ID: 527613
Sample Name: CV.exe
Cookbook: default.jbs
Time: 03:42:08
Date: 24/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

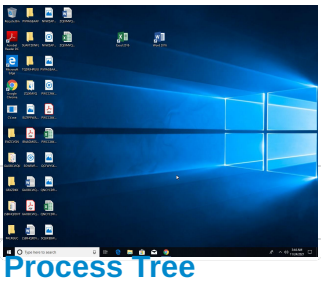
Windows Analysis Report CV.exe

Overview

General Information

Sample Name:	CV.exe
Analysis ID:	527613
MD5:	de2d175988e8d0..
SHA1:	d4e7bacea5b7ee..
SHA256:	37649a092c0ad8..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

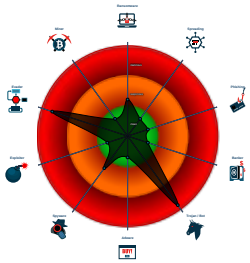
Nanocore

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Multi AV Scanner detection for doma…
- Yara detected Nanocore RAT
- Tries to detect sandboxes and other…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- CV.exe (PID: 4020 cmdline: "C:\Users\user\Desktop\CV.exe" MD5: DE2D175988E8D0E1D9C37482FB37C66C)
  - CV.exe (PID: 360 cmdline: C:\Users\user\Desktop\CV.exe MD5: DE2D175988E8D0E1D9C37482FB37C66C)
- dhcpmon.exe (PID: 5628 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: DE2D175988E8D0E1D9C37482FB37C66C)
  - dhcpmon.exe (PID: 1664 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: DE2D175988E8D0E1D9C37482FB37C66C)
  - dhcpmon.exe (PID: 5348 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: DE2D175988E8D0E1D9C37482FB37C66C)
  - dhcpmon.exe (PID: 7096 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: DE2D175988E8D0E1D9C37482FB37C66C)
  - WMIADAP.exe (PID: 7096 cmdline: wmiadap.exe /F /T /R MD5: 9783D0765F31980950445DFD40DB15DA)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "f4157c11-54e5-4893-8a60-6856b847",
  "Group": "Default",
  "Domain1": "dera31.ddns.net",
  "Domain2": "195.133.18.211",
  "Port": 1187,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000000.323309609.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000E.00000000.323309609.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000E.00000000.323309609.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
0000000E.00000000.322328292.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000E.00000000.322328292.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 50 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
14.2.dhcpmon.exe.425e434.5.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost

Source	Rule	Description	Author	Strings
14.2.dhcpmon.exe.425e434.5.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
14.2.dhcpmon.exe.425e434.5.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
14.2.dhcpmon.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
14.2.dhcpmon.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
Click to see the 82 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Yara detected Nanocore RAT

