ID: 877425
Sample Name: j2RMII0d3S.exe
Cookbook: default.jbs
Time: 13:46:04
Date: 29/05/2023
Version: 37.1.0 Beryl

Table of Contents

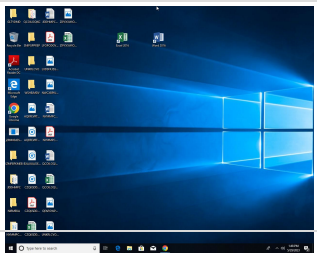
Windows Analysis Report

j2RMII0d3S.exe

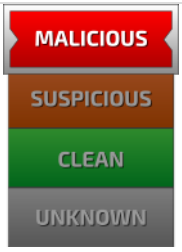
Overview

General Information

Sample Name:	j2RMII0d3S.exe
Original Sample Name:	adb719d2a3c5…
Analysis ID:	877425
MD5:	adb719d2a3c5…
SHA1:	488faf72df7a8f…
SHA256:	86016f9f3443fd..
Tags:	exe NanoCore RAT
Infos:	



Detection



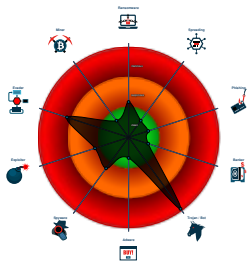
Nanocore

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Antivirus / Scanner detection for sub…
- Sigma detected: Scheduled temp fil…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT

Classification



Process Tree

- **System is w10x64**
- j2RMII0d3S.exe (PID: 6024 cmdline: C:\Users\user\Desktop\j2RMII0d3S.exe MD5: ADB719D2A3C51A77AB1ED355F91D3CA2)
  - schtasks.exe (PID: 5696 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp8D81.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5732 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5720 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp8EDA.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 2576 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- j2RMII0d3S.exe (PID: 5724 cmdline: C:\Users\user\Desktop\j2RMII0d3S.exe 0 MD5: ADB719D2A3C51A77AB1ED355F91D3CA2)
- dhcpmon.exe (PID: 2068 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: ADB719D2A3C51A77AB1ED355F91D3CA2)
- dhcpmon.exe (PID: 2764 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: ADB719D2A3C51A77AB1ED355F91D3CA2)
- **cleanup**

Malware Threat Intel

Provided by malpedia

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

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "72ec1ea3-16bf-4e76-a7cf-15ed5e2a",
  "Group": "Marcello",
  "Domain1": "december2n.duckdns.org",
  "Domain2": "december2nd.ddns.net",
  "Port": 61715,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Enable",
  "SetCriticalProcess": "Enable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Enable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "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

Initial Sample

Source	Rule	Description	Author	Strings
j2RMII0d3S.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
j2RMII0d3S.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
j2RMII0d3S.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
j2RMII0d3S.exe	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xfef5:$x1: NanoCore Client • 0xff05:$x1: NanoCore Client • 0x1014d:$x2: NanoCore.ClientPlugin • 0x1018d:$x3: NanoCore.ClientPluginHost • 0x10142:$i1: IClientApp • 0x10163:$i2: IClientData • 0x1016f:$i3: IClientNetwork • 0x1017e:$i4: IClientAppHost • 0x101a7:$i5: IClientDataHost • 0x101b7:$i6: IClientLoggingHost • 0x101ca:$i7: IClientNetworkHost • 0x101dd:$i8: IClientUIHost • 0x101eb:$i9: IClientNameObjectCollection • 0x10207:$i10: IClientReadOnlyNameObjectCollection • 0xff54:$s1: ClientPlugin • 0x10156:$s1: ClientPlugin • 0x1064a:$s2: EndPoint • 0x10653:$s3: IPAddress • 0x1065d:$s4: IPEndPoint • 0x12093:$s6: get_ClientSettings • 0x12637:$s7: get_Connected
j2RMII0d3S.exe	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
Click to see the 1 entries				

Dropped Files

Source	Rule	Description	Author	Strings
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xfef5:$x1: NanoCore Client • 0xff05:$x1: NanoCore Client • 0x1014d:$x2: NanoCore.ClientPlugin • 0x1018d:$x3: NanoCore.ClientPluginHost • 0x10142:$i1: IClientApp • 0x10163:$i2: IClientData • 0x1016f:$i3: IClientNetwork • 0x1017e:$i4: IClientAppHost • 0x101a7:$i5: IClientDataHost • 0x101b7:$i6: IClientLoggingHost • 0x101ca:$i7: IClientNetworkHost • 0x101dd:$i8: IClientUIHost • 0x101eb:$i9: IClientNameObjectCollection • 0x10207:$i10: IClientReadOnlyNameObjectCollection • 0xff54:$s1: ClientPlugin • 0x10156:$s1: ClientPlugin • 0x1064a:$s2: EndPoint • 0x10653:$s3: IPAddress • 0x1065d:$s4: IPEndPoint • 0x12093:$s6: get_ClientSettings • 0x12637:$s7: get_Connected

