ID: 527671
Sample Name: tj9KzQvUFy.exe
Cookbook: default.jbs
Time: 08:37:06
Date: 24/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Windows Analysis Report tj9KzQvUFy.exe

Overview

General Information

Sample Name:	tj9KzQvUFy.exe
Analysis ID:	527671
MD5:	e8ae42cfaafd650..
SHA1:	d4da7fb39e1ef6a..
SHA256:	c398ec8923c9de…
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:

Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

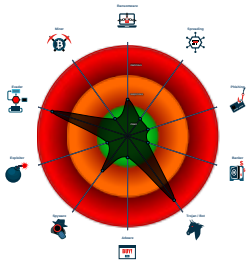
Nanocore

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

Signatures

- Snort IDS alert for network traffic (e.…
- 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…
- Sigma detected: Suspicius Add Tas…
- .NET source code contains potentia…
- Sigma detected: Powershell Defende…

Classification



Process Tree

- **System is w10x64**
- tj9KzQvUFy.exe (PID: 7016 cmdline: "C:\Users\user\Desktop\tj9KzQvUFy.exe" MD5: E8AE42CFAAFD650A14285AAF700D1F2B)
  - powershell.exe (PID: 6344 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\QWtzAVmnpKpJx.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6324 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6320 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\QWtzAVmnpKpJx" /XML "C:\Users\user\AppData\Local\Temp\tmp6B9E.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4680 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - tj9KzQvUFy.exe (PID: 6192 cmdline: C:\Users\user\Desktop\tj9KzQvUFy.exe MD5: E8AE42CFAAFD650A14285AAF700D1F2B)
    - schtasks.exe (PID: 6548 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmpC635.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6048 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6572 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmpCF6D.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6644 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- tj9KzQvUFy.exe (PID: 5776 cmdline: C:\Users\user\Desktop\tj9KzQvUFy.exe 0 MD5: E8AE42CFAAFD650A14285AAF700D1F2B)
  - powershell.exe (PID: 7064 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\QWtzAVmnpKpJx.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5420 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5724 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\QWtzAVmnpKpJx" /XML "C:\Users\user\AppData\Local\Temp\tmpB52A.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6328 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - tj9KzQvUFy.exe (PID: 1992 cmdline: C:\Users\user\Desktop\tj9KzQvUFy.exe MD5: E8AE42CFAAFD650A14285AAF700D1F2B)
  - tj9KzQvUFy.exe (PID: 4804 cmdline: C:\Users\user\Desktop\tj9KzQvUFy.exe MD5: E8AE42CFAAFD650A14285AAF700D1F2B)
- dhcpmon.exe (PID: 6732 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: E8AE42CFAAFD650A14285AAF700D1F2B)
- dhcpmon.exe (PID: 7072 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: E8AE42CFAAFD650A14285AAF700D1F2B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001B.00000002.448411736.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000001B.00000002.448411736.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000001B.00000002.448411736.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
00000009.00000000.377573313.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000009.00000000.377573313.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 65 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.tj9KzQvUFy.exe.6470000.8.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
9.2.tj9KzQvUFy.exe.6470000.8.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
9.2.tj9KzQvUFy.exe.6470000.8.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
1.2.tj9KzQvUFy.exe.2c617a8.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
9.0.tj9KzQvUFy.exe.400000.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Click to see the 122 entries

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Suspicius Add Task From User AppData Temp

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:

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

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

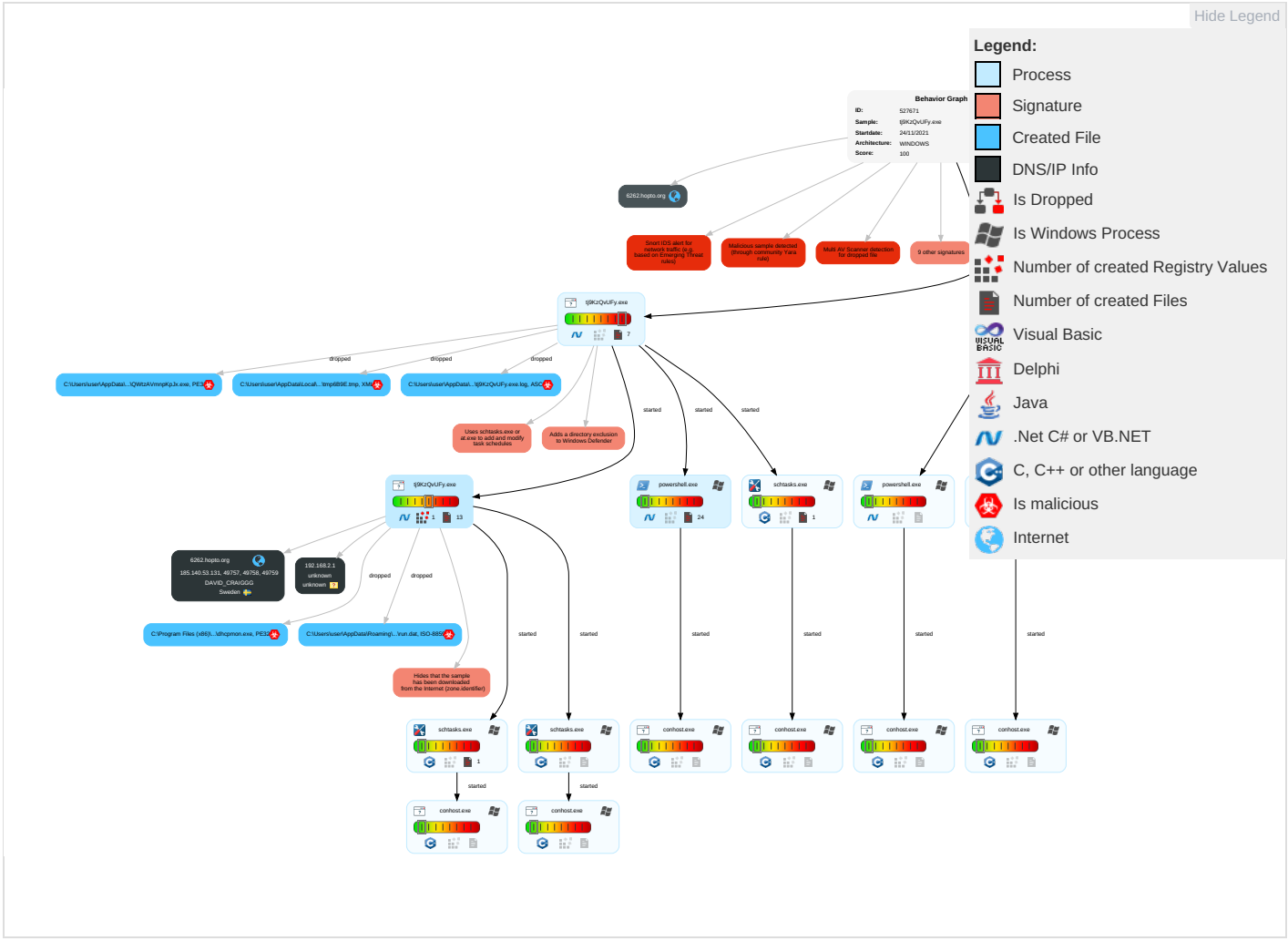
Detected Nanocore Rat

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	Network Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 2	Masquerading 2	Input Capture 2 1	Security Software Discovery 2 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdro Insecure Network Commun
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1	Manipula Device Commun
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocols

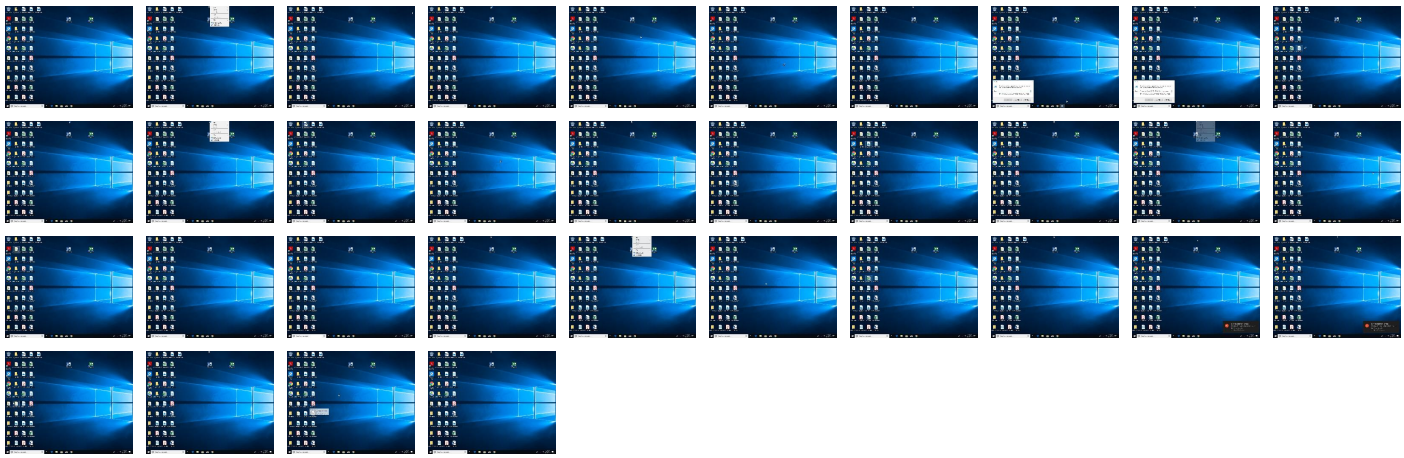
Behavior Graph



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
tj9KzQvUFy.exe	40%	Virustotal		Browse
tj9KzQvUFy.exe	57%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	57%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\QWtzAVmnpKpJx.exe	57%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
27.2.tj9KzQvUFy.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
27.0.tj9KzQvUFy.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.tj9KzQvUFy.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.2.tj9KzQvUFy.exe.6470000.8.unpack	100%	Avira	TR/NanoCore.fadte		Download File
27.0.tj9KzQvUFy.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
27.0.tj9KzQvUFy.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
27.0.tj9KzQvUFy.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.tj9KzQvUFy.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.tj9KzQvUFy.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
27.0.tj9KzQvUFy.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.tj9KzQvUFy.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.2.tj9KzQvUFy.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.tj9KzQvUFy.exe.400000.12.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.rbadams.com/Automation/Sequence	0%	Avira URL Cloud	safe	
http://www.rbadams.com/Automation/JobCollectionT	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.rbadams.com/Automation/ConfigurationT	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.rbadams.com/Automation/Job	0%	Avira URL Cloud	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.rbadams.com/Automation/JobQ	0%	Avira URL Cloud	safe	
http://www.rbadams.com/Automation/JobT	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.rbadams.com/Automation/JobCollectionN	0%	Avira URL Cloud	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.chinhdo.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.rbadams.com/Automation/JobCollectionK	0%	Avira URL Cloud	safe	
http://www.rbadams.com/Automation/JobD	0%	Avira URL Cloud	safe	
http://www.rbadams.com/Automation/PackageT	0%	Avira URL Cloud	safe	
http://www.rbadams.com/Automation/SequenceT	0%	Avira URL Cloud	safe	
http://www.rbadams.com/Automation/SequenceI	0%	Avira URL Cloud	safe	
http://www.rbadams.com/Automation/JobCollection	0%	Avira URL Cloud	safe	
http://www.rbadams.com/Automation/ISO	0%	Avira URL Cloud	safe	
http://www.rbadams.com/Automation/Configuration	0%	Avira URL Cloud	safe	
http://www.rbadams.com/Automation/PackageA	0%	Avira URL Cloud	safe	
http://www.rbadams.com/Automation/PackageH	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.rbadams.com/Automation/ISOT	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.rbadams.com/Automation/Configuration6	0%	Avira URL Cloud	safe	
http://www.rbadams.com/Automation/JobCollection#JobCollection.xsdKhttp://www.rbadams.com/Automation/	0%	Avira URL Cloud	safe	
http://www.rbadams.com/Automation/ISOD	0%	Avira URL Cloud	safe	
http://www.rbadams.com/Automation/Package	0%	Avira URL Cloud	safe	
http://www.rbadams.com/Automation/ISOG	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
6262.hopto.org	185.140.53.131	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.131	6262.hopto.org	Sweden		209623	DAVID_CRAIGGG	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	527671
Start date:	24.11.2021
Start time:	08:37:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 7s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	tj9KzQvUFy.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:	39
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@28/20@15/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • 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
08:38:10	API Interceptor	819x Sleep call for process: tj9KzQvUFy.exe modified
08:38:15	API Interceptor	67x Sleep call for process: powershell.exe modified
08:38:26	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\tj9KzQvUFy.exe" s>$(Arg0)
08:38:26	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
08:38:28	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
08:38:31	API Interceptor	2x 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\tj9KzQvUFy.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	656384
Entropy (8bit):	7.557907415976326
Encrypted:	false
SSDEEP:	12288:CBC1JfxsMZulg8mcbX9ON+iKFLfRcEvFU/vuRPAaQ:fxsMI2HN+LDGAFOuR
MD5:	E8AE42CFAAFD650A14285AAF700D1F2B
SHA1:	D4DA7FB39E1EF6AA56B01173EBB48FBD80ACB416
SHA-256:	C398EC8923C9DE2FE4FF2B9804F41663B1E929B22B3EE848576014F89663618A
SHA-512:	F035210CE60458C44925E88710D06EA51008A1174AD9B9C5D5FE39CD6875FC3662E537986D2487E91E8F17B9999F54C782D5EA6CB0A3E7561B03C7FEF5EFB724
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 57%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Q.a.....0..8.....V... ...`....@.. .....`..... ..@.....pV..O....`..L.....@..... ..... ..H.....text....6... ...8..... ..`.rsrc...L....`.....:.....@..@.rel oc.....@.....@..B.....V.....H.....dq..d..... .....Y.....{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*.0../.....(.....(!.....o"...(..... (#...(.....*F.(.....(.....*F.(.....(.....*J..(.....(.....*N...(.....(.....*".(.....*..{....*"..}....*&.(.....*F.(.....(.....*..{....*"..}....*F.(.....(.....*^.(.....}.....}....*..($.....s%...}.....s&...}.....}.....}.. ....}....*.0.. .....(.....,...{.....o'..

