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comessed	3ylxxU5Wko.exe, 00000000.00000003.248957423.000000000610A000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.248154930.000000000610B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.goodfont.co.kr	3ylxxU5Wko.exe, 00000000.00000002.280901191.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://google.com	3ylxxU5Wko.exe, 00000002.00000002.536518016.0000000007410000.00000004.08000000.00040000.00000000.sdmp, 3ylxxU5Wko.exe, 00000002.00000002.522256518.0000000004AD1000.00000004.00000800.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000002.00000002.509135114.0000000002F3D000.00000004.00000800.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000002.00000002.522256518.00000000049E6000.00000004.00000800.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000002.00000002.522256518.000000000479F000.00000004.00000800.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000002.00000002.522256518.0000000004970000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.comeY	3ylxxU5Wko.exe, 00000000.00000003.242410464.000000000610B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comB	3ylxxU5Wko.exe, 00000000.00000003.245029033.000000000612F000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.245212729.000000000612E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	3ylxxU5Wko.exe, 00000000.00000002.280901191.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

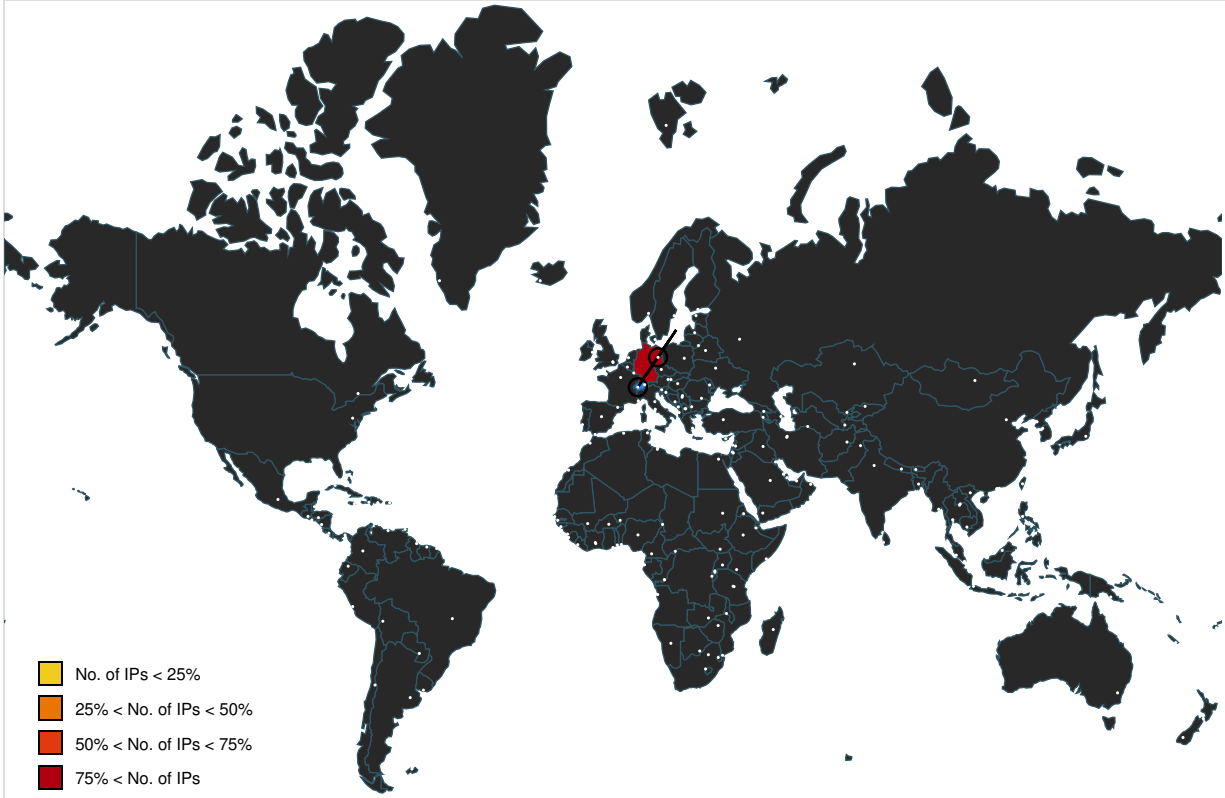
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.typography.netD	3ylxxU5Wko.exe, 00000000.00000002.280901191.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	3ylxxU5Wko.exe, 00000000.00000002.280901191.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	3ylxxU5Wko.exe, 00000000.00000002.280901191.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	3ylxxU5Wko.exe, 00000000.00000002.280901191.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comgrita	3ylxxU5Wko.exe, 00000000.00000003.248047661.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.248154930.000000000610B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/8	3ylxxU5Wko.exe, 00000000.00000003.246594659.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246548104.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246297960.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246804982.000000000610B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/5	3ylxxU5Wko.exe, 00000000.00000003.246594659.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246548104.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246297960.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246804982.000000000610B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/y/	3ylxxU5Wko.exe, 00000000.00000003.244185923.000000000610B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/c	3ylxxU5Wko.exe, 00000000.00000003.246297960.000000000610B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.comT=	3ylxxU5Wko.exe, 00000000.00000003.245035032.000000000610B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.comcom	3ylxxU5Wko.exe, 00000000.00000003.248890489.0000000006106000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.248957423.000000000610A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htme	3ylxxU5Wko.exe, 00000000.00000003.250191139.0000000006107000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.249911417.0000000006108000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.249982918.0000000006108000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.250069545.0000000006108000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.250363742.0000000006106000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.250279044.0000000006107000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comldv	3ylxxU5Wko.exe, 00000000.00000003.260510699.0000000006106000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	3ylxxU5Wko.exe, 00000000.00000002.280901191.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/Y0	3ylxxU5Wko.exe, 00000000.00000003.246594659.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.247048926.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246548104.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246957227.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246297960.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246881598.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246931816.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.247027959.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246804982.000000000610B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comac	3ylxxU5Wko.exe, 00000000.00000003.260510699.0000000006106000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comgrito	3ylxxU5Wko.exe, 00000000.00000003.248890489.0000000006106000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.248957423.000000000610A000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.248665387.000000000610A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comttodh	3ylxxU5Wko.exe, 00000000.00000003.248633787.000000000610A000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.248890489.0000000006106000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.248957423.000000000610A000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.248665387.000000000610A000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	3ylxxU5Wko.exe, 00000000.00000002.280901191.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	3ylxxU5Wko.exe, 00000000.00000002.280901191.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.coma	3ylxxU5Wko.exe, 00000000.00000003.242410464.000000000610B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	3ylxxU5Wko.exe, 00000000.00000002.280901191.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	3ylxxU5Wko.exe, 00000000.00000002.280901191.