Source	Rule	Description	Author	Strings
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
Click to see the 1 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.350824921.0000000000892000.00000002.00000001.01000000.00000003.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000000.350824921.0000000000892000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000000.350824921.0000000000892000.00000002.00000001.01000000.00000003.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000000.00000000.350824921.0000000000892000.00000002.00000001.01000000.00000003.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xff8d:$a1: NanoCore.ClientPluginHost • 0xff4d:$a2: NanoCore.ClientPlugin • 0x11ea6:$b1: get_BuilderSettings • 0xfda9:$b2: ClientLoaderForm.resources • 0x115c6:$b3: PluginCommand • 0xff7e:$b4: IClientAppHost • 0x1a3fe:$b5: GetBlockHash • 0x124fe:$b6: AddHostEntry • 0x161f1:$b7: LogClientException • 0x1246b:$b8: PipeExists • 0xffb7:$b9: IClientLoggingHost
00000003.00000002.367779928.0000000003F91000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 32 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.j2RMII0d3S.exe.30b17a0.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x40c2:$x1: NanoCore.ClientPluginHost
0.2.j2RMII0d3S.exe.30b17a0.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0x40c2:$x2: NanoCore.ClientPluginHost • 0x41a0:$s4: PipeCreated • 0x40dc:$s5: IClientLoggingHost

Source	Rule	Description	Author	Strings
0.2.j2RMII0d3S.exe.30b17a0.0.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x410c:$x2: NanoCore.ClientPlugin • 0x40c2:$x3: NanoCore.ClientPluginHost • 0x4122:$i3: IClientNetwork • 0x40dc:$i6: IClientLoggingHost • 0x3e5b:$s1: ClientPlugin • 0x4115:$s1: ClientPlugin
0.2.j2RMII0d3S.exe.30b17a0.0.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x40c2:$a1: NanoCore.ClientPluginHost • 0x410c:$a2: NanoCore.ClientPlugin • 0x40dc:$b9: IClientLoggingHost
3.2.j2RMII0d3S.exe.2fb3b90.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x42d2:$x1: NanoCore.ClientPluginHost
Click to see the 86 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

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

Timestamp:	192.168.2.3192.169.69.2649700617152025019 05/29/23-13:46:57.708417
SID:	2025019
Source Port:	49700
Destination Port:	61715
Protocol:	TCP
Classtype:	A Network Trojan was detected

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

Timestamp:	192.168.2.3192.169.69.2649708617152025019 05/29/23-13:48:20.994121
SID:	2025019
Source Port:	49708
Destination Port:	61715
Protocol:	TCP
Classtype:	A Network Trojan was detected

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

Timestamp:	192.168.2.3192.169.69.2649707617152025019 05/29/23-13:48:15.596900
SID:	2025019

Source Port:	49707
Destination Port:	61715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26	−
Timestamp:	192.168.2.3192.169.69.2649701617152025019 05/29/23-13:47:03.125196
SID:	2025019
Source Port:	49701
Destination Port:	61715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26	−
Timestamp:	192.168.2.3192.169.69.2649706617152025019 05/29/23-13:48:10.004732
SID:	2025019
Source Port:	49706
Destination Port:	61715
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 192.169.69.26	−
Timestamp:	192.168.2.3192.169.69.2649702617152025019 05/29/23-13:47:09.127331
SID:	2025019
Source Port:	49702
Destination Port:	61715
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

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

Networking

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

E-Banking Fraud

Yara detected Nanocore RAT

Operating System Destruction

Protects its processes via BreakOnTermination flag

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)

