ID: 432674
Sample Name: pIjxtI0ZlU.exe
Cookbook: default.jbs
Time: 16:42:19
Date: 10/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

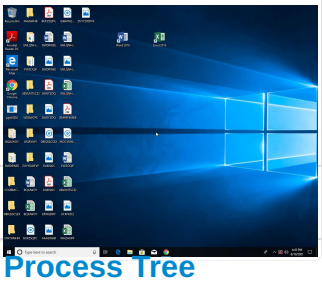
Analysis Report pIjxtI0ZlU.exe

Overview

General Information

Sample Name:	pIjxtI0ZlU.exe
Analysis ID:	432674
MD5:	a253962036d634..
SHA1:	769427fca217acc..
SHA256:	e6a6126a0e0da3..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

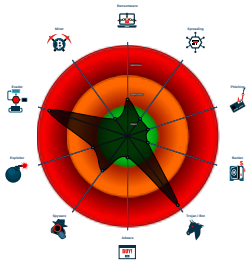
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Adds a directory exclusion to Windo…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- pIjxtI0ZlU.exe (PID: 5712 cmdline: 'C:\Users\user\Desktop\pIjxtI0ZlU.exe' MD5: A253962036D634B39E913BC0322584E5)
  - powershell.exe (PID: 5868 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\pIjxtI0ZlU.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5792 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 4624 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\cKGPEGrRS.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 64 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 4184 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\cKGPEGrRS' /XML 'C:\Users\user\AppData\Local\Temp\tmp6A8A.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1900 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 2860 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\cKGPEGrRS.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4204 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - pIjxtI0ZlU.exe (PID: 2208 cmdline: C:\Users\user\Desktop\pIjxtI0ZlU.exe MD5: A253962036D634B39E913BC0322584E5)
- dhcpmon.exe (PID: 6304 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: A253962036D634B39E913BC0322584E5)
  - powershell.exe (PID: 6432 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: 6440 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6448 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\cKGPEGrRS' /XML 'C:\Users\user\AppData\Local\Temp\tmpAF63.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6500 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 6584 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\cKGPEGrRS.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6596 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 6604 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: A253962036D634B39E913BC0322584E5)
  - dhcpmon.exe (PID: 6716 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: A253962036D634B39E913BC0322584E5)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "b90524a1-4a4b-41de-ac06-59066a86",
  "Group": "Panda",
  "Domain1": "emedoo.ddns.net",
  "Domain2": "127.0.0.1",
  "Port": 5230,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Enable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Enable",
  "EnableDebugMode": "Disable",
  "RunDelay": 50,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "emedoo.ddns.net",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.949190405.0000000006E90000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x59eb:$x1: NanoCore.ClientPluginHost • 0x5b48:$x2: IClientNetworkHost
00000009.00000002.949190405.0000000006E90000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x59eb:$x2: NanoCore.ClientPluginHost • 0x6941:$s3: PipeExists • 0x5be1:$s4: PipeCreated • 0x5a05:$s5: IClientLoggingHost
00000009.00000002.945200916.0000000005F30000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5fee:$x1: NanoCore.ClientPluginHost • 0x602b:$x2: IClientNetworkHost
00000009.00000002.945200916.0000000005F30000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x5fee:$x2: NanoCore.ClientPluginHost • 0x9441:$s4: PipeCreated • 0x6018:$s5: IClientLoggingHost
00000012.00000000.714388325.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Click to see the 65 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.pIjxtI0ZlU.exe.6e80000.32.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x13a8:$x1: NanoCore.ClientPluginHost
9.2.pIjxtI0ZlU.exe.6e80000.32.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x13a8:$x2: NanoCore.ClientPluginHost • 0x1486:$s4: PipeCreated • 0x13c2:$s5: IClientLoggingHost
9.2.pIjxtI0ZlU.exe.5f0e8a4.24.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x10937:$x1: NanoCore.ClientPluginHost • 0x10951:$x2: IClientNetworkHost
9.2.pIjxtI0ZlU.exe.5f0e8a4.24.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x10937:$x2: NanoCore.ClientPluginHost • 0x13c74:$s4: PipeCreated • 0x10924:$s5: IClientLoggingHost
9.2.pIjxtI0ZlU.exe.4362354.8.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x41ee:$x1: NanoCore.ClientPluginHost • 0x422b:$x2: IClientNetworkHost

Click to see the 172 entries

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Non Interactive PowerShell

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

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

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Adds a directory exclusion to Windows Defender