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\tj9KzQvUFy.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
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\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):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE47mE4Ko88:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz6
MD5:	D918C6A765EDB90D2A227FE23A3FEC98
SHA1:	8BA802AD8D740F114783F0DADC407CBFD2A209B3
SHA-256:	AB0E9F716E31502A4C6786575C5E64DFD9D24AF99056BBE2640A2FA322CFF4D6
SHA-512:	A937ABD8294BB32A612F8B3A376C94111D688379F0A4DB9FAA2FCEB71C25E18D621EEBCFDA5706B71C8473A4F38D8B3C4005D1589B564F9B1C9C441B6D3378 4
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\CLR_v4.0_32\UsageLogs\tj9KzQvUFy.exe.log	
Process:	C:\Users\user\Desktop\tj9KzQvUFy.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE47mE4Ko88:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz6
MD5:	D918C6A765EDB90D2A227FE23A3FEC98
SHA1:	8BA802AD8D740F114783F0DADC407CBFD2A209B3
SHA-256:	AB0E9F716E31502A4C6786575C5E64DFD9D24AF99056BBE2640A2FA322CFF4D6
SHA-512:	A937ABD8294BB32A612F8B3A376C94111D688379F0A4DB9FAA2FCEB71C25E18D621EEBCFDA5706B71C8473A4F38D8B3C4005D1589B564F9B1C9C441B6D3378 4
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\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22368
Entropy (8bit):	5.601656421547212
Encrypted:	false
SSDEEP:	384:VtCDCN0dVe3zsdNg90C+cVS0nEjultliDpaeQ99gtv7cxST1MaDZlbAV7nO6bS5M:n3zaNcjTECltdFat8xZCSfwYVk
MD5:	908EAC3BC9797FAA28DBB0402D7EBAB1

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
SHA1:	E2282CFA40FD83CAE6EC4B338F102A1F23B53B9C
SHA-256:	BBA6257BA15067DF4E23C9BAB8294CF37A471C195525C5BDCFDFC25563B1E7B2
SHA-512:	F22C3A986102873C9028FD7230F92A4B648A0B748849547A0EF9CBB9A89274711F7D1F0E4B26ABF93A0A8C4371A5CCC5A6DD2FCBA91435A294FA455D503F0ED
Malicious:	false
Reputation:	unknown
Preview:	@...e.....\...E.j.....@.....H.....<@.^.L."My...:P..... .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_1ahb5yvq.3r5.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
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_nodjwuc1.fnh.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__PSScriptPolicyTest_nuajyn5n.loo.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
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_tgnudcr1.dt0.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\tmp6B9E.tmp	
Process:	C:\Users\user\Desktop\tj9KzQvUFy.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	5.131364452417027
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1K2ky1mo2dUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtLi+xvn:cgea6YrFdOFzOzN33ODOiDdKrsuT+yv
MD5:	925190C2D78ECC86CF5154CCE6EBD9D4
SHA1:	EA86B51097422034A90129288EFCB2ACA009DFC3
SHA-256:	A55E12F841E438D6ABD5D348618D2322EE0CE5B533D570CBDDA2FA039ED1966E
SHA-512:	D1405C005192FF823537AC13BD48C4D942748B3B084E2638D37232555188B6EDAFD35A3F65946A1B8268D54152E69DC65DFAFB458708A48C581040C65FFDB34B
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</StartWhenAvailab

C:\Users\user\AppData\Local\Temp\tmpB52A.tmp	
Process:	C:\Users\user\Desktop\tj9KzQvUFy.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	5.131364452417027
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1K2ky1mo2dUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtLi+xvn:cgea6YrFdOFzOzN33ODOiDdKrsuT+yv
MD5:	925190C2D78ECC86CF5154CCE6EBD9D4
SHA1:	EA86B51097422034A90129288EFCB2ACA009DFC3
SHA-256:	A55E12F841E438D6ABD5D348618D2322EE0CE5B533D570CBDDA2FA039ED1966E
SHA-512:	D1405C005192FF823537AC13BD48C4D942748B3B084E2638D37232555188B6EDAFD35A3F65946A1B8268D54152E69DC65DFAFB458708A48C581040C65FFDB34B
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</StartWhenAvailab