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

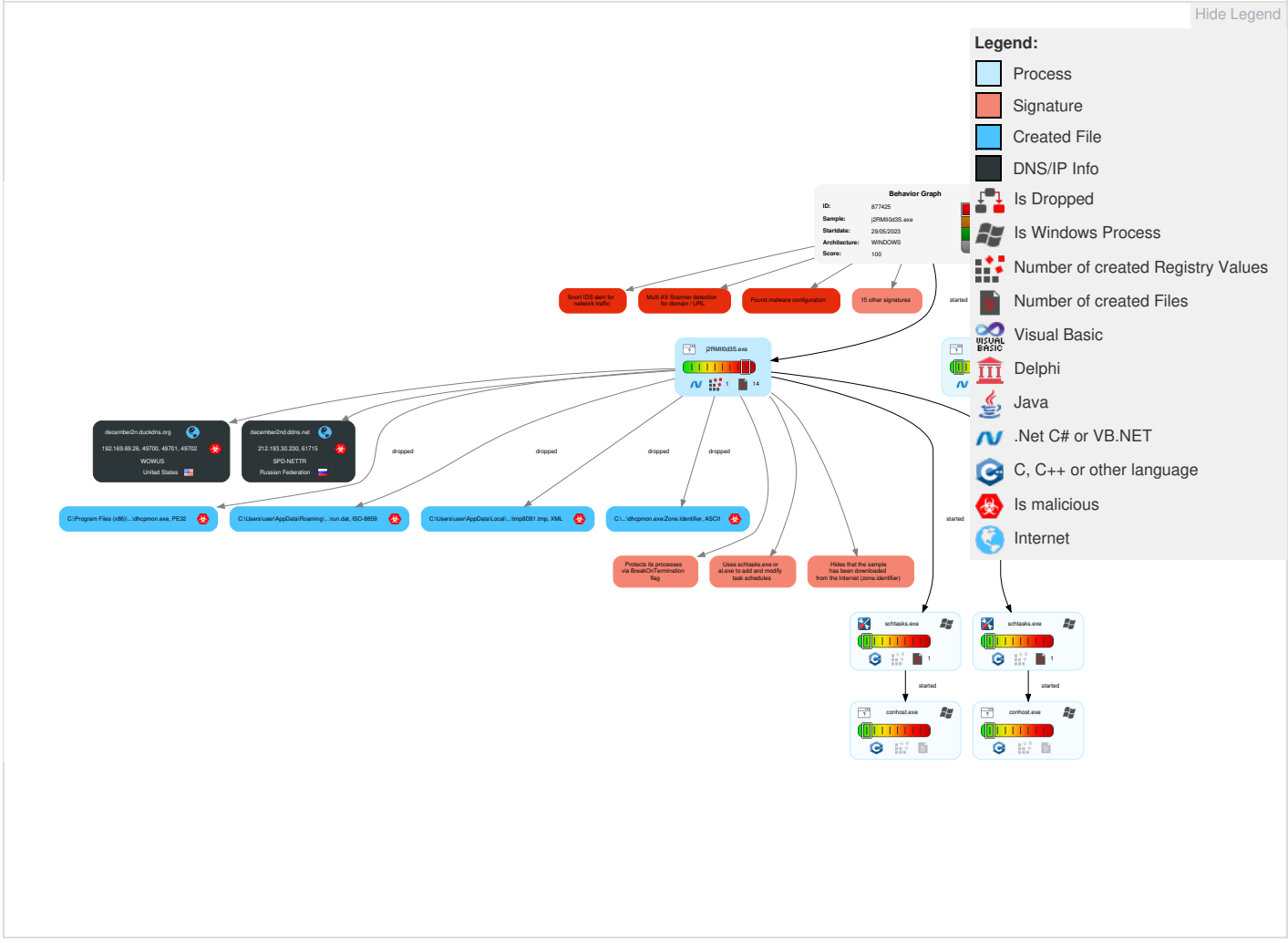
Yara detected Nanocore RAT

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 Scheduled Task/Job	1 Scheduled Task/Job	1 Access Token Manipulation	2 Masquerading	2 1 Input Capture	1 1 Security Software Discovery	Remote Services	2 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	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 2 Process Injection	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
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Scheduled Task/Job	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 Access Token Manipulation	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 2 Process Injection	LSA Secrets	1 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	1 Non-Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Deobfuscate/Decode Files or Information	Cached Domain Credentials	3 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	2 1 Application Layer Protocol	Jamming or Denial of Service		Abuse Accessibility Features

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Hidden Files and Directories	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	2 Obfuscated Files or Information	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
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 1 Software Packing	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
j2RMII0d3S.exe	97%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
j2RMII0d3S.exe	87%	Virustotal		Browse
j2RMII0d3S.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
j2RMII0d3S.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	97%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
december2nd.ddns.net	17%	Virustotal		Browse
december2n.duckdns.org	19%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
december2n.duckdns.org	100%	Avira URL Cloud	malware	
december2nd.ddns.net	100%	Avira URL Cloud	malware	
december2n.duckdns.org	19%	Virustotal		Browse
december2nd.ddns.net	17%	Virustotal		Browse

Domains and IPs

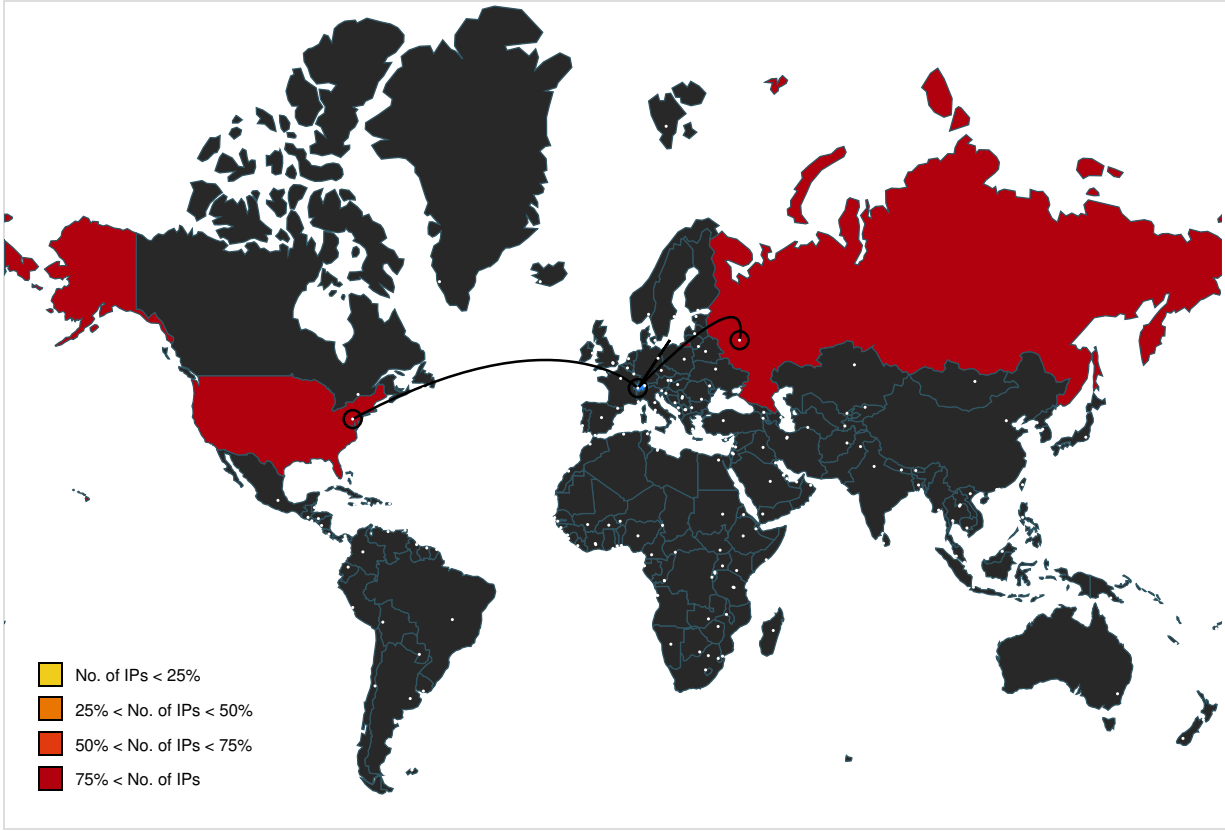
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
december2nd.ddns.net	212.193.30.230	true	true	• 17%, Virustotal, Browse	unknown
december2n.duckdns.org	192.169.69.26	true	true	• 19%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
december2nd.ddns.net	true	• 17%, Virustotal, Browse • Avira URL Cloud: malware	unknown
december2n.duckdns.org	true	• 19%, Virustotal, Browse • Avira URL Cloud: malware	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
212.193.30.230	december2nd.ddns.net	Russian Federation		57844	SPD-NETTR	true
192.169.69.26	december2n.duckdns.org	United States		23033	WOWUS	true