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

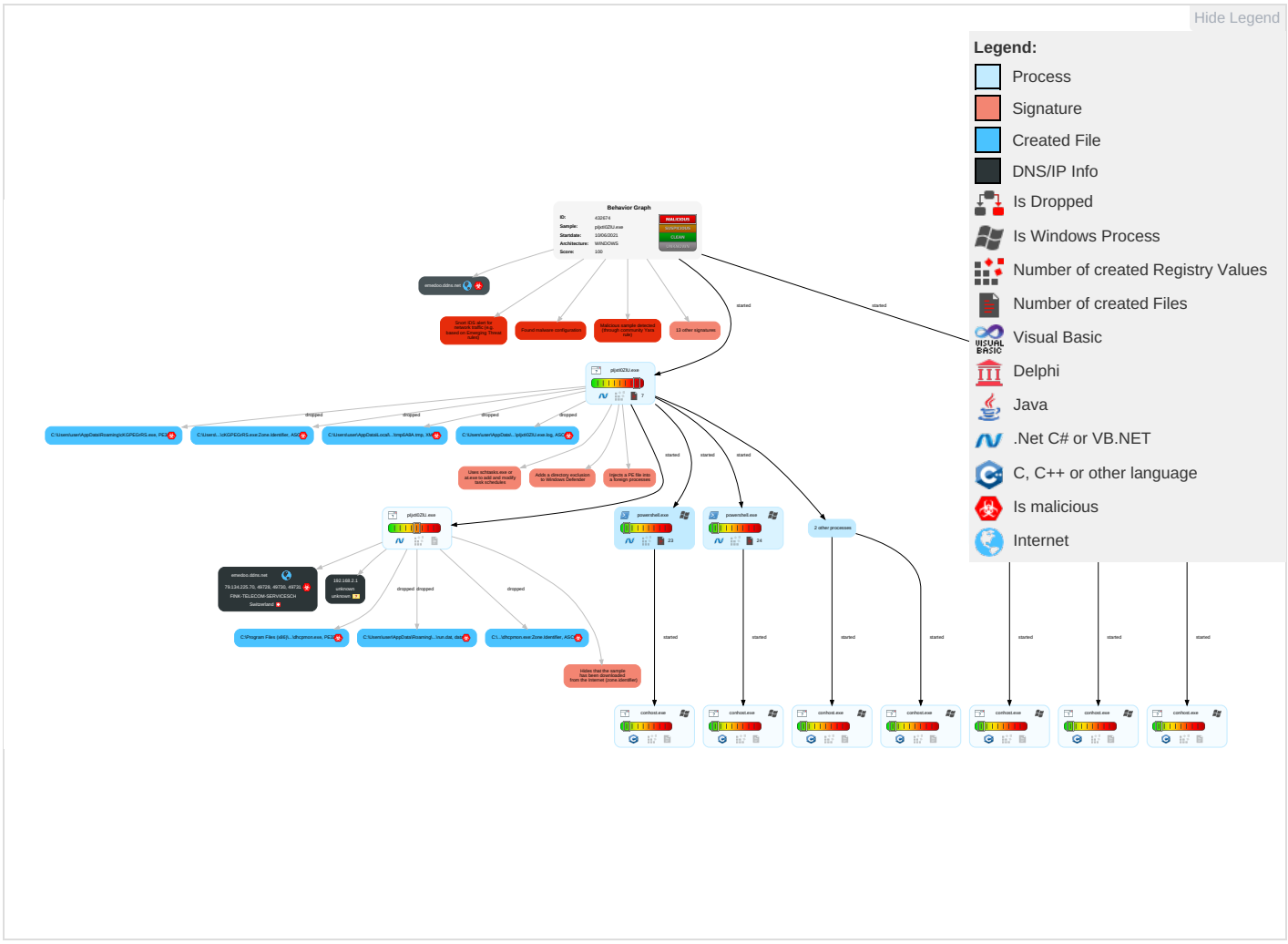
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1 1	Input Capture 2 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	E I N C
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Encrypted Channel 1	E F C
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 3	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1	E T L
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	System Information Discovery 1 4	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Software 1	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 2	LSA Secrets	Security Software Discovery 2 2 1	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 1	N D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 3 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 2 1	J D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Virtualization/Sandbox Evasion 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	F A
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	D I F

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	F E

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
pljxtl0ZIU.exe	40%	Metadefender		Browse
pljxtl0ZIU.exe	64%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
pljxtl0ZIU.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\cKGPEGrRS.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	40%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	64%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\cKGPEGrRS.exe	40%	Metadefender		Browse
C:\Users\user\AppData\Roaming\cKGPEGrRS.exe	64%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
18.0.dhcpmon.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
9.2.pIjxtI0ZlU.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
18.0.dhcpmon.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.pIjxtI0ZlU.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
18.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.2.pIjxtI0ZlU.exe.5b20000.18.unpack	100%	Avira	TR/NanoCore.fadte		Download File
9.0.pIjxtI0ZlU.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
emedoo.ddns.net	0%	Avira URL Cloud	safe	
http://crl.m	0%	URL Reputation	safe	
http://crl.m	0%	URL Reputation	safe	
http://crl.m	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://www.microsoft.ck	0%	Avira URL Cloud	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
127.0.0.1	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
emedoo.ddns.net	79.134.225.70	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
emedoo.ddns.net	true	• Avira URL Cloud: safe	unknown
127.0.0.1	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.70	emedoo.ddns.net	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432674
Start date:	10.06.2021
Start time:	16:42:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	pIjxtI0ZlU.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:	20
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@29/30@13/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 95% • 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
16:43:05	API Interceptor	466x Sleep call for process: pIjxtI0ZlU.exe modified
16:43:16	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
16:43:26	API Interceptor	2x Sleep call for process: dhcpmon.exe modified
16:43:57	API Interceptor	188x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.70	Transcation23032021pdf.exe	Get hash	malicious	Browse	
	Scanpdf04232021.exe	Get hash	malicious	Browse	
	New Tender04,pdf.exe	Get hash	malicious	Browse	
	dL1JMb6Tx6.exe	Get hash	malicious	Browse	
	03_extracted.exe	Get hash	malicious	Browse	
	ntfsmgr.jar	Get hash	malicious	Browse	
	myups.exe	Get hash	malicious	Browse	
	Inv!Overdues.xlsx	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	remittance.jar	Get hash	malicious	Browse	
	http://https://atlashotel.co.uk	Get hash	malicious	Browse	
	http://https://atlashotel.co.uk	Get hash	malicious	Browse	
	http://https://atlashotel.co.uk/	Get hash	malicious	Browse	
	http://https://onedrive.live.com/download?cid=61A1A28AC02783D7&resid=61A1A28AC02783D7%2521106&authkey=ANNsUsrVD6AJ5Z8	Get hash	malicious	Browse	
	http://https://specoriginalsltd.co.uk/	Get hash	malicious	Browse	
	http://https://specoriginalsltd.co.uk/	Get hash	malicious	Browse	
	http://https://ausbuildproltd.com/	Get hash	malicious	Browse	
	43Purchase 0rder Number POE 009389629 M89.exe	Get hash	malicious	Browse	
	25Img-cheque53.jpg.lnk	Get hash	malicious	Browse	
	11Img-Cheque.jpg.lnk	Get hash	malicious	Browse	
	59EFT voucher_eft-234GF.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
emedoo.ddns.net	Re R new proforma.exe	Get hash	malicious	Browse	• 185.140.53.138
	Devizni izvod za partiju 0050100073053.exe	Get hash	malicious	Browse	• 79.134.225.71

