ID: 507942
Sample Name:
E9sAsVQHNI.exe
Cookbook: default.jbs
Time: 23:15:46
Date: 22/10/2021
Version: 33.0.0 White Diamond

Table of Contents

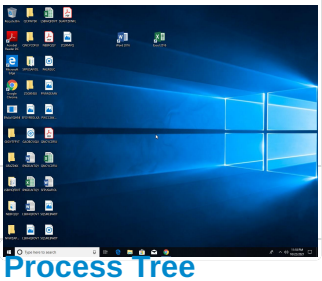
Windows Analysis Report E9sAsVQHNI.exe

Overview

General Information

Sample Name:	E9sAsVQHNI.exe
Analysis ID:	507942
MD5:	12897cc89f6a46e..
SHA1:	6b3d478c2895cc…
SHA256:	f7943cf69c4834c…
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

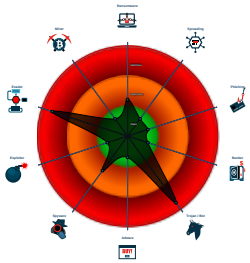
Nanocore

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
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Tries to detect sandboxes and other…
- Injects a PE file into a foreign proce…
- Sigma detected: Powershell Defende…
- Adds a directory exclusion to Windo…
- Hides that the sample has been dow…

Classification



Process Tree

- **System is w10x64**
- E9sAsVQHNI.exe (PID: 2208 cmdline: 'C:\Users\user\Desktop\E9sAsVQHNI.exe' MD5: 12897CC89F6A46E25F9D5445E9299003)
  - powershell.exe (PID: 3116 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\E9sAsVQHNI.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 1368 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 3512 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\VJGIel' /XML 'C:\Users\user\AppData\Local\Temp\tmp618B.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5876 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - E9sAsVQHNI.exe (PID: 5916 cmdline: C:\Users\user\Desktop\E9sAsVQHNI.exe MD5: 12897CC89F6A46E25F9D5445E9299003)
- dhcpmon.exe (PID: 4904 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 12897CC89F6A46E25F9D5445E9299003)
  - powershell.exe (PID: 6216 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6384 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 2240 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\VJGIel' /XML 'C:\Users\user\AppData\Local\Temp\tmpD9.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6032 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 6020 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 12897CC89F6A46E25F9D5445E9299003)
  - dhcpmon.exe (PID: 5208 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 12897CC89F6A46E25F9D5445E9299003)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.780712036.000000000494 4000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1047d:$x1: NanoCore.ClientPluginHost • 0x104ba:$x2: IClientNetworkHost • 0x13fed:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Source	Rule	Description	Author	Strings
0000000D.00000002.780712036.000000000494 4000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000D.00000002.780712036.000000000494 4000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x101e5:$a: NanoCore • 0x101f5:$a: NanoCore • 0x10429:$a: NanoCore • 0x1043d:$a: NanoCore • 0x1047d:$a: NanoCore • 0x10244:$b: ClientPlugin • 0x10446:$b: ClientPlugin • 0x10486:$b: ClientPlugin • 0x1036b:$c: ProjectData • 0x10d72:$d: DESCrypto • 0x1873e:$e: KeepAlive • 0x1672c:$g: LogClientMessage • 0x12927:$i: get_Connected • 0x110a8:$j: #=q • 0x110d8:$j: #=q • 0x110f4:$j: #=q • 0x11124:$j: #=q • 0x11140:$j: #=q • 0x1115c:$j: #=q • 0x1118c:$j: #=q • 0x111a8:$j: #=q
00000009.00000002.948337416.00000000051E 0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000009.00000002.948337416.00000000051E 0000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
Click to see the 58 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.E9sAsVQHNI.exe.39f458d.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0x23c50:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost • 0x23c7d:$x2: IClientNetworkHost
9.2.E9sAsVQHNI.exe.39f458d.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xb184:$x2: NanoCore.ClientPluginHost • 0x23c50:$x2: NanoCore.ClientPluginHost • 0xc25f:$s4: PipeCreated • 0x24d2b:$s4: PipeCreated • 0xb19e:$s5: IClientLoggingHost • 0x23c6a:$s5: IClientLoggingHost
9.2.E9sAsVQHNI.exe.39f458d.3.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
19.2.dhcpmon.exe.38f458d.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0x23c50:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost • 0x23c7d:$x2: IClientNetworkHost
19.2.dhcpmon.exe.38f458d.4.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xb184:$x2: NanoCore.ClientPluginHost • 0x23c50:$x2: NanoCore.ClientPluginHost • 0xc25f:$s4: PipeCreated • 0x24d2b:$s4: PipeCreated • 0xb19e:$s5: IClientLoggingHost • 0x23c6a:$s5: IClientLoggingHost
Click to see the 96 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Networking:

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

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

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

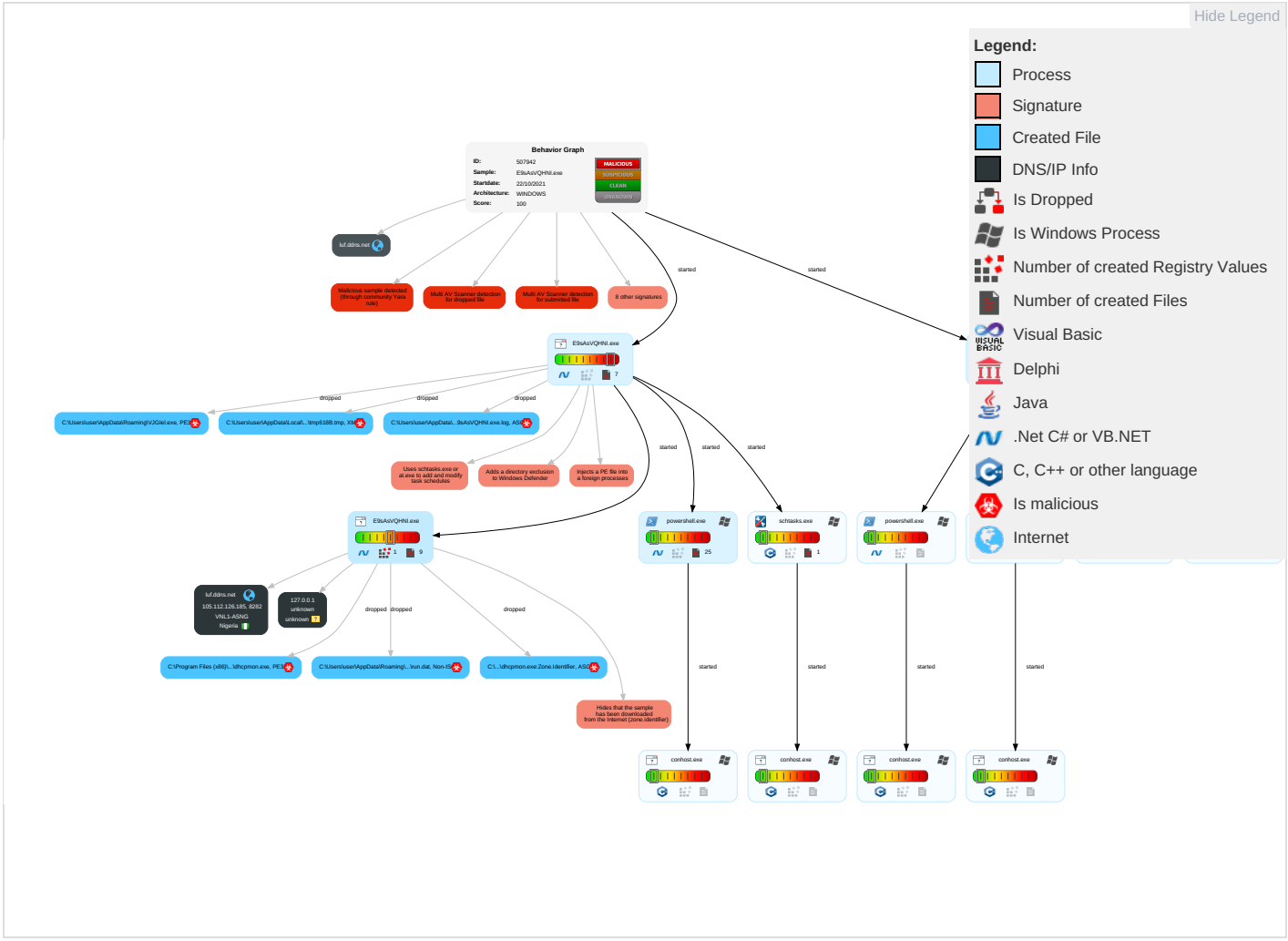
Detected Nanocore Rat

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	Netwo Effect
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 2	Input Capture 2 1	Query Registry 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	DLL Side-Loading 1	Scheduled Task/Job 1	Disable or Modify Tools 1 1	LSASS Memory	Security Software Discovery 2 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	System Information Discovery 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	DLL Side-Loading 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

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
E9sAsVQHNI.exe	43%	Virustotal		Browse
E9sAsVQHNI.exe	51%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	43%	Virustotal		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	51%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\VJGIel.exe	51%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
19.0.dhcpmon.exe.400000.5.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
19.0.dhcpmon.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
19.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
19.0.dhcpmon.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.2.E9sAsVQHNI.exe.53d0000.9.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Source	Detection	Scanner	Label	Link	Download
9.0.E9sAsVQHNI.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.E9sAsVQHNI.exe.400000.5.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.E9sAsVQHNI.exe.400000.7.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.E9sAsVQHNI.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.2.E9sAsVQHNI.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
19.0.dhcpmon.exe.400000.7.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://https://www.ShelteringOak.com/	0%	Virustotal		Browse
http://https://www.ShelteringOak.com/	0%	Avira URL Cloud	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	0%	URL Reputation	safe	
http://www.carterandcone.coml	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.founder.com.cn/cn	0%	URL Reputation	safe	