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	877425
Start date and time:	2023-05-29 13:46:04 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	j2RMII0d3S.exe
Original Sample Name:	adb719d2a3c51a77ab1ed355f91d3ca2.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/8@11/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed

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

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
13:46:54	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\j2RMII0d3S.exe" s>$(Arg0)
13:46:54	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
13:46:55	API Interceptor	965x Sleep call for process: j2RMII0d3S.exe modified
13:46:57	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\j2RMII0d3S.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	215040
Entropy (8bit):	7.479863878592803
Encrypted:	false
SSDEEP:	6144:gLV6Bta6dtJmakIM5sx/r1+Fw1VRQRnuDoPvEPWNSnswy:gLV6BtpmkHVYFSgRnrvEuNSW
MD5:	ADB719D2A3C51A77AB1ED355F91D3CA2
SHA1:	488FAF72DF7A8FD8E47E71B98D1149B0F4E6950B
SHA-256:	86016F9F3443FD0A79162579F2D359B1150E84182F9E3C162A2FB4932CCC2E23

SHA-512:	E4969ECC71B1F364780EEF72BC3D86641188AF916AC06697AA03037B0D923E907EC94EA25BBFE3681DA91985604F64D2DA9F4155EE1B24BB054AADEE2B4906E7
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: unknown
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 97%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....~..... .....@.. .....8...W.... ..xz..... ....H.....text..... ....`.reloc.....@..B.rsrc...xz... ...\|.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2.... ....3.... .....*.*....0..E.....s7....-(&s8....-&&s9....,$&s:.....s;.....*.....+.....+.....+.....0.....~....o<...*..0.....~....o=...*..0.....~....o>...*..0.....~....o?...*..0.....~....o@...*..0.....-.&(A...*&+...0..$..... ~B.....-.(...+.-.&+..B...+.~B...*.0.....-.&(A...*&+...0..

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

Process:	C:\Users\user\Desktop\j2RMII0d3S.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

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

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\j2RMII0d3S.exe.log

Process:	C:\Users\user\Desktop\j2RMII0d3S.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false

SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_3 2\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.Vi sualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp8D81.tmp

Process:	C:\Users\user\Desktop\j2RMII0d3S.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1300
Entropy (8bit):	5.116614001649491
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK07xtn:cbk4oL600QydbQxIYODOLedq38j
MD5:	F3BE702BA75B2AA9CDA586312A9A5464
SHA1:	886962BD925B7EB72C5517EBF307FE34AFE80DB0
SHA-256:	F7CE656F63AAC6AB8D4E1BE6D3EED3061C9F591D5E6DEC406C651B7C63071C93
SHA-512:	08CC11655ABC484A0EFF6D84BE88CAF4D4DF21DE6E7E6E9F42DB9C8FD39739C3FA5937A377FF5754AF63A21094D22D5CFDBB16EF078A8EA74C7D2324C2262 5C
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Princi pals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoing OnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyI fNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunO nlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp8EDA.tmp

Process:	C:\Users\user\Desktop\j2RMII0d3S.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733 4
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>.. </Princi pals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoing OnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyI fNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunO nlyIfIdle>.. <Wak

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

Process:	C:\Users\user\Desktop\j2RMII0d3S.exe
File Type:	ISO-8859 text, with NEL line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:PEt:PEt
MD5:	63412171686D0C8EDDD7EFCE61B0708C