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	dYy3yfSkwY.exe	Get hash	malicious	Browse	• 79.134.225.90
	Purchase Order Price List 061021.xlsx	Get hash	malicious	Browse	• 79.134.225.90
	ZVFVY7NwZ7.exe	Get hash	malicious	Browse	• 79.134.225.90
	0jyrU2E05S.exe	Get hash	malicious	Browse	• 79.134.225.72
	kylfnzzg3E.exe	Get hash	malicious	Browse	• 79.134.225.90
	Ref 0180066743.xlsx	Get hash	malicious	Browse	• 79.134.225.90
	MS2106071066.exe	Get hash	malicious	Browse	• 79.134.225.71
	Kangean PO.doc	Get hash	malicious	Browse	• 79.134.225.72
	facture.jar	Get hash	malicious	Browse	• 79.134.225.69
	c3yBu1IF57.exe	Get hash	malicious	Browse	• 79.134.225.92
	DPSGNwkO1Z.exe	Get hash	malicious	Browse	• 79.134.225.25
	SecuriteInfo.com.Trojan.Win32.Save.a.16917.exe	Get hash	malicious	Browse	• 79.134.225.94
	AedJpyQ9lM.exe	Get hash	malicious	Browse	• 79.134.225.90
	H538065217Invoice.exe	Get hash	malicious	Browse	• 79.134.225.9
	Purchase Order Price List.xlsx	Get hash	malicious	Browse	• 79.134.225.90
	P.I-84512.doc	Get hash	malicious	Browse	• 79.134.225.41
	l00VLAF9y0xQ9Vr.exe	Get hash	malicious	Browse	• 79.134.225.92
	Swift [ref QT #U2013 2102001-R2]pdf.exe	Get hash	malicious	Browse	• 79.134.225.10
	PO756654.exe	Get hash	malicious	Browse	• 79.134.225.99
	qdFDmi3Bhy.exe	Get hash	malicious	Browse	• 79.134.225.90

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\pIjxtI0ZIU.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	872960
Entropy (8bit):	7.804008605753687
Encrypted:	false

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
SSDEEP:	24576:sTG4f1eyPqmm+zEXrT+LURFgLL43PpFUoEn7:oGoFmTrT+LUgLLr7
MD5:	A253962036D634B39E913BC0322584E5
SHA1:	769427FCA217ACCDA232A61A9796AFFD6536C24B
SHA-256:	E6A6126A0E0DA3279205A265388761D74CEADE122FAFC5A393C2D6B9DCC3B8E1
SHA-512:	B23F44D6C1449F9268CF9ACC75ABB3F7402A8721BAC4BBE026EC8DC5F87FF3D576146E346D96A45F108D01A1B1AFC956C14E476A86C4A3D4E32E07C42F3301F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 40%, Browse • Antivirus: ReversingLabs, Detection: 64%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Z..`.....P..F.....e... ..... ..... ..@.....`e..O..... ....H.....text....E... ...F..... ..`.rsrc.....H.....@..@.rel oc.....P.....@..B.....e.....H.....;..x.....f....K..h.....(...*&..(!....*.s".....s#.....s$.....s%.....s&.....*...0.....~....o'....+..*.0..... .....~....o(....+..*.0.....~....o)....+..*.0.....~....o*....+..*.0.....~....o+....+..*&..(,....*...0..<.....~.....(-.....,!r...p.....(....o/...s0.....~....+..*.0.....~....+..*".....*.0..... (....r5..p~....o1....+..*...0..<.....~.....(-.....,!rG..p.....(.