http://https://www.shelteringoak.com/dl/WindowsHealthCheck/version.txt	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://https://www.shelteringoak.com/dl/WindowsHealthCheck/WindowsHealthCheck.exe	2%	Virustotal		Browse
http://https://www.shelteringoak.com/dl/WindowsHealthCheck/WindowsHealthCheck.exe	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
luf.ddns.net	105.112.126.185	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
105.112.126.185	luf.ddns.net	Nigeria		36873	VNL1-ASNG	false

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	507942
Start date:	22.10.2021
Start time:	23:15:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 55s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	E9sAsVQHNI.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@20/17@6/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.3% (good quality ratio 0.3%) • Quality average: 71.5% • Quality standard deviation: 31.9%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
23:16:56	API Interceptor	871x Sleep call for process: E9sAsVQHNI.exe modified
23:17:03	API Interceptor	69x Sleep call for process: powershell.exe modified
23:17:16	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
23:17:28	API Interceptor	1x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

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\E9sAsVQHNI.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1090560
Entropy (8bit):	7.943530607154984
Encrypted:	false
SSDEEP:	24576:jWFOB6AlAlKal/zPsKuLubbXwUv8hzZhg3+TE/+PnyuXzhU:zB6Y1O3yAwUkhzXgOTaYnyq
MD5:	12897CC89F6A46E25F9D5445E9299003
SHA1:	6B3D478C2895CCCBF8BFD6135338E517BB20707C
SHA-256:	F7943CF69C4834C48A432C2A76CAA9EECC80FA9FFFDF5868277556C6D3FEFD64
SHA-512:	0BAA5D19AE88A4BAB3D512717E0EA27D6D3EDCD4EA67712E90C0D5B0013E3FE6315E138514FC4BB39F07AF27E58D669CA87EA7126EDF43990A44FAFA1D64514F
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 51%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....0.....j.... .....@.. ....@.....O..... ....H.....text...p.... ....`.rsrc.....@..@.reloc..... .....@..B.....L.....H.....(.....P...f.....0.....(.....a...%.(....o....o.....%.r...p.%...%.r...p.%...(....o.....(.....s.....+....o.....o.. .....X..j.o.....-..o.....,..o .....,..o ....*.....P.1.....A.N.....".(!....*....0.....a...%.r...p.%.r...p.%.r...p.%.r...p.%.r#..p.%.r)..p.%.r/..p.%.r5..p.%.r;..p...l...+...l#..... @[....X... ....j[.....i/.. ....j.....+....-.rA..p..f.....("....+...*....0.....