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	3ylxxU5Wko.exe, 00000002.00000002.509135114.0000000002ED1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	3ylxxU5Wko.exe, 00000000.00000002.280901191.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comR.TTF	3ylxxU5Wko.exe, 00000000.00000003.248154930.000000000610B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/keb	3ylxxU5Wko.exe, 00000000.00000003.247230845.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246594659.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.247048926.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.247202053.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246548104.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246957227.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246297960.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246881598.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.247102368.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246931816.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.247027959.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246804982.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.247272353.000000000610B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comalsd	3ylxxU5Wko.exe, 00000000.00000003.248633787.000000000610A000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.248890489.000000000610000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.248957423.000000000610A000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.248665387.000000000610A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	3ylxxU5Wko.exe, 00000000.00000002.280901191.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	3ylxxU5Wko.exe, 00000000.00000002.280901191.0000000007302000.00000004.00000800.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.248890489.000000000610000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.248047661.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.248957423.000000000610A000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.248154930.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.248008760.000000000610400.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.248665387.000000000610A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/	3ylxxU5Wko.exe, 00000000.00000003.250069545.0000000006108000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.250279044.0000000006107000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comF	3ylxxU5Wko.exe, 00000000.00000003.248633787.000000000610A000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.248890489.000000000610000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.248957423.000000000610A000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.248665387.000000000610A000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Q	3ylxxU5Wko.exe, 00000000.00000003.246297960.000000000610B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/jp/	3ylxxU5Wko.exe, 00000000.00000003.247230845.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246594659.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.247048926.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.247202053.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246548104.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246957227.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246297960.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246881598.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.247102368.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246931816.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.247027959.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246804982.000000000610B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.come.com	3ylxxU5Wko.exe, 00000000.00000003.260510699.0000000006106000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	3ylxxU5Wko.exe, 00000000.00000002.280901191.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	3ylxxU5Wko.exe, 00000000.00000002.280901191.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn	3ylxxU5Wko.exe, 00000000.00000002.280901191.0000000007302000.00000004.00000800.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.244936759.00000000060F2000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.245120597.00000000060F2000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	3ylxxU5Wko.exe, 00000000.00000002.280901191.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/Y00	3ylxxU5Wko.exe, 00000000.00000003.246594659.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246548104.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246297960.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246804982.000000000610B000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	3ylxxU5Wko.exe, 00000000.00000002.280901191.0000000007302000.00000004.00000800.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246594659.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246548104.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246297960.000000000610B000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.246804982.000000000610B000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	3ylxxU5Wko.exe, 00000000.00000002.280901191.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.coml	3ylxxU5Wko.exe, 00000000.00000003.245029033.000000000612F000.00000004.00000020.00020000.00000000.sdmp, 3ylxxU5Wko.exe, 00000000.00000003.245212729.000000000612E000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.12.253.26	tzitziklishop.ddns.net	Germany		33657	CMCSUS	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	796775
Start date and time:	2023-02-02 08:00:16 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 29s
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:	24
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:	3yIxxU5Wko.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@25/11@6/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed

HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
08:01:14	API Interceptor	857x Sleep call for process: 3yIxxU5Wko.exe modified
08:01:22	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\3yIxxU5Wko.exe" s>$(Arg0)
08:01:22	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
08:01:24	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
08:01:31	API Interceptor	2x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\3yIxxU5Wko.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	934400
Entropy (8bit):	7.675280590834261

Encrypted:	false
SSDEEP:	24576:IsC41FjAqn8/ysidgzWrSrLYo6F0xMpqG4yPa:JXjAANsSgzWrSvMWiq
MD5:	6DF2C2CAACCC7947F8439F248CDD386F
SHA1:	419AB96D1452301F126F63AB7E3135C9201E3F61
SHA-256:	8ECC4898D03BF034A6586FF886D9883B2AC27D08BDFE70DBD9878A4D77D5DCE8
SHA-512:	2E9128E897D4D0E4FA4D2CD4055B360751EA608FD39BCBF309E9EE629E71AB3BDD9ED44A773B69BB47C0F653D8A735054C3022261C73FFB8F5D164CBADB401 8D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 28%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....(.c.....0..:.....nX... ...`....@.. ..... ..@.....X..W....`..... ....H.....text...t8... ...:..... ..`.rsrc.....`.....<.....@..@.rel oc.....@.....@..B.....PX.....H.....p.....X...p.....0.....*....0.....{#...*..0.....{$...*..0.....(%....}#.....}$...*....0.....u.. .....z ...9 .2.[a%..^E....;.....+9.,N. . ..Z ..h.a+.(&....{#....{#...o'...,'. .6.Z S..?a+.((....{$....{$...o)...+..+..*..0..4..... ....)UU.Z(&....{#...o*...X)UU.Z((....{$...o+...X*.0..b.....r. ..p.....%..{#.....%q.....-.&.+.....o,....%..{$.....%q.....-.&.+.....o,....

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

Process:	C:\Users\user\Desktop\3yIxxU5Wko.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64 E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\3yIxxU5Wko.exe.log

Process:	C:\Users\user\Desktop\3yIxxU5Wko.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178 FF6
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Ve rsion=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72 e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni .dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\S ystem.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b 77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E

SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmpFB74.tmp

Process:	C:\Users\user\Desktop\3yIxxU5Wko.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1303
Entropy (8bit):	5.106282763013836
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0VAxtn:cbk4oL600QydbQxIYODOLedq3Tj
MD5:	528BB8755DED259833140220F4ED719D
SHA1:	72EC7DE60FE49DCB0AF6A2D6BE46C861BA281512
SHA-256:	0AE5DBA961881DA5E12EF7CD8AE69A5A8DE80EF1873648C35C113F00C0F4F66A
SHA-512:	4DEF2C8E6176BE8718A0EB6641D8962D28CCC51A3BF7DBDBD8A114F38C926E3E2774BCA89995FC9415B5C6BA5D51159BB8A0E9C9FA97C942DAE4CCB528642D00
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpFD98.tmp

Process:	C:\Users\user\Desktop\3yIxxU5Wko.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755734
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

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

Process:	C:\Users\user\Desktop\3yIxxU5Wko.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9

MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C35(A5
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.

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

Process:	C:\Users\user\Desktop\3yIxxU5Wko.exe
File Type:	OpenPGP Public Key
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:pO:pO
MD5:	B084970AD244C8EB4E9C0480CBDF17A8
SHA1:	309DAE2188E884B93A6038FEF906F13B6405AA47
SHA-256:	D3C827AC551EB4F941C9DC6AA1A2BDB88F9C24C4C272F981C4189ACB817D47FA
SHA-512:	15A69698E625A1CE015A595E89D5413359073B4CAD02060A2AD9CD5E52D62B5F3823A72AC428CE4F1803A608A07E30ED7A1902DDB5C5F7683CD1E368EFF0481
Malicious:	**true**
Preview:	.f..6..H

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

Process:	C:\Users\user\Desktop\3yIxxU5Wko.exe
File Type:	data
Category:	modified
Size (bytes):	24
Entropy (8bit):	4.584962500721156
Encrypted:	false
SSDEEP:	3:9bzY6oRDJoTBn:RzWDqTB
MD5:	3FCC766D28BFD974C68B38C27D0D7A9A
SHA1:	45ED19A78D9B79E46EDBFC3E3CA58E90423A676B
SHA-256:	39A25F1AB5099005A74CF04F3C61C3253CD9BDA73B85228B58B45AAA4E838641
SHA-512:	C7D47BDAABEEBB8C9D9B31CC4CE968EAF291771762FA022A2F55F9BA4838E71FDBD3F83792709E47509C5D94629D6D274CC933371DC01560D13016D944012D5
Malicious:	false
Preview:	9iH...}Z.4..f.....l.d

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

Process:	C:\Users\user\Desktop\3yIxxU5Wko.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E926
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.I.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.|i4...i...;O...n.?.,. ....v?.5}.OY@.dG|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. I..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