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\pIjxtI0ZlU.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:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	false
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_3 2\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.Vi sualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\pIjxtI0ZlU.exe.log	
Process:	C:\Users\user\Desktop\pIjxtI0ZlU.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\pIjxtI0ZlU.exe.log	
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	15432
Entropy (8bit):	5.013651254695938
Encrypted:	false
SSDEEP:	384:Jib44EdVoGIpN6KQkj2Zkjh4iUxZvuiOOdBCNXp5nYoJib4J:0YV3IpNBQkj2Yh4iUxZvuiOOdBCNZlYO
MD5:	96C8600F85FEE8291031FEE1B9C99641
SHA1:	A902BA7EC2DE98ED7A6A146748128FE9D9ACFD98
SHA-256:	F04CBAE3845B54695F75A170593B854D7860E5FE3CA09AC8898E3A83528D207A
SHA-512:	6795F6F6963E61E7D0711D2D4E375BBB0A527B8E1EAE0D687517832BDAF500F6D49E4A144F0133C4A4373CCBC22D769E6490150A816B05CF57014C43A8F4F021
Malicious:	false
Preview:	PSMODULECACHE.....a...C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1.....Set-PackageSource.....Unregister-PackageSource.....Get-PackageSource.....Install-Package.....Save-Package.....Get-Package.....Find-Package.....Install-PackageProvider.....Import-PackageProvider.....Get-PackageProvider.....Register-PackageSource.....Uninstall-Package.....Find-PackageProvider.....D.....C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1.....Get-OperationValidation.....Invoke-OperationValidation.....PSMODULECACHE.....Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1....Uninstall-Module.....inmo.....fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command..

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2eauonq5.sf4.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
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_45xdmgad.ne3.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
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_4qishmbi.mwv.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_4qishmbi.mwv.ps1	
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_dvvweyxm.cq0.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
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_k0jcxbvr.oaj.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
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ls4citrk.03p.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
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_m3xc3fy5.3rw.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_m3xc3fy5.3rw.psm1	
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_tfw4koet.qzi.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
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_xwxtwu25.t5k.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
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_y3dvtdlu.gel.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
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp6A8A.tmp	
Process:	C:\Users\user\Desktop\pIjxtI0ZlU.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1642

C:\Users\user\AppData\Local\Temp\tmp6A8A.tmp	
Entropy (8bit):	5.179190126981541
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGBOtn:cbhK79lNQR/rydbz9I3YODOLNdq30o
MD5:	8B6094474FC32FB3A4338E648AAAF862
SHA1:	BDE51867C9528169C7AD3766895AC3ADA53234D7
SHA-256:	6816C07A604CA2CAEFAF5591A5ECF8FF1C97AC93408FE1B1CCC64DF50C8FF134
SHA-512:	1FBB311203B2EFA27C18F07CFB64887C458F534A7A636D762B37A7E058FE84195208E58CE46FEAFCBACD33C6EA10FA5476E37D899FDB5C0FD3AE564D46EC5C88
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <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\tmpAF63.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):	1642
Entropy (8bit):	5.179190126981541
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGBOtn:cbhK79lNQR/rydbz9I3YODOLNdq30o
MD5:	8B6094474FC32FB3A4338E648AAAF862
SHA1:	BDE51867C9528169C7AD3766895AC3ADA53234D7
SHA-256:	6816C07A604CA2CAEFAF5591A5ECF8FF1C97AC93408FE1B1CCC64DF50C8FF134
SHA-512:	1FBB311203B2EFA27C18F07CFB64887C458F534A7A636D762B37A7E058FE84195208E58CE46FEAFCBACD33C6EA10FA5476E37D899FDB5C0FD3AE564D46EC5C88
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <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\catalog.dat	
Process:	C:\Users\user\Desktop\pIjxtI0ZlU.exe
File Type:	data
Category:	dropped
Size (bytes):	2320
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwh:flC0IlC0IlC0IlC0IlC0IlC0IlC0IlCr
MD5:	0FBED11864C03FDED0E70014DCF84578
SHA1:	453723D938A03252F705B0A104986FE4C5CA7056
SHA-256:	70F5E49EE3091777827ED661B63842061220C899A708860986E9AA1BD87C5004
SHA-512:	DB53E3F1D18171F1D86C1B9BBF6BBD07153FC3E561834A35834BC0CA1E034FEDCD83AAAE7EDF9262C4E175C3D2287B647F55282E49627EAAF587F4371420466
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.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.....&.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.....&.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.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\pIjxtI0ZlU.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:927J8t:U7+
MD5:	A809CC4AB3446553E27FD56631548E89
SHA1:	059B4901CCB5ADAC8DB1B1405C9981704562A033