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\E9sAsVQHNI.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\E9sAsVQHNI.exe.log	
Process:	C:\Users\user\Desktop\E9sAsVQHNI.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\E9sAsVQHNI.exe.log	
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	unknown
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\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:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	false
Reputation:	unknown
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\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unknown
Category:	dropped
Size (bytes):	19660
Entropy (8bit):	5.577451911565371
Encrypted:	false
SSDEEP:	384:otADl+29nOzxRgSBKn+jul+OzoIptQ99V6NcgWM1M0Y0UP7zg:14K+ClncAKZINCp0AQ
MD5:	D09040BC52EF8F09555002BFD1A1F03E
SHA1:	F856C6282D9B6399F13523DC375A4AF607ED10E4
SHA-256:	FFA9712069B07F92A21ADC35EAD3288CD89B477CBA80AD3D6EF245AACA58AC81
SHA-512:	00177B912F44E3555A2FE5701EA198005FD0CEFE4A2A27F6A11A8ADFE0DE875544D9B53742A42319ACBC8EDA6A6DC1C39DAD99382AD187BA28EF713A2ABC34 4F
Malicious:	false
Reputation:	unknown
Preview:	@...e.....P.....u.....@.....H.....<@.^.L."My...::..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...]....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_bk5dfwdf.cpj.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_bk5dfwdf.cpj.ps1	
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_lnn0tieb.2xx.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unknown
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ntlvqwb3.ijv.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unknown
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_p122nr1e.bs4.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp618B.tmp	
Process:	C:\Users\user\Desktop\E9sAsVQHNI.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1639

C:\Users\user\AppData\Local\Temp\tmp618B.tmp	
Entropy (8bit):	5.1785032698281706
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjplgUYODOLD9RJh7h8gKBG1Btn:cbhK79lNQR/rydbz9l3YODOLNdq3S
MD5:	BAE07B8CB1F096A008E6F17AE20D6F7C
SHA1:	36C4C52F1DFDDEEAFDF117E728FCE37967A8FB48
SHA-256:	94830B7C7431D80B708060FC34DCCE160B0CD76338863EC1BF153FAE8F231E44
SHA-512:	2C19F035C9C2A6A7AE8E62FB15145DF5297938CF82A92698A541186E3E9DD534310BE15B111AAB3E5550FA1B95E552685C5F59C5DC7B15521C46715D8EAFA7A
Malicious:	**true**
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmpD9.tmp	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1639
Entropy (8bit):	5.1785032698281706
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjplgUYODOLD9RJh7h8gKBG1Btn:cbhK79lNQR/rydbz9l3YODOLNdq3S
MD5:	BAE07B8CB1F096A008E6F17AE20D6F7C
SHA1:	36C4C52F1DFDDEEAFDF117E728FCE37967A8FB48
SHA-256:	94830B7C7431D80B708060FC34DCCE160B0CD76338863EC1BF153FAE8F231E44
SHA-512:	2C19F035C9C2A6A7AE8E62FB15145DF5297938CF82A92698A541186E3E9DD534310BE15B111AAB3E5550FA1B95E552685C5F59C5DC7B15521C46715D8EAFA7A
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\E9sAsVQHNI.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:ju:y
MD5:	43CD6519880F95FCCA3B20D6F4161D97
SHA1:	9F259235B265DF2D6388BBDCE9ED89CC19741416
SHA-256:	C422AE2E7CCF6618CDC2107884B9AE4B7018EC0798C0928D927E09CDD516F72B
SHA-512:	3C1F335B7336EE42A80B9C8A60CE148AB7A8D2E8639654DAF7222A3F3CC30E13C3C946A5741C67AF70EEA40759AE7A2D67117481890391CD04EFC87F1D9E5B7C
Malicious:	**true**
Reputation:	unknown
Preview:	..O...H