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

Process:	C:\Users\user\Desktop\3yIxxU5Wko.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	40
Entropy (8bit):	4.142896608419108
Encrypted:	false
SSDEEP:	3:oNN2+WWcsuJ:oNN2RWduJ
MD5:	B524911B681E2F42B054FD0311DE9476
SHA1:	0FF43787FABE00B8332EC9A741350FF439BCCD7F
SHA-256:	56E15BE1ECB9F3DBED863C1336410A6DD0007C5B1845621208668A2A15A342D7
SHA-512:	CA95C1F25DC5D84100942A4141CA9C4BFF8AAC0E669FBC493F50ED63EDE9571051C9D369FD5DE142CEDC25A7567D672AA8E4D5F4F97E174FC7CEE536A2680F6
Malicious:	false
Preview:	C:\Users\user\Desktop\3yIxxU5Wko.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.675280590834261
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	3yIxxU5Wko.exe
File size:	934400
MD5:	6df2c2caaccc7947f8439f248cdd386f
SHA1:	419ab96d1452301f126f63ab7e3135c9201e3f61
SHA256:	8ecc4898d03bf034a6586ff886d9883b2ac27d08bdfe70dbd9878a4d77d5dce8
SHA512:	2e9128e897d4d0e4fa4d2cd4055b360751ea608fd39bcbf309e9ee629e71ab3bdd9ed44a773b69bb47c0f653d8a735054c3022261c73ffb8f5d164cbadb4018d
SSDEEP:	24576:IsC41FjAqn8/ysidgzWrSrLYo6F0xMpqG4yPa:JXjAANsSgzWrSvMWiq
TLSH:	2A158D8737B1A8BFF68B407544283F886FA07113BF56E25397373A849B098FBB694151
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....(.c.....0..:.....nX... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4e586e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x63DB289A [Thu Feb 2 03:06:02 2023 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4

File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xe5814	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe6000	0x3c8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	

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

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xe3874	0xe3a00	False	0.8137194964991763	data	7.679578810089011	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xe6000	0x3c8	0x400	False	0.388671875	data	3.0176806594804035	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe8000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xe6058	0x36c	data		

Imports

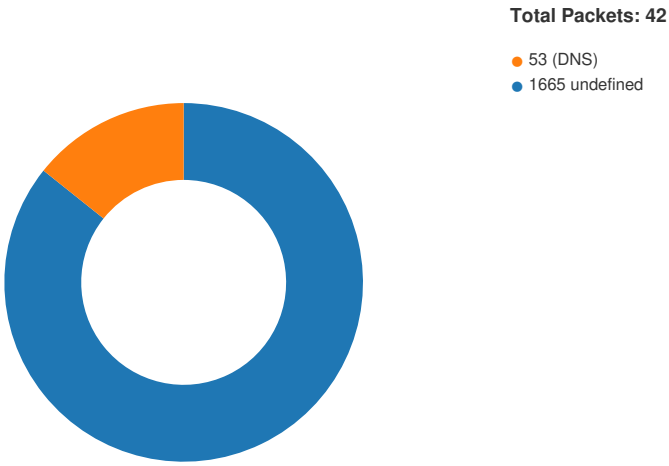
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.645.12.253.264971816652816766 02/02/23-08:01:58.369947	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49718	1665	192.168.2.6	45.12.253.26
45.12.253.26192.168.2.61665497152841753 02/02/23-08:01:51.077424	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	1665	49715	45.12.253.26	192.168.2.6
192.168.2.645.12.253.264971316652816766 02/02/23-08:01:29.730882	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49713	1665	192.168.2.6	45.12.253.26
192.168.2.645.12.253.264971416652816766 02/02/23-08:01:39.744017	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49714	1665	192.168.2.6	45.12.253.26
192.168.2.645.12.253.264971516652816766 02/02/23-08:01:51.165371	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49715	1665	192.168.2.6	45.12.253.26
45.12.253.26192.168.2.61665497182810290 02/02/23-08:01:58.690998	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	1665	49718	45.12.253.26	192.168.2.6
45.12.253.26192.168.2.61665497182841753 02/02/23-08:01:58.903710	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	1665	49718	45.12.253.26	192.168.2.6