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
SHA-256:	8EF32C0109E66CB0F663793C1CAD8823E42A41DECA38E1F3641631A103F5D94C
SHA-512:	A394735C84D711B7FC2818A2EC3146158B9A78968DDD2973792617E4390CBEBE04F78DD68218CAC19EA746B1E9B6A2FD04CEA92CBFDE38D347CC32828256D43
Malicious:	**true**
Preview:	..X..,.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\pIjxtI0ZlU.exe
File Type:	data
Category:	modified
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671ECB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\pIjxtI0ZlU.exe
File Type:	data
Category:	dropped
Size (bytes):	426840
Entropy (8bit):	**7.999608491116724**
Encrypted:	**true**
SSDEEP:	12288:zKf137EiDsTjevgA4p0V7njXuWSvdVU7V4OC0Rr:+134i2lp67i5d8+OCg
MD5:	963D5E2C9C0008DFF05518B47C367A7F
SHA1:	C183D601FABBC9AC8FBFA0A0937DECC677535E74
SHA-256:	5EACF2974C9BB2C2E24CDC651C4840DD6F4B76A98F0E85E90279F1DBB2E6F3C0
SHA-512:	0C04E1C1A13070D48728D9F7F300D9B26DEC6EC8875D8D3017EAD52B9EE5BDF9B651A7F0FCC537761212831107646ED72B8ED017E7477E600BC0137EF857AE2
Malicious:	false
Preview:	..g&jo...IPg...GM....R>i...o...I.>.&.r{....8...}...E....v.!7.u3e.. .....db...}.....".t(.xC9.cp.B....7...'.....%.....w.^._.....B.W%.<..i.0.{9.xS...5...)..w..$..C..?`F..u.5.T.X.w'Si..z.n{...Y!m...RA...xg....[7...z..9@.K.-...T..+.ACe....R....enO.....AoNMT.\^....}H&..4I...B.:..@..J...v..rI5..kP.....2j....B..B.~.T..>.c..emW;Rn<9..[.r.o....R[....@=...:...L.g<.....I..%4[.G^.~.I'.....v.p&.....+..S...9d/.{..H.`@.1.....f.\s...X.a.].<.h*...J4*...k.x....%3.....3.c..?%....>.!.}..)(.{...H...3..`].Q.[sN..JX(.%pH....+.....(...v.....H...3..8.a_..J..?4...y.N(..D.*h..g.jD..I...44Q?..N.....oX.A.....I...n?./.....$.!.;.^9"H.....*...OkF....v.m_.e.v..f...".bq{.....O.-....%R+...-..P.i..t5....2Z# ...#...,L..{..j..heT -=Z.P;...g.m)<owJ].J..../.p..8.u8.&..#.m9...j%..g&....g.x.I,....u.[....>./W.....*X...b*Z...ex.0..x.}.....Tb...[..H_M._.^N.d&...g._."@4N.pDs].GbT.....&p.....Nw...%$=.....{..J.1....2....<E{..<!G..

C:\Users\user\AppData\Roaming\cKGPEGrRS.exe	
Process:	C:\Users\user\Desktop\pIjxtI0ZlU.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	872960
Entropy (8bit):	7.804008605753687
Encrypted:	false
SSDEEP:	24576:sTG4f1eyPqmm+zEXrT+LURFgLL43PpFUoEn7:oGoFmTrT+LUgLLr7
MD5:	A253962036D634B39E913BC0322584E5
SHA1:	769427FCA217ACCDA232A61A9796AFFD6536C24B
SHA-256:	E6A6126A0E0DA3279205A265388761D74CEADE122FAFC5A393C2D6B9DCC3B8E1
SHA-512:	B23F44D6C1449F9268CF9ACC75ABB3F7402A8721BAC4BBE026EC8DC5F87FF3D576146E346D96A45F108D01A1B1AFC956C14E476A86C4A3D4E32E07C42F3301F
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 40%, Browse • Antivirus: ReversingLabs, Detection: 64%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Z..`.....P..F.....e... ..... ..... ..@.....`e..O..... ..... .H.....text....E... ...F..... ..`.rsrc.....H.....@..@.rel oc.....P.....@..B.....e.....H.....;..x.....f....K..h.....(...*&..(!....*.s".....s#.....s$.....s%.....s&.....*...0.....~....o'....+..*.0..... .....~....o(....+..*.0.....~....o)....+..*.0.....~....o*....+..*.0.....~....o+....+..*&..(,....*...0..<.....~.....(-.....!r...p.....(....o/...s0.....~.....+..*.0.....~.....+..*".....*.0..... (....r5..p~....o1....+..*...0..<.....~.....(-.....!rG..p.....(.

C:\Users\user\AppData\Roaming\cKGPEGrRS.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\pIjxtI0ZIU.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:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20210610\PowerShell_transcript.618321.3dgWtHGR.20210610164313.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):	1520
Entropy (8bit):	5.345603285666763
Encrypted:	false
SSDEEP:	24:BxSAY7vBZCF+x2DOXUWeSuaBeW4HjeTKKjX4CIym1ZJXJuaBDxSAZC7vBZCF+x24:BZWvjCMoO+ShJ4qDYB1ZXhDZCvjCMoOj
MD5:	A5A4E8D5C02F3E9236B780EA46191D18
SHA1:	58496ACFDC13A3240EBCE1A929749C3A55503884
SHA-256:	91892DD90697543A0F35F38678F9CFCB9DFEACA24D614370F3FC75D9456B6034
SHA-512:	8488944B4DD144A8373E8B3F2A1E8174C4E0F9D180E58B11FB84A42936218F04A89321BC5D43B64F9B1283A465004EFEE75A400B928B156A5BA628720820D000
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210610164340..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 618321 (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\cKGPEGrRS.exe..Process ID: 2860..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: 20210610164343..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\cKGPEGrRS.exe..**********..Windows PowerShell transcript start..Start time: 20210610165105..Username: computer\user..RunAs User: computer\user.