C:\Users\user\AppData\Roaming\VJGIeI.exe	
Process:	C:\Users\user\Desktop\E9sAsVQHNI.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1090560
Entropy (8bit):	7.943530607154984
Encrypted:	false
SSDEEP:	24576:jWFOB6AlAlKal/zPsKuLubbXwUv8hzZhg3+TE/+PnyuXzhU:zB6Y1O3yAwUkhzXgOTaYnyq
MD5:	12897CC89F6A46E25F9D5445E9299003
SHA1:	6B3D478C2895CCCBF8BFD6135338E517BB20707C
SHA-256:	F7943CF69C4834C48A432C2A76CAA9EECC80FA9FFFDF5868277556C6D3FEFD64

C:\Users\user\AppData\Roaming\VJGIel.exe	
SHA-512:	0BAA5D19AE88A4BAB3D512717E0EA27D6D3EDCD4EA67712E90C0D5B0013E3FE6315E138514FC4BB39F07AF27E58D669CA87EA7126EDF43990A44FAFA1D6451 4F
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 51%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....0.....j.... .....@.. ....@.....O..... ....H.....text...p.... ....`.rsrc.....@..@.reloc..... .....@..B.....L.....H.....(.....P...f.....0.....(.....a...%.(....o....o.....%.r...p.%...%.r...p.%...(....o.....(....s.....+....o.....o.. .....X..j.o.....-..o.....,..o .....,..o ....*.....P.1.....A.N.....".(!....*....0.....a...%.r...p.%.r...p.%.r...p.%.r...p.%.r#..p.%.r)..p.%.r/..p.%.r5..p.%.r;..p...l...+...l#..... @[....X... ....j[.....i/.. ....j.....+....-.rA..p..f.....("....+...*....0.....

C:\Users\user\AppData\Roaming\VJGIel.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\E9sAsVQHNI.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
Malicious:	false
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20211022\PowerShell_transcript.609290.IkzwAfpe.20211022231731.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	Unknown
Category:	dropped
Size (bytes):	3691
Entropy (8bit):	5.22421762739372
Encrypted:	false
SSDEEP:	96:BZAjON0qDo1ZnZVjON0qDo1ZNVlzvOzGMzGMzwVZf:WvvyGgGgwn
MD5:	2155BD71FAB2F277F641A0725A5DA39E
SHA1:	518F35F4405C1605CEB10F59F3A4E9C4A1B914A2
SHA-256:	D1642701A21FC7E52A23F7A1A60B218ED548A93133EC5199B086F005D576D29B
SHA-512:	3221FA9F18DA7ACA6D2AEFC98B809174E3C50B122A38B881BAA742AF5DD4E647DBFB4317392BC40F84CFB007AFA32F1306249824864A207F9D29B0B45AC8FE5 6
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211022231732..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 609290 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference - ExclusionPath C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe..Process ID: 6216..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20211022231732..**********..PS>Add-MpPreference -ExclusionPath C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe..**********..Windows PowerShell transcript start..Start time: 20211022232251..Username: computer\user..RunAs User: co mputer\

C:\Users\user\Documents\20211022\PowerShell_transcript.609290.eNdXD_qN.20211022231702.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5733
Entropy (8bit):	5.397343890660485
Encrypted:	false
SSDEEP:	96:BZojONvGqDo1ZuYZCjONvGqDo1Zy7818j8jZ5jONvGqDo1ZPm8T8T8nZI:Fz0fq2F9IIT
MD5:	9F2C2F26B623E1B9FB378EF66A406AC9
SHA1:	9444CD15E72D3AC4217B45BE67A896D582DBD1B5
SHA-256:	2E8C54EA155C0B31FDA11154564CB7FC835076D8E2CA446D818063ED1E57B83F
SHA-512:	71DC246B93B7233F2F500B40F94F2228AA2C2297A2194DABDE6F07CEAAEAE3DF8C38518AE308E32DBCA155657CA2B4162A4D8A2D4A36F53F3DE597EC1F8C22 E2
Malicious:	false
Reputation:	unknown