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 2, 2023 08:01:27.405668974 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:27.432528973 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:27.432635069 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:27.607346058 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:27.694688082 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:27.694792986 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:27.714261055 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:27.786218882 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:27.786303043 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:27.814512014 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:27.870546103 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:27.905664921 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:27.990725994 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.061522961 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.061603069 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.061652899 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.061685085 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.061702013 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.061750889 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.088815928 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.088848114 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.088865995 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.088884115 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.088902950 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.088918924 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.088922024 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.088943005 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.088951111 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.088965893 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.088970900 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.089005947 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.115677118 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.115745068 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.115791082 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.115796089 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.115838051 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.115883112 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.115885973 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.115933895 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.115982056 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.115986109 CET	1665	49713	45.12.253.26	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 2, 2023 08:01:28.116033077 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.116079092 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.116080046 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.116126060 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.116173029 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.116178989 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.116220951 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.116267920 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.116281986 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.116314888 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.116358042 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.116364956 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.116410971 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.116452932 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.143675089 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.143743038 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.143791914 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.143795013 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.143838882 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.143882036 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.143887043 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.143934965 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.143982887 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.143987894 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.144031048 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.144077063 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.144077063 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.144124985 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.144167900 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.144171000 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.144217014 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.144258976 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.144263983 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.144310951 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.144352913 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.144359112 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.144432068 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.144471884 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.144478083 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.144526005 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.144558907 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.144593954 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.144604921 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.144654036 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.144655943 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.144702911 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.144742012 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.144750118 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.144798040 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.144839048 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.144845963 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.144893885 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.144933939 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.144941092 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.144990921 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.145032883 CET	49713	1665	192.168.2.6	45.12.253.26
Feb 2, 2023 08:01:28.145040035 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.145087004 CET	1665	49713	45.12.253.26	192.168.2.6
Feb 2, 2023 08:01:28.145127058 CET	49713	1665	192.168.2.6	45.12.253.26

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 2, 2023 08:01:27.352694035 CET	49448	53	192.168.2.6	8.8.8.8
Feb 2, 2023 08:01:27.374512911 CET	53	49448	8.8.8.8	192.168.2.6
Feb 2, 2023 08:01:39.035572052 CET	59082	53	192.168.2.6	8.8.8.8
Feb 2, 2023 08:01:39.055030107 CET	53	59082	8.8.8.8	192.168.2.6
Feb 2, 2023 08:01:50.927093983 CET	59504	53	192.168.2.6	8.8.8.8
Feb 2, 2023 08:01:50.948883057 CET	53	59504	8.8.8.8	192.168.2.6
Feb 2, 2023 08:01:58.230649948 CET	63863	53	192.168.2.6	8.8.8.8
Feb 2, 2023 08:01:58.250291109 CET	53	63863	8.8.8.8	192.168.2.6
Feb 2, 2023 08:02:06.182754040 CET	62538	53	192.168.2.6	8.8.8.8
Feb 2, 2023 08:02:06.200422049 CET	53	62538	8.8.8.8	192.168.2.6
Feb 2, 2023 08:02:09.400620937 CET	51530	53	192.168.2.6	8.8.8.8
Feb 2, 2023 08:02:09.422087908 CET	53	51530	8.8.8.8	192.168.2.6

DNS Queries

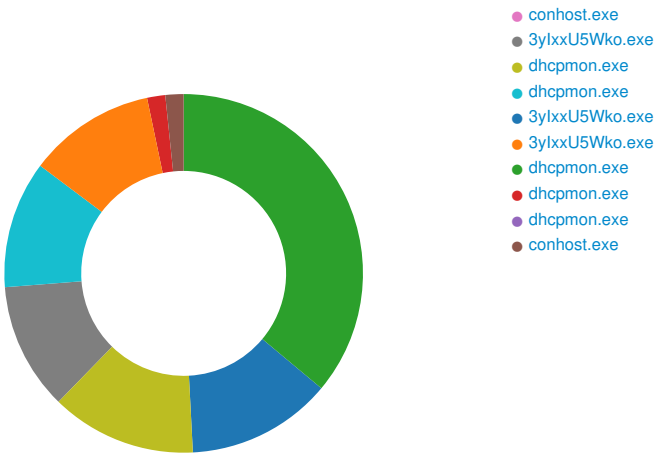
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 2, 2023 08:01:27.352694035 CET	192.168.2.6	8.8.8.8	0xd218	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 2, 2023 08:01:39.035572052 CET	192.168.2.6	8.8.8.8	0x739c	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 2, 2023 08:01:50.927093983 CET	192.168.2.6	8.8.8.8	0x6fb7	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 2, 2023 08:01:58.230649948 CET	192.168.2.6	8.8.8.8	0x11ef	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 2, 2023 08:02:06.182754040 CET	192.168.2.6	8.8.8.8	0x444f	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false
Feb 2, 2023 08:02:09.400620937 CET	192.168.2.6	8.8.8.8	0xd6fb	Standard query (0)	tzitziklis hop.ddns.net	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 2, 2023 08:01:27.374512911 CET	8.8.8.8	192.168.2.6	0xd218	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 2, 2023 08:01:39.055030107 CET	8.8.8.8	192.168.2.6	0x739c	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 2, 2023 08:01:50.948883057 CET	8.8.8.8	192.168.2.6	0x6fb7	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 2, 2023 08:01:58.250291109 CET	8.8.8.8	192.168.2.6	0x11ef	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 2, 2023 08:02:06.200422049 CET	8.8.8.8	192.168.2.6	0x444f	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false
Feb 2, 2023 08:02:09.422087908 CET	8.8.8.8	192.168.2.6	0xd6fb	No error (0)	tzitziklis hop.ddns.net		45.12.253.26	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: 3yIxxU5Wko.exe PID: 5192, Parent PID: 3452