C:\Users\user\AppData\Local\Temp\tmpC635.tmp	
Process:	C:\Users\user\Desktop\tj9KzQvUFy.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1303
Entropy (8bit):	5.118393522725328
Encrypted:	false

C:\Users\user\AppData\Local\Temp\tmpC635.tmp	
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Vk8xtn:cbk4oL600QydbQxIYODOLedq398j
MD5:	6EC593E46F7BEE4B30DD57AE5BAB2952
SHA1:	1BB562C3F8C681255432DE611B861228B452D592
SHA-256:	FA4649283C310D4CB5B284F9A502926920FBDC809D2779B61F0EC210C614A76B
SHA-512:	80E15A3185FEE61670524055910544BA7A51A350F97E5D9B542BE12E277B8023BFF80E77433C3036C899FFD39CB850BD5FBF1CF2C8CC2DDBAE7E3A389B448EC
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 />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpCF6D.tmp	
Process:	C:\Users\user\Desktop\tj9KzQvUFy.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
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 />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\tj9KzQvUFy.exe
File Type:	data
Category:	modified
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C356A5
Malicious:	false
Reputation:	unknown
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\tj9KzQvUFy.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:fL:D
MD5:	21450A64CFEC3970CF69AE13E3D9E3A4
SHA1:	BBDFE38F21DDC5BD006B95DA332449514DDFD9CB
SHA-256:	59835E723F60578EBDAF479249B29E20BB1EE34E38051A97316B2DE28D8C7E60

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
SHA-512:	10543C186E8209618F66CBA6C624B3FFB4DFCA746CD19660961A9EDB1DC1605A48BB2AC2265B3D246F1AC8D84FD95F1C9EEE5C15D0D4662D4A9E4D962FD0DAC
Malicious:	**true**
Reputation:	unknown
Preview:	.<..h..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\tj9KzQvUFy.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	40
Entropy (8bit):	4.311768795973195
Encrypted:	false
SSDEEP:	3:oNN2+WRP30z4An:oNN2R9K4An
MD5:	CF30FCEA281280CCA6A52A926336FCFD
SHA1:	20FD692C9E954DC6BEC262E4EB0D99BB02368CA2
SHA-256:	D9A538B7F915D5533151EF2E6E4ACADF4500FFE242CBA4991582E1F5B5441898
SHA-512:	C60027433E01198116F6C4A69A2AAD3897A4627645C12E9520D221386AC6988C4EED7BBEFAFA864AA54AB92BF114005B925B7899CD55C6D10315BA221B22F9C3
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\Desktop\tj9KzQvUFy.exe

C:\Users\user\AppData\Roaming\QWtzAVmnpKpJx.exe	
Process:	C:\Users\user\Desktop\tj9KzQvUFy.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	656384
Entropy (8bit):	7.557907415976326
Encrypted:	false
SSDEEP:	12288:CBC1JfxsMZulg8mcbX9ON+iKFLfRcEvFU/vuRPAaQ:fxsMI2HN+LDGAFOuR
MD5:	E8AE42CFAAFD650A14285AAF700D1F2B
SHA1:	D4DA7FB39E1EF6AA56B01173EBB48FBD80ACB416
SHA-256:	C398EC8923C9DE2FE4FF2B9804F41663B1E929B22B3EE848576014F89663618A
SHA-512:	F035210CE60458C44925E88710D06EA51008A1174AD9B9C5D5FE39CD6875FC3662E537986D2487E91E8F17B9999F54C782D5EA6CB0A3E7561B03C7FEF5EFB724
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 57%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Q.a.....0..8.....V... ...`....@.. .....`..... ..@.....pV..O....`..L.....@..... ..... ..H.....text....6... ...8..... ..`.rsrc...L....`.....:.....@..@.rel oc.....@.....@..B.....V.....H.....dq..d..... .....Y.....{....*"..}....*..{....*"..}....*..{....*"..}....*..{....*"..}....*.0../.....(.....(!.....o"...(..... (#...(.....*F.(.....(.....*F.(.....(.....*J..(.....(.....*N...(.....(.....*".(.....*..{....*"..}....*&.(.....*F.(.....(.....*..{....*"..}....*F.(.....(.....*^.(.....}.....}....*..($.....s%...}.....s&...}.....}.....}.. ....}....*.0.. .....(.....,...{.....o'..