C:\Users\user\Documents\20211022\PowerShell_transcript.609290.eNdXD_qN.20211022231702.txt	
Preview:	**********..Windows PowerShell transcript start..Start time: 20211022231703..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 609290 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\E9sAsVQHNI.exe..Process ID: 3116..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..********** **********..**********..Command start time: 20211022231703..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\E9sAsVQHNI.exe..**********..Windows PowerShell transcript start..Start time: 20211022232025..Username: computer\user..RunAs User: computer\user..Configuration

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.943530607154984
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	E9sAsVQHNI.exe
File size:	1090560
MD5:	12897cc89f6a46e25f9d5445e9299003
SHA1:	6b3d478c2895cccbf8bfd6135338e517bb20707c
SHA256:	f7943cf69c4834c48a432c2a76caa9eecc80fa9fffdf5868277556c6d3fefd64
SHA512:	0baa5d19ae88a4bab3d512717e0ea27d6d3edcd4ea6772e90c0d5b0013e3fe6315e138514fc4bb39f07af27e58d669ca87ea7126edf43990a44fafa1d64514f
SSDEEP:	24576:jWFOB6AlAlKal/zPsKuLubbXwUv8hzZhg3+TE/+PnyuXzhU:zB6Y1O3yAwUkhzXgOTaYnyq
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....0.....j.... ....@.. ..... @.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x50b76a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xFF629EA8 [Sat Oct 10 21:27:04 2105 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x109770	0x109800	False	0.953898341867	data	7.94856442088	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x10c000	0x6c4	0x800	False	0.36962890625	data	3.72331433617	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x10e000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 22, 2021 23:17:13.923624992 CEST	192.168.2.4	37.235.1.174	0xc417	Standard query (0)	luf.ddns.net	A (IP address)	IN (0x0001)
Oct 22, 2021 23:17:33.120450974 CEST	192.168.2.4	37.235.1.174	0x4cab	Standard query (0)	luf.ddns.net	A (IP address)	IN (0x0001)
Oct 22, 2021 23:17:51.312005997 CEST	192.168.2.4	37.235.1.174	0x9ee	Standard query (0)	luf.ddns.net	A (IP address)	IN (0x0001)
Oct 22, 2021 23:18:25.229526997 CEST	192.168.2.4	37.235.1.174	0xdb0c	Standard query (0)	luf.ddns.net	A (IP address)	IN (0x0001)
Oct 22, 2021 23:18:42.074781895 CEST	192.168.2.4	37.235.1.174	0xd609	Standard query (0)	luf.ddns.net	A (IP address)	IN (0x0001)
Oct 22, 2021 23:18:58.681713104 CEST	192.168.2.4	37.235.1.174	0xce97	Standard query (0)	luf.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 22, 2021 23:17:13.965949059 CEST	37.235.1.174	192.168.2.4	0xc417	No error (0)	luf.ddns.net		105.112.126.185	A (IP address)	IN (0x0001)
Oct 22, 2021 23:17:33.162286043 CEST	37.235.1.174	192.168.2.4	0x4cab	No error (0)	luf.ddns.net		105.112.126.185	A (IP address)	IN (0x0001)
Oct 22, 2021 23:17:51.353658915 CEST	37.235.1.174	192.168.2.4	0x9ee	No error (0)	luf.ddns.net		105.112.126.185	A (IP address)	IN (0x0001)
Oct 22, 2021 23:18:25.271047115 CEST	37.235.1.174	192.168.2.4	0xdb0c	No error (0)	luf.ddns.net		105.112.126.185	A (IP address)	IN (0x0001)
Oct 22, 2021 23:18:42.126657009 CEST	37.235.1.174	192.168.2.4	0xd609	No error (0)	luf.ddns.net		105.112.126.185	A (IP address)	IN (0x0001)
Oct 22, 2021 23:18:58.724258900 CEST	37.235.1.174	192.168.2.4	0xce97	No error (0)	luf.ddns.net		105.112.126.185	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: E9sAsVQHNI.exe PID: 2208 Parent PID: 3484