General

Target ID:	0
Start time:	08:01:07
Start date:	02/02/2023
Path:	C:\Users\user\Desktop\3yIxxU5Wko.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\3yIxxU5Wko.exe
Imagebase:	0xce0000
File size:	934400 bytes
MD5 hash:	6DF2C2CAACCC7947F8439F248CDD386F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.265161826.0000000004019000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.265161826.0000000004019000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.265161826.0000000004019000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.265161826.0000000004019000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.262140358.0000000003160000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.265161826.00000000044B0000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.265161826.00000000044B0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.265161826.00000000044B0000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.265161826.00000000044B0000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72F0CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72F0CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\3yIxxU5Wko.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7321C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\3yIxxU5Wko.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	7321C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72EE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72EE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72E403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72EECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72E403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72E403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72E403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72E403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72EE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72EE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71D51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71D51B4F	ReadFile

Analysis Process: 3yIxxU5Wko.exe PID: **3232**, Parent PID: **5192**

General

Target ID:	1
Start time:	08:01:16
Start date:	02/02/2023

Path:	C:\Users\user\Desktop\3yIxxU5Wko.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\3yIxxU5Wko.exe
Imagebase:	0x3c0000
File size:	934400 bytes
MD5 hash:	6DF2C2CAACCC7947F8439F248CDD386F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 3yIxxU5Wko.exe PID: **5480**, Parent PID: **5192**

General

Target ID:	2
Start time:	08:01:17
Start date:	02/02/2023
Path:	C:\Users\user\Desktop\3yIxxU5Wko.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\3yIxxU5Wko.exe
Imagebase:	0xad0000
File size:	934400 bytes
MD5 hash:	6DF2C2CAACCC7947F8439F248CDD386F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.536518016.0000000007410000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.536518016.0000000007410000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.536518016.0000000007410000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.536518016.0000000007410000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.532206387.00000000055F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.532206387.00000000055F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.532206387.00000000055F0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.532206387.00000000055F0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.537510131.0000000007830000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.537510131.0000000007830000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.537510131.0000000007830000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.537510131.0000000007830000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.509135114.0000000002ED1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.522256518.0000000004AD1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.522256518.0000000004AD1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.522256518.0000000004AD1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.509135114.0000000002F3D000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.509135114.0000000002F3D000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.536448146.0000000007400000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.536448146.0000000007400000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.536448146.0000000007400000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.536448146.0000000007400000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.534992759.0000000006BF0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.534992759.0000000006BF0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)

- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.534992759.0000000006BF0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.534992759.0000000006BF0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.536233579.00000000073E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.536233579.00000000073E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.536233579.00000000073E0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.536233579.00000000073E0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.535807006.0000000007390000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.535807006.0000000007390000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.535807006.0000000007390000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.535807006.0000000007390000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 00000002.00000002.522256518.00000000049E6000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.522256518.00000000049E6000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.537164844.00000000076D0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.537164844.00000000076D0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.537164844.00000000076D0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.537164844.00000000076D0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.536346079.00000000073F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.536346079.00000000073F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.536346079.00000000073F0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.536346079.00000000073F0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.536644841.0000000007420000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.536644841.0000000007420000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.536644841.0000000007420000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.536644841.0000000007420000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.536904085.00000000076B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.536904085.00000000076B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.536904085.00000000076B0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.536904085.00000000076B0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.533150179.00000000064A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.533150179.00000000064A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.533150179.00000000064A0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.533150179.00000000064A0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.533150179.00000000064A0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000003.282621709.0000000006851000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.537796470.0000000007860000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.537796470.0000000007860000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000002.00000002.537796470.0000000007860000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.537796470.0000000007860000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.522256518.0000000004970000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000002.00000002.522256518.0000000004970000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.522256518.0000000004970000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.522256518.000000000479F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000002.00000002.522256518.000000000479F000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000002.00000002.522256518.000000000479F000.00000004.00000800.00020000.00000000.sdmp, Author: unknown

Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72F0CF06	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	72F0CF06	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	71D5BEFF	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	71D51E60	CreateFileW
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71D5BEFF	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	71D5DD66	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	71D5DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpFB74.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	71D57038	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	71D51E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpFD98.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	71D57038	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71D5BEFF	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	71D5BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	3	71D51E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	71D51E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	71D51E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpFB74.tmp	success or wait	1	71D56A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpFD98.tmp	success or wait	1	71D56A95	DeleteFileW
C:\Users\user\Desktop\3yIxxU5Wko.exe:Zone.Identifier	success or wait	1	71CD2935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ D06ED635-68F6-4E9A-955C-4899F5 F57B9A\run.dat	0	8	fd 66 1d fd 36 05 fd 48	f6H	success or wait	1	71D51B4F	WriteFile
C:\Program Files (x86)\DHCP Mo nitor\dhcpmon.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 28 fd 63 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 3a 0e 00 00 06 00 00 00 00 00 00 6e 58 0e 00 00 20 00 00 00 60 0e 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 0e 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL(c0:nX `@ @	success or wait	4	71D5DD66	CopyFileW
C:\Program Files (x86)\DHCP Mo nitor\dhcpmon.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	71D5DD66	CopyFileW
C:\Users\user\AppData\Local\Te mp\tmpFB74.tmp	0	1303	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	71D51B4F	WriteFile
C:\Users\user\AppData\Roaming\ D06ED635-68F6-4E9A-955C-4899F5 F57B9A\task.dat	0	40	43 3a 5c 55 73 65 72 73 5c 65 6e 67 69 6e 65 65 72 5c 44 65 73 6b 74 6f 70 5c 33 79 49 78 78 55 35 57 6b 6f 2e 65 78 65	C:\Users\user\Desktop\3yIxxU5Wko.exe	success or wait	1	71D51B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpFD98.tmp	0	1310	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	71D51B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	0	232	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd fd 26 15 fd fd 69 2b fd 49 63 28 31 fd 50 fd fd 50 fd 63 4c 54 fd fd 42 41 fd 62 fd fd 1b fd fd fd fd fd 34 68 fd 12 fd 74 fd 2b fd 07 5a 5c fd fd 20 fd 69 fd fd a4 fd fd 40 fd 33 fd fd 7b 0c fd 1c 67 72 76 2b 56 fd fd fd 42 19 0e fd 0d fd fd 15 5d fd 50 fd fd 16 57 fd 34 43 7d 75 4c 1e fd fd 0b fd 73 7e fd fd 46 04 fd fd 7d fd fd fd fd fd 00 45 fd fd fd fd fd fd 45 fd 14 fd 36 45 fd fd fd fd fd 7b 5f 05 18 7b fd 79 53 fd fd fd 37 fd fd 22 16 68 4b fd 21 03 78 fd 32 fd fd 69 e3 fd 7a 4a fd bb fd 20 fd fd fd fd 66 fd 67 3f fd 5f 0b fd fd fd 30 fd 3a 65 5b 37 77 7b 31 fd 21 fd 34 fd fd fd fd fd 26 fd	Gjh\3A5x&i+c(1PPcLTAb 4ht+Z\ i@ 3{grv+VB]PW4C}uLs~F} EE6E{{yS7"hK!x2izJ f? _0:e[7w{1!4&	success or wait	4	71D51B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	0	327432	70 54 eb fd 21 fd 08 57 fd fd 47 14 4a fd fd 61 60 29 17 40 8b 69 fd fd 77 70 4b fd 73 6f 40 fd 06 fd 35 fd 3d 10 5e fd 1d 51 fd 6f 79 fd 3d 65 40 39 fd 42 fd fd fd 46 fd fd 30 39 75 22 33 fd fd 20 30 74 fd 19 52 44 6e 5f 34 64 fd fd 17 02 fd 45 fd fd 06 69 fd 08 fd fd fd fd 7e 0c fd fd 7c fd fd 66 58 5f 0e fd fd 58 66 fd 70 5e fd fd fd fd 03 fd 3e 61 cb fd 24 fd fd fd 65 05 36 3a 37 64 fd 28 61 05 41 fd fd fd 3d fd 29 2a 0d fd fd fd fd 7b 42 1c 5b fd fd fd 79 25 fd 2a 31 fd 69 fd 51 fd 3c 12 90 78 74 29 58 13 11 48 09 fd 20 fd 24 48 46 37 67 0f fd fd 49 fd 2a 33 03 7b 0c 6e fd fd fd fd 4c 5b 79 3b 69 fd fd 73 2d 1e fd fd fd 28 35 69 8b fd fd 10 fd fd 02 fd fd 08 17 4a 09 35 62 37 7d fd fd 66 4b fd fd 48 56	pT!WGJa)@iwpKso@5=^ Qoy=e@9BF09u"3 0tRDn_4dEi~|fX_Xfp^>a$ e6:7d(aA=)* {B[y%*iQ<xtXH HF7gI*3{nLy;is- (5iJ5b7}fKHV	success or wait	1	71D51B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	0	24	39 69 48 fd 1a c5 7d 5a cd 34 00 fd 66 0d c7 fd fd fd 6c fd 64	9iH}Z4fld	success or wait	1	71D51B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72EE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72EE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72E403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72EECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72E403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72E403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72E403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72E403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72EE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72EE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71D51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71D51B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	72ECD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	72ECD72F	unknown
C:\Users\user\Desktop\3yIxxU5Wko.exe	unknown	4096	success or wait	1	72ECD72F	unknown
C:\Users\user\Desktop\3yIxxU5Wko.exe	unknown	512	success or wait	1	72ECD72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	71D5646A	RegSetValueExW