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

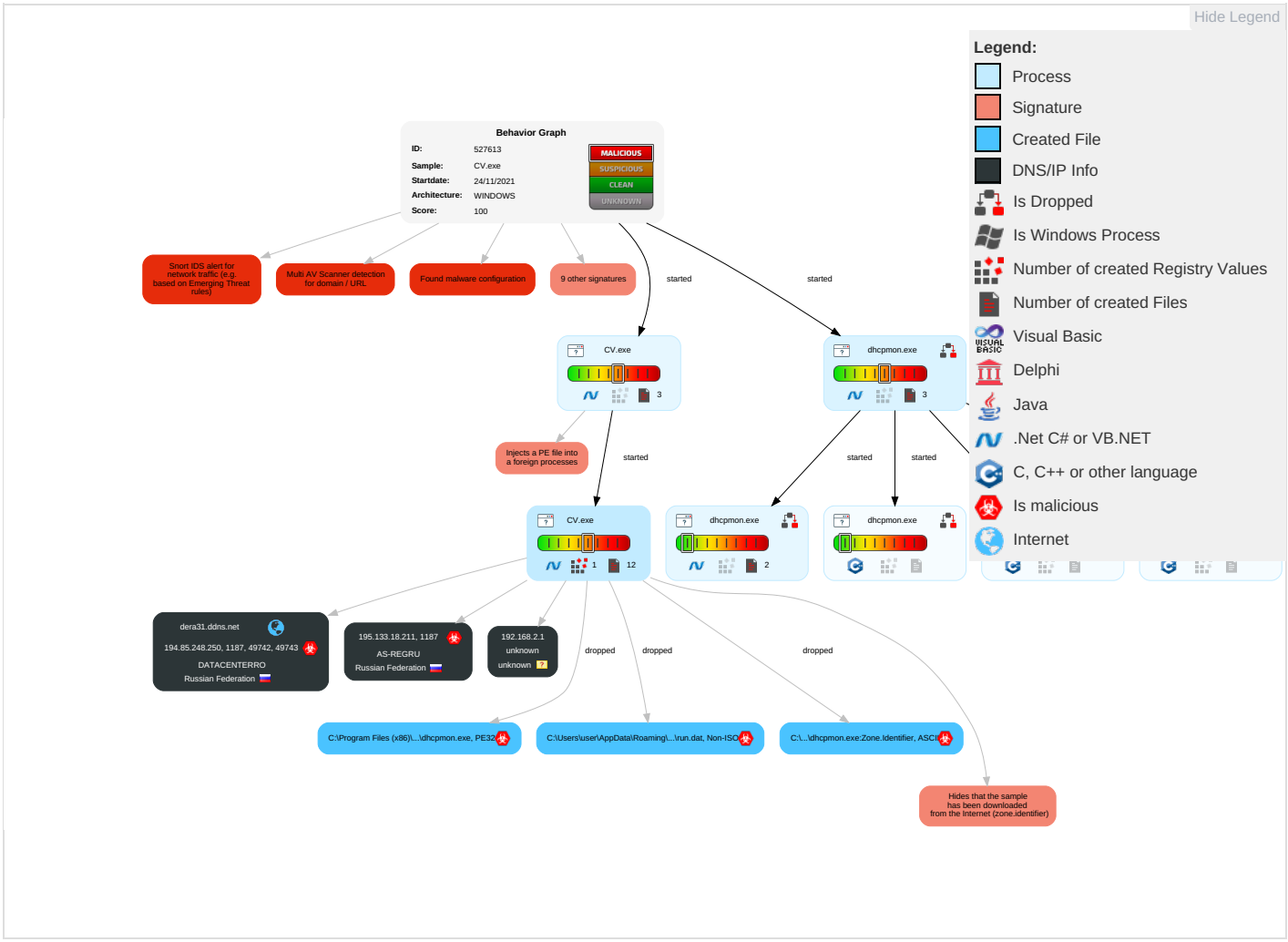
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Ne Eff
Valid Accounts	Windows Management Instrumentation	Path Interception	Access Token Manipulation 1	Masquerading 2	Input Capture 1 1	Security Software Discovery 1 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Ea Ins Ne Co
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Ex Re Ca
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	Ex Tra Lo
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SI Sw
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1 2	LSA Secrets	System Information Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Ma De Co
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jar De Se
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Ro Ac

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Ne Eff
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Do Ins Pro
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 1 3	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Ro Ba

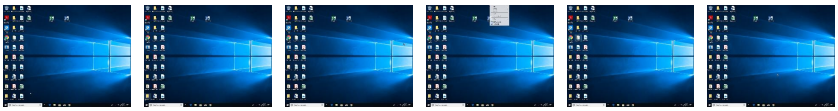
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.0.dhcpmon.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.0.dhcpmon.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.0.dhcpmon.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.CV.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.CV.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.CV.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.CV.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
14.0.dhcpmon.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.0.dhcpmon.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.CV.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
dera31.ddns.net	6%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/jp/?	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com2	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0/F	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnA	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//e	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.tiro.comA	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.founder.com.cn/cny	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.comaB	0%	Avira URL Cloud	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.founder.com.cn/cnb	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/X	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0et	0%	Avira URL Cloud	safe	
http://www.tiro.comslnt	0%	URL Reputation	safe	
http://www.tiro.comn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/?0	0%	Avira URL Cloud	safe	
http://www.fontbureau.commno4	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
dera31.ddns.net	0%	Avira URL Cloud	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.comicm	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/?	0%	URL Reputation	safe	
http://www.fontbureau.comdj	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.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.carterandcone.com-u	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/j	0%	URL Reputation	safe	
http://www.founder.com.cn/cn&	0%	URL Reputation	safe	
http://www.tiro.comic	0%	URL Reputation	safe	
195.133.18.211	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/talic	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dera31.ddns.net	194.85.248.250	true	true	• 6%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
dera31.ddns.net	true	• Avira URL Cloud: safe	unknown
195.133.18.211	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
195.133.18.211	unknown	Russian Federation		197695	AS-REGRU	true
194.85.248.250	dera31.ddns.net	Russian Federation		35478	DATACENTERRO	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	527613
Start date:	24.11.2021
Start time:	03:42:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CV.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:	27
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@11/6@9/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1% (good quality ratio 0.8%) • Quality average: 36.2% • Quality standard deviation: 21.6%