C:\Users\user\Documents\20210610\PowerShell_transcript.618321.78lZVBm4.20210610164310.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):	2823
Entropy (8bit):	5.436494782453794
Encrypted:	false
SSDEEP:	48:BZGvjCMoO+ShJsqDYB1ZzhDZevjCMoO+ShJsqDYB1ZEFDtich+3Ntich+3N:BZqjCMNHeqDo1ZdDZSjCMNHeqDo1Z+aw
MD5:	C666C3F68F4928C6D7363CB2BBB1E5CD
SHA1:	75912C9F9E3BDCEFFC190B2057B5157934CEF20A
SHA-256:	58653F4998E5D79E9D3A6EC13C3FF345EFCE8374BAE235D6DAAE1D02CC10D9AD
SHA-512:	981F7FDACE34F8E41C9337450BD7C9E66567BEDC3AFD2C41ABDF6E45046A2E8144E4B09D3235EF83CA4CF77D5C6AC59677DFC816A90249881E37B278A2CEC9D2
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210610164335..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 618321 (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\cKGPEGrRS.exe..Process ID: 4624..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: 20210610164336..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\cKGPEGrRS.exe..**********..Windows PowerShell transcript start..Start time: 20210610165138..Username: computer\user..RunAs User: computer\user.

C:\Users\user\Documents\20210610\PowerShell_transcript.618321.MsaG93zL.20210610164344.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):	844
Entropy (8bit):	5.324758790991886
Encrypted:	false
SSDEEP:	24:BxSAF7vBZCF+x2DOXUWeSuaBeWDHjeTKKjX4CIym1ZJXqPVuaBy:BZxvjCMoO+ShJDqDYB1Zyhy
MD5:	9A236061426BE1A5D92F02F7B0051A18

C:\Users\user\Documents\20210610\PowerShell_transcript.618321.MsaG93zL.20210610164344.txt	
SHA1:	B192D64602542CBCFEF1E92C977C824743404EC2
SHA-256:	ADD10A80772094E571CF9616387E3E2489534E63E4BE806B736CEB3519E92793
SHA-512:	AD2350601CE722BA10A9984636EB6282B1909FFA4440EF6251A4BBBB965859D6C2D5CE92283C4EED1DF67EC060BA09F1426C32443E2F028CF730541E287BA56(
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210610164440..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 618321 (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\cKGPEGrRS.exe..Process ID: 6584..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: 20210610164441..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\cKGPEGrRS.exe..

C:\Users\user\Documents\20210610\PowerShell_transcript.618321.izxR1blY.20210610164310.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):	5079
Entropy (8bit):	5.416594602844092
Encrypted:	false
SSDEEP:	96:BZtjCMNyqDo1ZNZ0jCMNyqDo1Z4oiQjZZjCMNyqDo1ZH5A9:kjoa
MD5:	CD8A5E0B4479AD8E27E91127BA4E296A
SHA1:	953C54B8E93EE7F2FB7E936DDF1FE497A3DA826B
SHA-256:	85E0B6834BE209908470F6516551D35D85936E61B4177A777BE451D4E7A85301
SHA-512:	5AEB1A1ABF69A1AF0455F2A4180506B7DFF6C034E964BBFDF8056397C602CBCB481F6D64441D3A5256C1BBEEF285537DF2CC1F2D022560375AC6836C98592F6
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210610164332..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 618321 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\pIjxtI0ZlU.exe..Process ID: 5868..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: 20210610164333..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\pIjxtI0ZlU.exe..**********..Windows PowerShell transcript start..Start time: 20210610165114..Username: computer\user..RunAs User: computer\user..Configuration

C:\Users\user\Documents\20210610\PowerShell_transcript.618321.nB5QM3Ux.20210610164336.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):	850
Entropy (8bit):	5.32274872558091
Encrypted:	false
SSDEEP:	24:BxSAIN7vBZCF+x2DOXUWeSur+WRHjeTKKjX4CIym1ZJXgFurS:BZsvjCMoO+SepRqDYB1Z2eS
MD5:	B564DF21F06DDE543264248679CBAA90
SHA1:	C0CB3985420035D6F4BEB0D5C1A7C93ED629AA84
SHA-256:	B623138C11C1783DAB074FDF22F39004358FDD2A4294032CA43FD2D9E8596467
SHA-512:	B24C49E5BE23EE343869C2A8AFDF8E218905888251AAD4C27631F12FF5EC7D667C43BB3D83303456F1FADE2988E4C0576B544AF962E0C580C584EE27E5C0945
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210610164438..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 618321 (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: 6432..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: 20210610164438..**********..PS>Add-MpPreference -ExclusionPath C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.804008605753687
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:	pIjxtI0ZlU.exe