Analysis Process: schtasks.exe PID: **320**, Parent PID: **5480**

General

Target ID:	3
Start time:	08:01:20
Start date:	02/02/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmpFB74.tmp
Imagebase:	0x8c0000
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\tmpFB74.tmp	unknown	2	success or wait	1	8CAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpFB74.tmp	unknown	1304	success or wait	1	8CABD9	ReadFile

Analysis Process: conhost.exe PID: **3108**, Parent PID: **320**

General

Target ID:	4
Start time:	08:01:20
Start date:	02/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: **5348**, Parent PID: **5480**

General

Target ID:	5
Start time:	08:01:20
Start date:	02/02/2023
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmpFD98.tmp
Imagebase:	0x8c0000
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\tmpFD98.tmp	unknown	2	success or wait	1	8CAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpFD98.tmp	unknown	1311	success or wait	1	8CABD9	ReadFile

Analysis Process: conhost.exe PID: **3732**, Parent PID: **5348**

General

Target ID:	6
Start time:	08:01:20
Start date:	02/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff6da640000
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: 3yIxxU5Wko.exe PID: **4748**, Parent PID: **1064**

General

Target ID:	7
Start time:	08:01:22
Start date:	02/02/2023
Path:	C:\Users\user\Desktop\3yIxxU5Wko.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\3yIxxU5Wko.exe 0
Imagebase:	0x7c0000
File size:	934400 bytes
MD5 hash:	6DF2C2CAACCC7947F8439F248CDD386F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72F0CF06	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	72F0CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72EE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72EE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72E403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72EECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72E403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72E403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72E403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72E403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72EE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72EE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71D51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71D51B4F	ReadFile

Analysis Process: dhcpmon.exe PID: **4976**, Parent PID: **1064**

General

Target ID:	8
Start time:	08:01:23
Start date:	02/02/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0x740000
File size:	934400 bytes
MD5 hash:	6DF2C2CAACCC7947F8439F248CDD386F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000008.00000002.317358866.0000000002D60000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 28%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72F0CF06	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	72F0CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7321C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	7321C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72EE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72EE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72E403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72EECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72E403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72E403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72E403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72E403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72EE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72EE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71D51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71D51B4F	ReadFile

Analysis Process: dhcpmon.exe PID: **3424**, Parent PID: **3452**

General

Target ID:	16
Start time:	08:01:33
Start date:	02/02/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0x8d0000
File size:	934400 bytes
MD5 hash:	6DF2C2CAACCC7947F8439F248CDD386F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72F0CF06	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	72F0CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72EE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72EE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72E403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72EECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72E403DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72E403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72E403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72E403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72EE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72EE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71D51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71D51B4F	ReadFile

Analysis Process: 3yIxxU5Wko.exe PID: **5868**, Parent PID: **4748**

General

Target ID:	17
Start time:	08:01:34
Start date:	02/02/2023
Path:	C:\Users\user\Desktop\3yIxxU5Wko.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\3yIxxU5Wko.exe
Imagebase:	0x380000
File size:	934400 bytes
MD5 hash:	6DF2C2CAACCC7947F8439F248CDD386F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 3yIxxU5Wko.exe PID: **2376**, Parent PID: **4748**

General

Target ID:	18
Start time:	08:01:34
Start date:	02/02/2023
Path:	C:\Users\user\Desktop\3yIxxU5Wko.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\3yIxxU5Wko.exe
Imagebase:	0x680000
File size:	934400 bytes
MD5 hash:	6DF2C2CAACCC7947F8439F248CDD386F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.344314956.0000000003A89000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.344314956.0000000003A89000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000012.00000002.344314956.0000000003A89000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.336403877.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.336403877.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.336403877.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000012.00000002.336403877.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.341772229.0000000002A81000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.341772229.0000000002A81000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000012.00000002.341772229.0000000002A81000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72F0CF06	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	72F0CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72EE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72EE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72E403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72EECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72E403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72E403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72E403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72E403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72EE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72EE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71D51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71D51B4F	ReadFile

Analysis Process: dhcpmon.exe PID: **1748**, Parent PID: **4976**

General

Target ID:	19
Start time:	08:01:35
Start date:	02/02/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x1a0000
File size:	934400 bytes

MD5 hash:	6DF2C2CAACCC7947F8439F248CDD386F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: dhcpmon.exe PID: **4500**, Parent PID: **4976**

General

Target ID:	20
Start time:	08:01:36
Start date:	02/02/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x630000
File size:	934400 bytes
MD5 hash:	6DF2C2CAACCC7947F8439F248CDD386F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.345914663.0000000002AC1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.345914663.0000000002AC1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000014.00000002.345914663.0000000002AC1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: dhcpmon.exe PID: **5884**, Parent PID: **3424**

General

Target ID:	21
Start time:	08:01:50
Start date:	02/02/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x8d0000
File size:	934400 bytes
MD5 hash:	6DF2C2CAACCC7947F8439F248CDD386F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: conhost.exe PID: **5348**, Parent PID: **5836**

General

Target ID:	23
Start time:	08:02:33
Start date:	02/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

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

Disassembly

No disassembly