General

Start time:	23:16:49
Start date:	22/10/2021
Path:	C:\Users\user\Desktop\E9sAsVQHNI.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\E9sAsVQHNI.exe'
Imagebase:	0x110000
File size:	1090560 bytes
MD5 hash:	12897CC89F6A46E25F9D5445E9299003
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: 00000000.00000002.726746792.0000000003A24000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.726746792.0000000003A24000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.726746792.0000000003A24000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.722817180.00000000025B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.724435556.00000000035B9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.724435556.00000000035B9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.724435556.00000000035B9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 3116 Parent PID: 2208

General

Start time:	23:17:01
Start date:	22/10/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\E9sAsVQHNI.exe'
Imagebase:	0x1180000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 1368 Parent PID: 3116

General

Start time:	23:17:01
Start date:	22/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 3512 Parent PID: 2208

General

Start time:	23:17:02
Start date:	22/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\VJGIel' /XML 'C:\Users\user\AppData\Local\Temp\tmp618B.tmp'
Imagebase:	0x8e0000
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 Show Windows behavior

Analysis Process: conhost.exe PID: 5876 Parent PID: 3512

General

Start time:	23:17:03
Start date:	22/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: E9sAsVQHNI.exe PID: 5916 Parent PID: 2208

General

Start time:	23:17:03
Start date:	22/10/2021
Path:	C:\Users\user\Desktop\E9sAsVQHNI.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\E9sAsVQHNI.exe
Imagebase:	0x510000
File size:	1090560 bytes
MD5 hash:	12897CC89F6A46E25F9D5445E9299003
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: 00000009.00000002.948337416.00000000051E0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.948337416.00000000051E0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.716563336.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.716563336.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.716563336.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.947543722.00000000039E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.947543722.00000000039E9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.948515528.00000000053D0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.948515528.00000000053D0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.948515528.00000000053D0000.00000004.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.944512667.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.944512667.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.944512667.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.715559984.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.715559984.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.715559984.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.715990081.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.715990081.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.715990081.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities — Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities — Show Windows behavior

Key Value Created

Analysis Process: dhcpmon.exe PID: 4904 Parent PID: 3424

General

Start time:	23:17:24
Start date:	22/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xf90000
File size:	1090560 bytes
MD5 hash:	12897CC89F6A46E25F9D5445E9299003
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: 0000000D.00000002.780712036.0000000004944000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.780712036.0000000004944000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.780712036.0000000004944000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.779038136.00000000044D9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.779038136.00000000044D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.779038136.00000000044D9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000D.00000002.776167678.00000000034D1000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 43%, Virustotal, Browse • Detection: 51%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 6216 Parent PID: 4904

General

Start time:	23:17:30
Start date:	22/10/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x1180000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: 6384 Parent PID: 6216

General

Start time:	23:17:30
Start date:	22/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 2240 Parent PID: 4904

General

Start time:	23:17:30
Start date:	22/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\VJGIel' /XML 'C:\Users\user\AppData\Local\Temp\tmpD9.tmp'
Imagebase:	0x8e0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 6032 Parent PID: 2240

General

Start time:	23:17:31
Start date:	22/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6020 Parent PID: 4904

General

Start time:	23:17:31
Start date:	22/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false

Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x140000
File size:	1090560 bytes
MD5 hash:	12897CC89F6A46E25F9D5445E9299003
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: 5208 Parent PID: 4904

General

Start time:	23:17:32
Start date:	22/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x4d0000
File size:	1090560 bytes
MD5 hash:	12897CC89F6A46E25F9D5445E9299003
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: 00000013.00000000.770688814.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000000.770688814.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000000.770688814.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000000.771993806.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000000.771993806.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000000.771993806.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000000.770077209.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000000.770077209.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000000.770077209.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.797200941.00000000038A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.797200941.00000000038A9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.792430541.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.792430541.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.792430541.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.797105427.00000000028A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.797105427.00000000028A1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Disassembly

Code Analysis