SHA1:	0CADE59C91C060DA09F47A02422AF8C4FEE706D0
SHA-256:	C05ED9F30CE1CBBFE7A5D30D699534BDFDA522B8808F5F9990BF6BA4DD72CBBA
SHA-512:	4C16BD9EC2C4047155CD467ABFD7B4BDE2FD4392A3A4701AFE126776D85205268AE7DAB43E2045E0006E27D4F41E5A99E41BBA9E4E75ED1E2F0E6CBB4ACA502B
Malicious:	**true**
Preview:	.6I.`.H

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

Process:	C:\Users\user\Desktop\j2RMII0d3S.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	37
Entropy (8bit):	4.486348298002912
Encrypted:	false
SSDEEP:	3:oNWXp5vPXBNC:oNWXpFq
MD5:	D1C7985B75C5F1DFFEDE7EC2C1178803
SHA1:	CD04FD7558F103AE0AC564F7EEC82A049A530AFC
SHA-256:	E93FDB2BB74DE2174544D99A391DC2809DAAA65FE9719CEA759B83F6B19652F3
SHA-512:	0661D94743EFF0234DFC18CC05307B0F12169ADC334AB15B3FE3516D071D837AEF17297175C614A8E28CBE7E0C3C17EF2A235332BEC600A7D12A0EFF5AD4884
Malicious:	false
Preview:	C:\Users\user\Desktop\j2RMII0d3S.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.479863878592803
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	j2RMII0d3S.exe
File size:	215040
MD5:	adb719d2a3c51a77ab1ed355f91d3ca2
SHA1:	488faf72df7a8fd8e47e71b98d1149b0f4e6950b
SHA256:	86016f9f3443fd0a79162579f2d359b1150e84182f9e3c162a2fb4932ccc2e23
SHA512:	e4969ecc71b1f364780eef72bc3d86641188af916ac06697aa03037b0d923e907ec94ea25bbfe3681da91985604f64d2da9f4155ee1b24bb054aadee2b4906e7
SSDEEP:	6144:gLV6Bta6dtJmakIM5sx/r1+Fw1VRQRnuDoPvEPWNSnswy:gLV6BtpmkHVYFSgRnrvEuNSW
TLSH:	0E24DF1A3BA8892FE2DE867D702212568779C2E3A8C3F3DF18D454B64F667E506071D3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.......PE..L....'.T.....~..... .....@.. .....

File Icon

Icon Hash:	90cecececе8e8eb0

Static PE Info

General

Entrypoint:	0x41e792
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE

DLL Characteristics:	
Time Stamp:	0x54E927A1 [Sun Feb 22 00:49:37 2015 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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1e738	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x22000	0x17a78	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x20000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1c798	0x1c800	False	0.5945124040570176	data	6.598063137150476	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.reloc	0x20000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x22000	0x17a78	0x17c00	False	0.9967927631578948	data	7.997791309450557	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x22058	0x17a20	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3192.169.69.26 4970061715202501905/29/23-13:46:57.708417	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49700	61715	192.168.2.3	192.169.69.26
192.168.2.3192.169.69.26 4970861715202501905/29/23-13:48:20.994121	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49708	61715	192.168.2.3	192.169.69.26
192.168.2.3192.169.69.26 4970761715202501905/29/23-13:48:15.596900	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49707	61715	192.168.2.3	192.169.69.26
192.168.2.3192.169.69.26 4970161715202501905/29/23-13:47:03.125196	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49701	61715	192.168.2.3	192.169.69.26
192.168.2.3192.169.69.26 4970661715202501905/29/23-13:48:10.004732	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49706	61715	192.168.2.3	192.169.69.26
192.168.2.3192.169.69.26 4970261715202501905/29/23-13:47:09.127331	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49702	61715	192.168.2.3	192.169.69.26