C:\Users\user\AppData\Roaming\QWtzAVmnpKpJx.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\tj9KzQvUFy.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\20211124\PowerShell_transcript.364339.QLt3jixE.20211124083814.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped

C:\Users\user\Documents\20211124\PowerShell_transcript.364339.QLt3jixE.20211124083814.txt	
Size (bytes):	5831
Entropy (8bit):	5.381220662105565
Encrypted:	false
SSDEEP:	96:BZQTL6NyqDo1ZbZVTL6NyqDo1ZbzN7jZ2TL6NyqDo1ZkOrriZ5:m
MD5:	8A0E01BBF093912B164C9DC567CA73DB
SHA1:	E1CF369CEE596486CB3CD86C99DF372E37697402
SHA-256:	B73C0BF752A153BC02FCDE4BA57B6E50F56B48510DFC631254B0DD57FB23BB72
SHA-512:	F98FE2A6ED252B26C4DF6DF71C08A7AEF03BC6EB60B55A6CD8E1D0EA661075C0058F37BF4CCB8CB56254C1BC33C619010581570B1F1AE4EE06823A18CA3BAI 4C
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211124083815..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 364339 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\QWtzAVmnpKpJx.exe..Process ID: 6344..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: 20211124083815..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\QWtzAVmnpKpJx.exe..**********..Windows PowerShell transcript start..Start time: 20211124084134..Username: computer\user..RunAs User:

C:\Users\user\Documents\20211124\PowerShell_transcript.364339.eUfTHFx+.20211124083835.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):	5831
Entropy (8bit):	5.381836446497762
Encrypted:	false
SSDEEP:	96:BZyTL6NAqDo1Z9Z+pTL6NAqDo1ZnzN7jZ8TL6NAqDo1ZZOrrGZJ:pW
MD5:	A7B74313CCFD915447AACDDABD94D045
SHA1:	AC28C49C99D693D7EC07ACAC629CBA7906905D38
SHA-256:	57DB0B95119111E11B318DFA2082B7CF2C3B14675165CA617BEC6C55C5775EE7
SHA-512:	A0A0A3635F6A398DCDA8435F029B08C25AE23094632F8D2CD1C794701F969994735B87ED05E608EAA7EEAECDA2FA27E75EBCF60928B97DE5D4FED27071D382 0
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211124083840..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 364339 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\QWtzAVmnpKpJx.exe..Process ID: 7064..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: 20211124083840..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\QWtzAVmnpKpJx.exe..**********..Windows PowerShell transcript start..Start time: 20211124084256..Username: computer\user..RunAs User:

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.557907415976326
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:	tj9KzQvUFy.exe
File size:	656384
MD5:	e8ae42cfaafd650a14285aaf700d1f2b
SHA1:	d4da7fb39e1ef6aa56b01173ebb48fbd80acb416
SHA256:	c398ec8923c9de2fe4ff2b9804f41663b1e929b22b3ee848576014f89663618a
SHA512:	f035210ce60458c44925e88710d06ea51008a1174ad9b9c5d5fe39cd6875fc3662e537986d2487e91e8f17b9999f54c782d5ea6cb0a3e7561b03c7fef5efb724
SSDEEP:	12288:CBC1JfxsMZulg8mcbX9ON+iKFLfRcEvFU/vuRPAaQ:fxsMI2HN+LDGAFOuR

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Q.a.....0..8.....V... ...`....@.. .....`.....@.....

File Icon

Icon Hash:	e8868692b296f030

Static PE Info

General

Entrypoint:	0x4756c2
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:	0x6197519F [Fri Nov 19 07:26:23 2021 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	0x736d8	0x73800	False	0.932974414908	data	7.91653185027	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x76000	0x2c64c	0x2c800	False	0.270985121138	data	5.66808975489	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa4000	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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/24/21-08:38:29.508269	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49757	6262	192.168.2.6	185.140.53.131
11/24/21-08:38:36.025646	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49758	6262	192.168.2.6	185.140.53.131

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/24/21-08:38:45.099934	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60342	8.8.8.8	192.168.2.6
11/24/21-08:38:45.380386	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49759	6262	192.168.2.6	185.140.53.131
11/24/21-08:38:52.040276	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56023	8.8.8.8	192.168.2.6
11/24/21-08:38:52.292564	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49762	6262	192.168.2.6	185.140.53.131
11/24/21-08:38:59.173830	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60261	8.8.8.8	192.168.2.6
11/24/21-08:38:59.415917	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49766	6262	192.168.2.6	185.140.53.131
11/24/21-08:39:05.760961	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58336	8.8.8.8	192.168.2.6
11/24/21-08:39:05.972486	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49772	6262	192.168.2.6	185.140.53.131
11/24/21-08:39:13.011030	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49775	6262	192.168.2.6	185.140.53.131
11/24/21-08:39:19.940148	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49694	8.8.8.8	192.168.2.6
11/24/21-08:39:20.153679	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49795	6262	192.168.2.6	185.140.53.131
11/24/21-08:39:26.974417	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63718	8.8.8.8	192.168.2.6
11/24/21-08:39:27.210586	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49811	6262	192.168.2.6	185.140.53.131
11/24/21-08:39:34.151963	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49816	6262	192.168.2.6	185.140.53.131
11/24/21-08:39:42.384893	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49819	6262	192.168.2.6	185.140.53.131
11/24/21-08:39:49.673241	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49844	6262	192.168.2.6	185.140.53.131
11/24/21-08:39:56.347222	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51818	8.8.8.8	192.168.2.6
11/24/21-08:39:56.652893	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49845	6262	192.168.2.6	185.140.53.131
11/24/21-08:40:03.510735	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49847	6262	192.168.2.6	185.140.53.131
11/24/21-08:40:10.253712	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53799	8.8.8.8	192.168.2.6
11/24/21-08:40:11.184129	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49848	6262	192.168.2.6	185.140.53.131