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
03:43:01	API Interceptor	931x Sleep call for process: CV.exe modified
03:43:06	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
03:43:16	API Interceptor	1x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
195.133.18.211	circular_11_17_21.exe	Get hash	malicious	Browse	
	Bank Report.exe	Get hash	malicious	Browse	
	cliff.kuhfeldt's CV.exe	Get hash	malicious	Browse	
	Jessica Ohnesorge'CV.exe	Get hash	malicious	Browse	
	Change Of Registration Form.exe	Get hash	malicious	Browse	
	Payment invoice.exe	Get hash	malicious	Browse	
	Wire Transfer Slip.exe	Get hash	malicious	Browse	
	Advise.exe	Get hash	malicious	Browse	
	Bank Report.exe	Get hash	malicious	Browse	
	N5HlpHINh2.exe	Get hash	malicious	Browse	
	BL draft.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
dera31.ddns.net	circular_11_17_21.exe	Get hash	malicious	Browse	• 195.133.18.211
	Bank Report.exe	Get hash	malicious	Browse	• 195.133.18.211
	cliff.kuhfeldt's CV.exe	Get hash	malicious	Browse	• 195.133.18.211
	Jessica Ohnesorge'CV.exe	Get hash	malicious	Browse	• 195.133.18.211
	Change Of Registration Form.exe	Get hash	malicious	Browse	• 195.133.18.211
	Payment invoice.exe	Get hash	malicious	Browse	• 195.133.18.211
	Wire Transfer Slip.exe	Get hash	malicious	Browse	• 195.133.18.211
	Advise.exe	Get hash	malicious	Browse	• 195.133.18.211
	Bank Report.exe	Get hash	malicious	Browse	• 195.133.18.211
	N5HlpHINh2.exe	Get hash	malicious	Browse	• 195.133.18.211
	BL draft.exe	Get hash	malicious	Browse	• 195.133.18.211

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-REGRU	wnRWWNwExD.exe	Get hash	malicious	Browse	• 194.58.112.165
	o3j25D1Pg1.exe	Get hash	malicious	Browse	• 195.133.18.66
	PjvBTyWpg6.exe	Get hash	malicious	Browse	• 31.31.196.67
	Ez6r9fZIXc.exe	Get hash	malicious	Browse	• 37.140.192.43
	PURCHASE ORDER.doc	Get hash	malicious	Browse	• 194.58.112.174

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	circular_11_17_21.exe	Get hash	malicious	Browse	• 195.133.18.211
	Bank Report.exe	Get hash	malicious	Browse	• 195.133.18.211
	6iXle7QJdI.exe	Get hash	malicious	Browse	• 194.87.206.125
	cliff.kuhfeldt's CV.exe	Get hash	malicious	Browse	• 195.133.18.211
	D3mOH96307.exe	Get hash	malicious	Browse	• 194.87.206.125
	05hZwJ8NB7	Get hash	malicious	Browse	• 193.124.16.215
	EC833E37264C772DE689338F22B307BC864390E62D1CD.exe	Get hash	malicious	Browse	• 31.31.198.18
	Jessica Ohnesorge'CV.exe	Get hash	malicious	Browse	• 195.133.18.211
	Change Of Registration Form.exe	Get hash	malicious	Browse	• 195.133.18.211
	#U0401XCEL.xlam	Get hash	malicious	Browse	• 31.31.198.180
	#U0401XCEL.xlam	Get hash	malicious	Browse	• 31.31.198.180
	Payment invoice.exe	Get hash	malicious	Browse	• 195.133.18.211
	tt copy 200393903.exe	Get hash	malicious	Browse	• 194.58.112.174
	Wire Transfer Slip.exe	Get hash	malicious	Browse	• 195.133.18.211
	yaflq3D6ft	Get hash	malicious	Browse	• 195.133.18.213
DATACENTERRO	TMR590241368.exe	Get hash	malicious	Browse	• 194.85.248.115
	vIyyHkRXJn	Get hash	malicious	Browse	• 194.85.250.154
	267A80yAhp	Get hash	malicious	Browse	• 194.85.250.154
	QJYxAALd23	Get hash	malicious	Browse	• 194.85.250.154
	z4bJfjXDDQ	Get hash	malicious	Browse	• 194.85.250.154
	XXaLHoecGp	Get hash	malicious	Browse	• 194.85.250.154
	AGiCic4uDz	Get hash	malicious	Browse	• 194.85.250.154
	3B3BMxYG8n	Get hash	malicious	Browse	• 194.85.250.154
	6WMo1OYmk3	Get hash	malicious	Browse	• 194.85.250.154
	dycuTng5W8	Get hash	malicious	Browse	• 194.85.250.154
	xINX4f5M8s	Get hash	malicious	Browse	• 194.85.250.154
	SSIuSyaBAF	Get hash	malicious	Browse	• 194.85.250.154
	IMG600094173852.exe	Get hash	malicious	Browse	• 194.85.248.115
	cdQc14SeRu	Get hash	malicious	Browse	• 194.85.248.128
	t5dIUw7hgh	Get hash	malicious	Browse	• 194.85.248.128
	9hYMlirC3x	Get hash	malicious	Browse	• 194.85.248.128
	qd7l0rgtfU	Get hash	malicious	Browse	• 194.85.248.128
	aKU4GDKdTZ	Get hash	malicious	Browse	• 194.85.248.128
	oGszHCs1c7	Get hash	malicious	Browse	• 194.85.248.128
	8xj3h1p4UR	Get hash	malicious	Browse	• 194.85.248.128