General

File size:	872960
MD5:	a253962036d634b39e913bc0322584e5
SHA1:	769427fca217accda232a61a9796affd6536c24b
SHA256:	e6a6126a0e0da3279205a265388761d74ceade122fafc5a393c2d6b9dcc3b8e1
SHA512:	b23f44d6c1449f9268cf9acc75abb3f7402a8721bac4bbe026ec8dc5f87ff3d576146e346d96a45f108d01a1b1afc956c14e476a86c4a3d4e32e07c42f3301ff
SSDEEP:	24576:sTG4f1eyPqmm+zEXrT+LURFgLL43PpFUoEn7:oGoFmTrT+LUgLLr7
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Z..`.....P..F.....e... ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x110d65b2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x11000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60B49D5A [Mon May 31 08:24:58 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
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	0xd45b8	0xd4600	False	0.864505545541	data	7.81196430764	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xd8000	0x68c	0x800	False	0.373046875	data	3.67984589901	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xda000	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
06/10/21-16:43:16.181856	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49728	5230	192.168.2.4	79.134.225.70
06/10/21-16:43:24.245980	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49730	5230	192.168.2.4	79.134.225.70
06/10/21-16:43:32.581695	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49731	5230	192.168.2.4	79.134.225.70
06/10/21-16:43:41.654459	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49732	5230	192.168.2.4	79.134.225.70
06/10/21-16:43:51.838026	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49733	5230	192.168.2.4	79.134.225.70
06/10/21-16:44:00.160563	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49735	5230	192.168.2.4	79.134.225.70
06/10/21-16:44:09.365596	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49736	5230	192.168.2.4	79.134.225.70
06/10/21-16:44:25.075133	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49737	5230	192.168.2.4	79.134.225.70
06/10/21-16:44:35.323686	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49738	5230	192.168.2.4	79.134.225.70
06/10/21-16:44:45.292661	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49739	5230	192.168.2.4	79.134.225.70
06/10/21-16:44:55.386230	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49740	5230	192.168.2.4	79.134.225.70
06/10/21-16:45:12.434729	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49741	5230	192.168.2.4	79.134.225.70
06/10/21-16:45:35.247464	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49742	5230	192.168.2.4	79.134.225.70

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 10, 2021 16:43:15.909375906 CEST	192.168.2.4	8.8.4.4	0xf40c	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
Jun 10, 2021 16:43:24.033548117 CEST	192.168.2.4	8.8.4.4	0xd569	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
Jun 10, 2021 16:43:32.141026020 CEST	192.168.2.4	8.8.4.4	0x17dc	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
Jun 10, 2021 16:43:40.648566961 CEST	192.168.2.4	8.8.4.4	0xc42c	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
Jun 10, 2021 16:43:51.682612896 CEST	192.168.2.4	8.8.4.4	0xe131	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
Jun 10, 2021 16:43:59.743705034 CEST	192.168.2.4	8.8.4.4	0x4168	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
Jun 10, 2021 16:44:08.700932980 CEST	192.168.2.4	8.8.4.4	0x93f6	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
Jun 10, 2021 16:44:24.462752104 CEST	192.168.2.4	8.8.4.4	0x9607	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
Jun 10, 2021 16:44:34.109848022 CEST	192.168.2.4	8.8.4.4	0x9bb7	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
Jun 10, 2021 16:44:44.421998978 CEST	192.168.2.4	8.8.4.4	0x2cbc	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
Jun 10, 2021 16:44:54.815670967 CEST	192.168.2.4	8.8.4.4	0x78a7	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
Jun 10, 2021 16:45:10.016948938 CEST	192.168.2.4	8.8.4.4	0xbd06	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
Jun 10, 2021 16:45:35.085431099 CEST	192.168.2.4	8.8.4.4	0x2836	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)

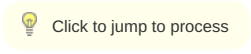
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 10, 2021 16:43:15.982986927 CEST	8.8.4.4	192.168.2.4	0xf40c	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)
Jun 10, 2021 16:43:24.096941948 CEST	8.8.4.4	192.168.2.4	0xd569	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)
Jun 10, 2021 16:43:32.200649023 CEST	8.8.4.4	192.168.2.4	0x17dc	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)
Jun 10, 2021 16:43:40.710187912 CEST	8.8.4.4	192.168.2.4	0xc42c	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)
Jun 10, 2021 16:43:51.741216898 CEST	8.8.4.4	192.168.2.4	0xe131	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)
Jun 10, 2021 16:43:59.802645922 CEST	8.8.4.4	192.168.2.4	0x4168	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)
Jun 10, 2021 16:44:08.761003017 CEST	8.8.4.4	192.168.2.4	0x93f6	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)
Jun 10, 2021 16:44:24.524466991 CEST	8.8.4.4	192.168.2.4	0x9607	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)
Jun 10, 2021 16:44:34.170095921 CEST	8.8.4.4	192.168.2.4	0x9bb7	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)
Jun 10, 2021 16:44:44.480829954 CEST	8.8.4.4	192.168.2.4	0x2cbc	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)
Jun 10, 2021 16:44:54.875230074 CEST	8.8.4.4	192.168.2.4	0x78a7	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)
Jun 10, 2021 16:45:10.075479984 CEST	8.8.4.4	192.168.2.4	0xbd06	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)
Jun 10, 2021 16:45:35.148183107 CEST	8.8.4.4	192.168.2.4	0x2836	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: pIjxtI0ZlU.exe PID: 5712 Parent PID: 5892