Network Port Distribution

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 29, 2023 13:46:57.226466894 CEST	49700	61715	192.168.2.3	192.169.69.26
May 29, 2023 13:46:57.637429953 CEST	61715	49700	192.169.69.26	192.168.2.3
May 29, 2023 13:46:57.640563965 CEST	49700	61715	192.168.2.3	192.169.69.26
May 29, 2023 13:46:57.708416939 CEST	49700	61715	192.168.2.3	192.169.69.26
May 29, 2023 13:46:58.137830973 CEST	61715	49700	192.169.69.26	192.168.2.3
May 29, 2023 13:47:02.455513954 CEST	49701	61715	192.168.2.3	192.169.69.26
May 29, 2023 13:47:03.122101068 CEST	61715	49701	192.169.69.26	192.168.2.3
May 29, 2023 13:47:03.122229099 CEST	49701	61715	192.168.2.3	192.169.69.26
May 29, 2023 13:47:03.125195980 CEST	49701	61715	192.168.2.3	192.169.69.26
May 29, 2023 13:47:03.630732059 CEST	61715	49701	192.169.69.26	192.168.2.3
May 29, 2023 13:47:08.459780931 CEST	49702	61715	192.168.2.3	192.169.69.26
May 29, 2023 13:47:09.124166965 CEST	61715	49702	192.169.69.26	192.168.2.3
May 29, 2023 13:47:09.126477957 CEST	49702	61715	192.168.2.3	192.169.69.26
May 29, 2023 13:47:09.127331018 CEST	49702	61715	192.168.2.3	192.169.69.26
May 29, 2023 13:47:09.630583048 CEST	61715	49702	192.169.69.26	192.168.2.3
May 29, 2023 13:47:13.779561043 CEST	49703	61715	192.168.2.3	212.193.30.230
May 29, 2023 13:47:16.791878939 CEST	49703	61715	192.168.2.3	212.193.30.230
May 29, 2023 13:47:22.808032036 CEST	49703	61715	192.168.2.3	212.193.30.230
May 29, 2023 13:47:31.846654892 CEST	49704	61715	192.168.2.3	212.193.30.230
May 29, 2023 13:47:34.856089115 CEST	49704	61715	192.168.2.3	212.193.30.230
May 29, 2023 13:47:40.856447935 CEST	49704	61715	192.168.2.3	212.193.30.230
May 29, 2023 13:47:50.429981947 CEST	49705	61715	192.168.2.3	212.193.30.230
May 29, 2023 13:47:53.435672045 CEST	49705	61715	192.168.2.3	212.193.30.230
May 29, 2023 13:47:59.436348915 CEST	49705	61715	192.168.2.3	212.193.30.230
May 29, 2023 13:48:09.419836998 CEST	49706	61715	192.168.2.3	192.169.69.26
May 29, 2023 13:48:09.991420031 CEST	61715	49706	192.169.69.26	192.168.2.3
May 29, 2023 13:48:09.991580009 CEST	49706	61715	192.168.2.3	192.169.69.26
May 29, 2023 13:48:10.004731894 CEST	49706	61715	192.168.2.3	192.169.69.26
May 29, 2023 13:48:10.499377012 CEST	61715	49706	192.169.69.26	192.168.2.3
May 29, 2023 13:48:14.860579014 CEST	49707	61715	192.168.2.3	192.169.69.26
May 29, 2023 13:48:15.490601063 CEST	61715	49707	192.169.69.26	192.168.2.3
May 29, 2023 13:48:15.490741014 CEST	49707	61715	192.168.2.3	192.169.69.26
May 29, 2023 13:48:15.596899986 CEST	49707	61715	192.168.2.3	192.169.69.26
May 29, 2023 13:48:16.006156921 CEST	61715	49707	192.169.69.26	192.168.2.3
May 29, 2023 13:48:20.447710991 CEST	49708	61715	192.168.2.3	192.169.69.26
May 29, 2023 13:48:20.992687941 CEST	61715	49708	192.169.69.26	192.168.2.3
May 29, 2023 13:48:20.993057013 CEST	49708	61715	192.168.2.3	192.169.69.26
May 29, 2023 13:48:20.994121075 CEST	49708	61715	192.168.2.3	192.169.69.26
May 29, 2023 13:48:21.497798920 CEST	61715	49708	192.169.69.26	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 29, 2023 13:48:25.979818106 CEST	49709	61715	192.168.2.3	212.193.30.230
May 29, 2023 13:48:28.978722095 CEST	49709	61715	192.168.2.3	212.193.30.230
May 29, 2023 13:48:34.981157064 CEST	49709	61715	192.168.2.3	212.193.30.230
May 29, 2023 13:48:51.351829052 CEST	49710	61715	192.168.2.3	212.193.30.230
May 29, 2023 13:48:54.343498945 CEST	49710	61715	192.168.2.3	212.193.30.230
May 29, 2023 13:49:00.357142925 CEST	49710	61715	192.168.2.3	212.193.30.230

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 29, 2023 13:46:57.090930939 CEST	52387	53	192.168.2.3	8.8.8.8
May 29, 2023 13:46:57.204461098 CEST	53	52387	8.8.8.8	192.168.2.3
May 29, 2023 13:47:02.331147909 CEST	56924	53	192.168.2.3	8.8.8.8
May 29, 2023 13:47:02.453748941 CEST	53	56924	8.8.8.8	192.168.2.3
May 29, 2023 13:47:08.427948952 CEST	60625	53	192.168.2.3	8.8.8.8
May 29, 2023 13:47:08.456681013 CEST	53	60625	8.8.8.8	192.168.2.3
May 29, 2023 13:47:13.741415977 CEST	49302	53	192.168.2.3	8.8.8.8
May 29, 2023 13:47:13.776850939 CEST	53	49302	8.8.8.8	192.168.2.3
May 29, 2023 13:47:31.807533026 CEST	53975	53	192.168.2.3	8.8.8.8
May 29, 2023 13:47:31.843962908 CEST	53	53975	8.8.8.8	192.168.2.3
May 29, 2023 13:47:50.407968044 CEST	51139	53	192.168.2.3	8.8.8.8
May 29, 2023 13:47:50.427670002 CEST	53	51139	8.8.8.8	192.168.2.3
May 29, 2023 13:48:09.305305004 CEST	52955	53	192.168.2.3	8.8.8.8
May 29, 2023 13:48:09.418483973 CEST	53	52955	8.8.8.8	192.168.2.3
May 29, 2023 13:48:14.829972029 CEST	60582	53	192.168.2.3	8.8.8.8
May 29, 2023 13:48:14.858628035 CEST	53	60582	8.8.8.8	192.168.2.3
May 29, 2023 13:48:20.426019907 CEST	57134	53	192.168.2.3	8.8.8.8
May 29, 2023 13:48:20.446468115 CEST	53	57134	8.8.8.8	192.168.2.3
May 29, 2023 13:48:25.943614960 CEST	62050	53	192.168.2.3	8.8.8.8
May 29, 2023 13:48:25.978658915 CEST	53	62050	8.8.8.8	192.168.2.3
May 29, 2023 13:48:51.321815014 CEST	56042	53	192.168.2.3	8.8.8.8
May 29, 2023 13:48:51.350569010 CEST	53	56042	8.8.8.8	192.168.2.3