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 24, 2021 08:38:29.175595999 CET	192.168.2.6	8.8.8.8	0xac6c	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 08:38:35.749134064 CET	192.168.2.6	8.8.8.8	0x88c4	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 08:38:45.078562975 CET	192.168.2.6	8.8.8.8	0xa4f2	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 08:38:52.018465996 CET	192.168.2.6	8.8.8.8	0xae6d	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 08:38:59.152193069 CET	192.168.2.6	8.8.8.8	0xe677	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 08:39:05.738451004 CET	192.168.2.6	8.8.8.8	0x81df	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 08:39:12.781300068 CET	192.168.2.6	8.8.8.8	0x81cc	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 08:39:19.918241978 CET	192.168.2.6	8.8.8.8	0xd31f	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 24, 2021 08:39:26.954230070 CET	192.168.2.6	8.8.8.8	0x2f18	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 08:39:33.915369034 CET	192.168.2.6	8.8.8.8	0x5a22	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 08:39:42.152251959 CET	192.168.2.6	8.8.8.8	0x23ce	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 08:39:49.306451082 CET	192.168.2.6	8.8.8.8	0x8d88	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 08:39:56.327341080 CET	192.168.2.6	8.8.8.8	0x28b9	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 08:40:03.282618046 CET	192.168.2.6	8.8.8.8	0x7f35	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 08:40:10.232549906 CET	192.168.2.6	8.8.8.8	0x8f60	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 24, 2021 08:38:29.193285942 CET	8.8.8.8	192.168.2.6	0xac6c	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 08:38:35.768896103 CET	8.8.8.8	192.168.2.6	0x88c4	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 08:38:45.099934101 CET	8.8.8.8	192.168.2.6	0xa4f2	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 08:38:52.040276051 CET	8.8.8.8	192.168.2.6	0xae6d	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 08:38:59.173830032 CET	8.8.8.8	192.168.2.6	0xe677	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 08:39:05.760961056 CET	8.8.8.8	192.168.2.6	0x81df	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 08:39:12.802176952 CET	8.8.8.8	192.168.2.6	0x81cc	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 08:39:19.940148115 CET	8.8.8.8	192.168.2.6	0xd31f	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 08:39:26.974416971 CET	8.8.8.8	192.168.2.6	0x2f18	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 08:39:33.933423042 CET	8.8.8.8	192.168.2.6	0x5a22	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 08:39:42.169732094 CET	8.8.8.8	192.168.2.6	0x23ce	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 08:39:49.329001904 CET	8.8.8.8	192.168.2.6	0x8d88	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 08:39:56.347222090 CET	8.8.8.8	192.168.2.6	0x28b9	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 08:40:03.302814007 CET	8.8.8.8	192.168.2.6	0x7f35	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 08:40:10.253711939 CET	8.8.8.8	192.168.2.6	0x8f60	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: tj9KzQvUFy.exe PID: 7016 Parent PID: 2076

General

Start time:	08:38:02
Start date:	24/11/2021
Path:	C:\Users\user\Desktop\tj9KzQvUFy.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\tj9KzQvUFy.exe"
Imagebase:	0x880000
File size:	656384 bytes
MD5 hash:	E8AE42CFAAFD650A14285AAF700D1F2B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.380810422.0000000002C41000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.381024024.0000000002D5E000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.382063003.0000000003C49000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.382063003.0000000003C49000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.382063003.0000000003C49000.00000004.00000001.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: 6344 Parent PID: 7016

General

Start time:	08:38:13
Start date:	24/11/2021
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\AppData\Roaming\QWtzAVmnpKpJx.exe
Imagebase:	0xd30000
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: 6324 Parent PID: 6344

General

Start time:	08:38:13
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 6320 Parent PID: 7016

General

Start time:	08:38:13
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\QWtzAVmnpKpJx" /XML "C:\Users\user\AppData\Local\Temp\tmp6B9E.tmp
Imagebase:	0x810000
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