General

Start time:	16:43:05
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\pIjxtI0ZlU.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\Desktop\pIjxtI0ZlU.exe'
Imagebase:	0xe60000
File size:	872960 bytes
MD5 hash:	A253962036D634B39E913BC0322584E5
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: 00000000.00000002.663388588.00000000045E1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.663388588.00000000045E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.663388588.00000000045E1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.660754559.0000000003615000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 5868 Parent PID: 5712

General

Start time:	16:43:07
Start date:	10/06/2021
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\pIjxtI0ZlU.exe'
Imagebase:	0xf30000
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: 5792 Parent PID: 5868

General

Start time:	16:43:08
Start date:	10/06/2021
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: powershell.exe PID: 4624 Parent PID: 5712

General

Start time:	16:43:08
Start date:	10/06/2021
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\cKGPEGrRS.exe'
Imagebase:	0xf30000
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: 64 Parent PID: 4624

General

Start time:	16:43:08
Start date:	10/06/2021
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: 4184 Parent PID: 5712

General

Start time:	16:43:08
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\cKGPEGrRS' /XML 'C:\Users\user\AppData\Local\Temp\tmp6A8A.tmp'
Imagebase:	0x220000
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: 1900 Parent PID: 4184

General

Start time:	16:43:09
Start date:	10/06/2021
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: powershell.exe PID: 2860 Parent PID: 5712

General

Start time:	16:43:10
Start date:	10/06/2021
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\cKGPEGrRS.exe'
Imagebase:	0xf30000
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: 4204 Parent PID: 2860

General

Start time:	16:43:10
Start date:	10/06/2021
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: pIjxtI0ZlU.exe PID: 2208 Parent PID: 5712

General

Start time:	16:43:10
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\pIjxtI0ZlU.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\pIjxtI0ZlU.exe
Imagebase:	0xb40000
File size:	872960 bytes
MD5 hash:	A253962036D634B39E913BC0322584E5
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: 00000009.00000002.949190405.0000000006E90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.949190405.0000000006E90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.945200916.0000000005F30000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.945200916.0000000005F30000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.655614404.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.655614404.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.655614404.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000009.00000003.667634443.0000000004619000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.656249300.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth

- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.656249300.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000009.00000000.656249300.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: NanoCore, Description: unknown, Source: 00000009.00000002.936110160.0000000003285000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.944714710.0000000005ED0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.944714710.0000000005ED0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.944949810.0000000005EF0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.944949810.0000000005EF0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.947720444.00000000068F0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.947720444.00000000068F0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.938032088.0000000004294000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.948576490.0000000006D10000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.948576490.0000000006D10000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.948873822.0000000006D40000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.948873822.0000000006D40000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.943539466.0000000005B20000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.943539466.0000000005B20000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.943539466.0000000005B20000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.945020551.0000000005F00000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.945020551.0000000005F00000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.947857649.0000000006910000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.947857649.0000000006910000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.949135204.0000000006E80000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.949135204.0000000006E80000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.943137206.0000000005880000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.943137206.0000000005880000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.948362673.0000000006BB0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.948362673.0000000006BB0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.917666929.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.917666929.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000009.00000002.917666929.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.947592348.00000000068E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.947592348.00000000068E0000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	low

Analysis Process: dhcpmon.exe PID: 6304 Parent PID: 3424

General

Start time:	16:43:24
Start date:	10/06/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x4f0000
File size:	872960 bytes
MD5 hash:	A253962036D634B39E913BC0322584E5
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: 0000000A.00000002.754193726.0000000002D46000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.770095334.0000000003D11000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.770095334.0000000003D11000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.770095334.0000000003D11000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 40%, Metadefender, Browse • Detection: 64%, ReversingLabs
Reputation:	low

Analysis Process: powershell.exe PID: 6432 Parent PID: 6304

General

Start time:	16:43:30
Start date:	10/06/2021
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:	0xf30000
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: 6440 Parent PID: 6432

General

Start time:	16:43:31

Start date:	10/06/2021
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: 6448 Parent PID: 6304

General

Start time:	16:43:31
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\cKGPEGrRS' /XML 'C:\Users\user\AppData\Local\Temp\tmpAF63.tmp'
Imagebase:	0x220000
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: 6500 Parent PID: 6448

General

Start time:	16:43:32
Start date:	10/06/2021
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

Analysis Process: powershell.exe PID: 6584 Parent PID: 6304

General

Start time:	16:43:33
Start date:	10/06/2021
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\cKGPEGrRS.exe'
Imagebase:	0xf30000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: conhost.exe PID: 6596 Parent PID: 6584

General

Start time:	16:43:34
Start date:	10/06/2021
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

Analysis Process: dhcpmon.exe PID: 6604 Parent PID: 6304

General

Start time:	16:43:34
Start date:	10/06/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x1f0000
File size:	872960 bytes
MD5 hash:	A253962036D634B39E913BC0322584E5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: 6716 Parent PID: 6304

General

Start time:	16:43:36
Start date:	10/06/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x530000
File size:	872960 bytes
MD5 hash:	A253962036D634B39E913BC0322584E5
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: 00000012.00000000.714388325.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000000.714388325.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000000.714388325.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000000.724479012.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000000.724479012.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000000.724479012.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.774513061.0000000003CE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.774513061.0000000003CE1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.751437689.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.751437689.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.751437689.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.773226669.0000000002CE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.773226669.0000000002CE1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Disassembly

Code Analysis