DNS Queries

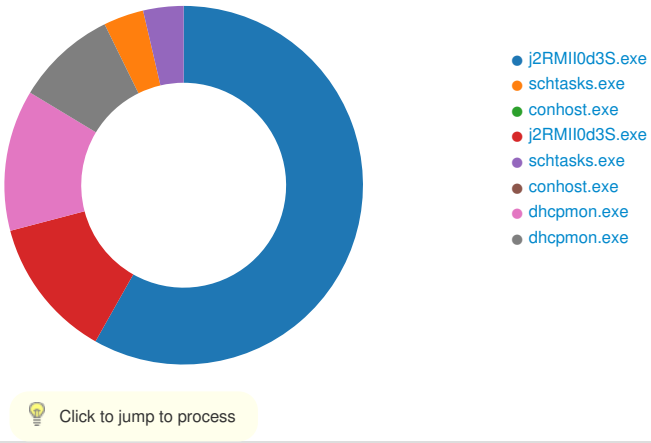
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
May 29, 2023 13:46:57.090930939 CEST	192.168.2.3	8.8.8.8	0x428f	Standard query (0)	december2n.duckdns.org	A (IP address)	IN (0x0001)	false
May 29, 2023 13:47:02.331147909 CEST	192.168.2.3	8.8.8.8	0xd84f	Standard query (0)	december2n.duckdns.org	A (IP address)	IN (0x0001)	false
May 29, 2023 13:47:08.427948952 CEST	192.168.2.3	8.8.8.8	0xd316	Standard query (0)	december2n.duckdns.org	A (IP address)	IN (0x0001)	false
May 29, 2023 13:47:13.741415977 CEST	192.168.2.3	8.8.8.8	0x4ea3	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
May 29, 2023 13:47:31.807533026 CEST	192.168.2.3	8.8.8.8	0x1312	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
May 29, 2023 13:47:50.407968044 CEST	192.168.2.3	8.8.8.8	0xaa9b	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
May 29, 2023 13:48:09.305305004 CEST	192.168.2.3	8.8.8.8	0x3e7a	Standard query (0)	december2n.duckdns.org	A (IP address)	IN (0x0001)	false
May 29, 2023 13:48:14.829972029 CEST	192.168.2.3	8.8.8.8	0x11c	Standard query (0)	december2n.duckdns.org	A (IP address)	IN (0x0001)	false
May 29, 2023 13:48:20.426019907 CEST	192.168.2.3	8.8.8.8	0x7d29	Standard query (0)	december2n.duckdns.org	A (IP address)	IN (0x0001)	false
May 29, 2023 13:48:25.943614960 CEST	192.168.2.3	8.8.8.8	0xe43f	Standard query (0)	december2nd.ddns.net	A (IP address)	IN (0x0001)	false
May 29, 2023 13:48:51.321815014 CEST	192.168.2.3	8.8.8.8	0xc25c	Standard query (0)	december2nd.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
May 29, 2023 13:46:57.204461098 CEST	8.8.8.8	192.168.2.3	0x428f	No error (0)	december2n.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
May 29, 2023 13:47:02.453748941 CEST	8.8.8.8	192.168.2.3	0xd84f	No error (0)	december2n.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
May 29, 2023 13:47:08.456681013 CEST	8.8.8.8	192.168.2.3	0xd316	No error (0)	december2n.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
May 29, 2023 13:47:13.776850939 CEST	8.8.8.8	192.168.2.3	0x4ea3	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
May 29, 2023 13:47:31.843962908 CEST	8.8.8.8	192.168.2.3	0x1312	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
May 29, 2023 13:47:50.427670002 CEST	8.8.8.8	192.168.2.3	0xaa9b	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
May 29, 2023 13:48:09.418483973 CEST	8.8.8.8	192.168.2.3	0x3e7a	No error (0)	december2n.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
May 29, 2023 13:48:14.858628035 CEST	8.8.8.8	192.168.2.3	0x11c	No error (0)	december2n.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
May 29, 2023 13:48:20.446468115 CEST	8.8.8.8	192.168.2.3	0x7d29	No error (0)	december2n.duckdns.org		192.169.69.26	A (IP address)	IN (0x0001)	false
May 29, 2023 13:48:25.978658915 CEST	8.8.8.8	192.168.2.3	0xe43f	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false
May 29, 2023 13:48:51.350569010 CEST	8.8.8.8	192.168.2.3	0xc25c	No error (0)	december2nd.ddns.net		212.193.30.230	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: j2RMII0d3S.exe PID: **6024**, Parent PID: **3452**