File Read

Analysis Process: conhost.exe PID: 4680 Parent PID: 6320

General

Start time:	08:38:14
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: tj9KzQvUFy.exe PID: 6192 Parent PID: 7016

General

Start time:	08:38:15
Start date:	24/11/2021
Path:	C:\Users\user\Desktop\tj9KzQvUFy.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\tj9KzQvUFy.exe
Imagebase:	0x960000
File size:	656384 bytes
MD5 hash:	E8AE42CFAAFD650A14285AAF700D1F2B
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: 00000009.00000000.377573313.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.377573313.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.377573313.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.610929952.0000000002CF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.607967437.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.607967437.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.607967437.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.370237715.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.370237715.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.370237715.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.378298727.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.378298727.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.378298727.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.613519812.0000000003CF9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.613519812.0000000003CF9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.376991452.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.376991452.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.376991452.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.615717844.00000000055F0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.615717844.00000000055F0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.616228293.0000000006470000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.616228293.0000000006470000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.616228293.0000000006470000.00000004.00020000.sdmp, Author: Joe Security
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: schtasks.exe PID: 6548 Parent PID: 6192

General

Start time:	08:38:24
Start date:	24/11/2021
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\tmpC635.tmp
Imagebase:	0x810000
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

File Read

Analysis Process: conhost.exe PID: 6048 Parent PID: 6548

General

Start time:	08:38:25
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: tj9KzQvUFy.exe PID: 5776 Parent PID: 936

General

Start time:	08:38:26
Start date:	24/11/2021
Path:	C:\Users\user\Desktop\tj9KzQvUFy.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\tj9KzQvUFy.exe 0
Imagebase:	0xaa0000
File size:	656384 bytes
MD5 hash:	E8AE42CFAAFD650A14285AAF700D1F2B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000E.00000002.435389639.0000000002FC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.437386781.0000000003FC9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.437386781.0000000003FC9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.437386781.0000000003FC9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000E.00000002.436014172.00000000030EB000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 6572 Parent PID: 6192

General

Start time:	08:38:26
Start date:	24/11/2021
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\tmpCF6D.tmp
Imagebase:	0x810000
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: 6644 Parent PID: 6572

General

Start time:	08:38:27
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 6732 Parent PID: 936

General

Start time:	08:38:29
Start date:	24/11/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0x5c0000
File size:	656384 bytes
MD5 hash:	E8AE42CFAAFD650A14285AAF700D1F2B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000011.00000002.405648724.0000000002AC1000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 57%, ReversingLabs
Reputation:	low

Analysis Process: dhcpmon.exe PID: 7072 Parent PID: 3440

General

Start time:	08:38:34
Start date:	24/11/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0x800000
File size:	656384 bytes
MD5 hash:	E8AE42CFAAFD650A14285AAF700D1F2B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000013.00000002.428142089.0000000002CC1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: powershell.exe PID: 7064 Parent PID: 5776

General

Start time:	08:38:34
Start date:	24/11/2021
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\AppData\Roaming\QWtzAVmnpKpJx.exe
Imagebase:	0xd30000
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: 5420 Parent PID: 7064

General

Start time:	08:38:34
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: 5724 Parent PID: 5776

General

Start time:	08:38:35
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\QWtzAVmnpKpJx" /XML "C:\Users\user\AppData\Local\Temp\tmpB52A.tmp
Imagebase:	0x810000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6328 Parent PID: 5724

General

Start time:	08:38:39
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: tj9KzQvUFy.exe PID: 1992 Parent PID: 5776

General

Start time:	08:38:41
Start date:	24/11/2021
Path:	C:\Users\user\Desktop\tj9KzQvUFy.exe
Wow64 process (32bit):	false

Commandline:	C:\Users\user\Desktop\tj9KzQvUFy.exe
Imagebase:	0x280000
File size:	656384 bytes
MD5 hash:	E8AE42CFAAFD650A14285AAF700D1F2B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: tj9KzQvUFy.exe PID: 4804 Parent PID: 5776

General

Start time:	08:38:42
Start date:	24/11/2021
Path:	C:\Users\user\Desktop\tj9KzQvUFy.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\tj9KzQvUFy.exe
Imagebase:	0xf60000
File size:	656384 bytes
MD5 hash:	E8AE42CFAAFD650A14285AAF700D1F2B
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: 0000001B.00000002.448411736.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000002.448411736.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000002.448411736.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000000.428587320.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000000.428587320.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000000.428587320.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000000.430610675.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000000.430610675.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000000.430610675.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000002.449720348.0000000004499000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000002.449720348.0000000004499000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000002.449610369.0000000003491000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000002.449610369.0000000003491000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000000.429163974.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000000.429163974.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000000.429163974.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001B.00000000.429929302.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000000.429929302.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000000.429929302.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Disassembly

Code Analysis