General

Target ID:	0
Start time:	13:46:53

Start date:	29/05/2023
Path:	C:\Users\user\Desktop\j2RMII0d3S.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\j2RMII0d3S.exe
Imagebase:	0x890000
File size:	215040 bytes
MD5 hash:	ADB719D2A3C51A77AB1ED355F91D3CA2
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: 00000000.00000000.350824921.0000000000892000.00000002.00000001.01000000.00000003.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000000.350824921.0000000000892000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000000.350824921.0000000000892000.00000002.00000001.01000000.00000003.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000000.350824921.0000000000892000.00000002.00000001.01000000.00000003.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.622206945.0000000005CB0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.622206945.0000000005CB0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.622206945.0000000005CB0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000000.00000002.622206945.0000000005CB0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.622206945.0000000005CB0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.622179477.0000000005CA0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.622179477.0000000005CA0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000000.00000002.622179477.0000000005CA0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.622179477.0000000005CA0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.618336015.00000000030A1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.621912046.0000000005450000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.621912046.0000000005450000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000000.00000002.621912046.0000000005450000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.621912046.0000000005450000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C6560AC	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	6C6560AC	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	52C0D15	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	52C0E0F	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	52C0D15	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	52C1094	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	52C1094	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp8D81.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	52C1290	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	52C0E0F	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp8EDA.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	52C1290	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	52C0D15	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	52C0D15	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6C6560AC	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	6C6560AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\j2RMII0d3S.exe:Zone.Identifier	success or wait	1	52C1625	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	fd 36 49 85 60 fd 48	6I`H	success or wait	1	52C0FC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 27 fd 54 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 06 00 00 fd 01 00 00 7e 01 00 00 00 00 00 fd fd 01 00 00 20 00 00 00 00 02 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 03 00 00 02 00 00 00 00 00 00 02 00 00 00 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'T~ @	success or wait	2	52C1094	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	52C1094	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp8D81.tmp	0	1300	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	52C0FC7	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	0	37	43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 44 65 73 6b 74 6f 70 5c 6a 32 52 4d 49 49 30 64 33 53 2e 65 78 65	C:\Users\user\Desktop\j2RMII0d3S.exe	success or wait	1	52C0FC7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8EDA.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	52C0FC7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C685544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6C685544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C688738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6C72BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6C72BF06	unknown
C:\Users\user\Desktop\j2RMII0d3S.exe	unknown	4096	success or wait	1	6C72BF06	unknown
C:\Users\user\Desktop\j2RMII0d3S.exe	unknown	512	success or wait	1	6C72BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C685544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	6C685544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	52C0FC7	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	52C1186	RegSetValueExW

Analysis Process: schtasks.exe PID: **5696**, Parent PID: **6024**

General

Target ID:	1
Start time:	13:46:54
Start date:	29/05/2023
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\tmp8D81.tmp
Imagebase:	0x1240000
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\tmp8D81.tmp	unknown	2	success or wait	1	124AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp8D81.tmp	unknown	1301	success or wait	1	124ABD9	ReadFile

Analysis Process: conhost.exe PID: **5732**, Parent PID: **5696**

General

Target ID:	2
Start time:	13:46:54
Start date:	29/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: j2RMII0d3S.exe PID: **5724**, Parent PID: **1080**

General

Target ID:	3
Start time:	13:46:54
Start date:	29/05/2023
Path:	C:\Users\user\Desktop\j2RMII0d3S.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\j2RMII0d3S.exe 0
Imagebase:	0x9c0000
File size:	215040 bytes
MD5 hash:	ADB719D2A3C51A77AB1ED355F91D3CA2
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: 00000003.00000002.367779928.0000000003F91000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.367779928.0000000003F91000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.367779928.0000000003F91000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.367695665.0000000002F91000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.367695665.0000000002F91000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.367695665.0000000002F91000.00000004.00000800.00020000.00000000.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	6C6560AC	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	6C6560AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\j2RMII0d3S.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C6434A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\j2RMII0d3S.exe.log	0	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",03,"	success or wait	1	6C92A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C685544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6C685544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C688738	ReadFile

Analysis Process: schtasks.exe PID: **5720**, Parent PID: **6024**

General	
Target ID:	4
Start time:	13:46:54
Start date:	29/05/2023
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\tmp8EDA.tmp
Imagebase:	0x1240000
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\tmp8EDA.tmp	unknown	2	success or wait	1	124AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp8EDA.tmp	unknown	1311	success or wait	1	124ABD9	ReadFile

Analysis Process: conhost.exe PID: **2576**, Parent PID: **5720**

General	
Target ID:	5
Start time:	13:46:55
Start date:	29/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: **2068**, Parent PID: **1080**

General	
Target ID:	6
Start time:	13:46:57
Start date:	29/05/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0xc10000
File size:	215040 bytes
MD5 hash:	ADB719D2A3C51A77AB1ED355F91D3CA2
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: 00000006.00000002.372099535.0000000003281000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.372099535.0000000003281000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000002.372099535.0000000003281000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: unknown
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 97%, 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	6C6560AC	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	6C6560AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6C6434A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	0	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",03,"	success or wait	1	6C92A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C685544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6C685544	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C688738	ReadFile

Analysis Process: dhcpmon.exe PID: **2764**, Parent PID: **3452**

General

Target ID:	7
Start time:	13:47:02
Start date:	29/05/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0xd10000
File size:	215040 bytes
MD5 hash:	ADB719D2A3C51A77AB1ED355F91D3CA2
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	6C6560AC	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	6C6560AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C685544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	6C685544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	6C688738	ReadFile

Disassembly

No disassembly