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\CV.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	431104
Entropy (8bit):	7.8927039026454215
Encrypted:	false
SSDEEP:	6144:EimL+T2bm+Ds2n+/10GrM2cwktwooxz6MuDHWfqvfNP80/lg82D6F2:7Q5yDY+/1tcwYa6HD7vfa0tP5A
MD5:	DE2D175988E8D0E1D9C37482FB37C66C
SHA1:	D4E7BACEA5B7EE3DEB72F73CFF98B286661F612E
SHA-256:	37649A092C0AD878F4FB8D8578C2E7CA110360BA1575E0697BAF1EFA8E5CB409
SHA-512:	A9B300CDDDCA05FF8235DEFD5718C4F491D94F2F8840DBDA81E874C69AB2049E082177E439B2A3AAC5AC1D3BC214B038F4E38FE454CE57077DE25220BBE2E5A1
Malicious:	**true**
Reputation:	low

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...O..a.....0..... .....@.. ....@.....X...O..... ....H.....text...0.... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....`...C.....n...x.....0..7.....r...p(....s.....+.....X....i2..o.....+...*..0.....r...p..(.....9.....(.....s.....s.. .....8.....-...o....1...o....]...+.....,...o.....,...o.....+.....,%...o.....,...o....o.....,...o.....+.....,.....o.....X.....i?W.....o.....8.....(.....,....o...,....o.... .]...+.....,...o!...&.....+3.....o.....

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\CV.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**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\CV.exe.log	
Process:	C:\Users\user\Desktop\CV.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_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\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_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\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\CV.exe
File Type:	data
Category:	modified

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Size (bytes):	232
Entropy (8bit):	7.117516745217376
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7V9NhyleajI0fuONKcpMe5i:X4LEnybgCFCtvd7V9NYRj+GONKaMv
MD5:	CF55DF705B79F961ED069D8E84D2AF1C
SHA1:	574CDF36753CF356A25872BCCAA3CC6FFCD5D23F
SHA-256:	DF982E10764D21FCB1469EB6EA1175AC69544C68900B0DD8C79A0FE8A8F300F5
SHA-512:	518A037DF1D6FBC8A296DA5B96B67E073FB1F674090AFE3243E52A65B169DE35FC041C2C05F7EEF9EC74A0100A422E53B3D7D920E5ADF6CE42B82FE94244F5E
Malicious:	false
Reputation:	moderate, very likely benign file
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...Q.F...@.h.....y.[....e..<..n....B...PP...azZ).~..Uj.>..H.b.O..AX.E.S&.O.k.3O'.Lge...$..teI....Hw.CT.].Z.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\CV.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:gcntn:g4t
MD5:	09C4C91F5364F32EF3A66B193BEA2356
SHA1:	FA2B1407EB49037BD09F6ABBC2246412EEAF2E68
SHA-256:	AB67530DE412585A0B18BECBF5502466C563397A87E30429D52ED39EBC575A4D
SHA-512:	391C5AD23773CC4F6F49AC77231C5E9EE198857B4559E5FF75B0CA44640792F0E23BA67B241F8E7B7AB61B3641DD748941A42930A5A034C74667864E28548FD6
Malicious:	**true**
Reputation:	low
Preview:	r.D.?..H

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.8927039026454215
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	CV.exe
File size:	431104
MD5:	de2d175988e8d0e1d9c37482fb37c66c
SHA1:	d4e7bacea5b7ee3deb72f73cff98b286661f612e
SHA256:	37649a092c0ad878f4fb8d8578c2e7ca110360ba1575e0697baf1efa8e5cb409
SHA512:	a9b300cdddca05ff8235defd5718c4f491d94f2f8840dbda81e874c69ab2049e082177e439b2a3aac5ac1d3bc214b038f4e38fe454ce57077de25220bbe2e5a1
SSDEEP:	6144:EimL+T2bm+Ds2n+/10GrM2cwktwooxz6MuDHWfqvfNP80/lg82D6F2:7Q5yDY+/1tcwYa6HD7vfa0tP5A
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...O..a.....0..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x46a5aa
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:	0x619D974F [Wed Nov 24 01:37:19 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	0x68630	0x68800	False	0.920347076854	PGP symmetric key encrypted data - Plaintext or unencrypted data	7.90812052873	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x6c000	0x610	0x800	False	0.33154296875	data	3.42607921431	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6e000	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
11/24/21-03:43:08.212325	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57459	8.8.8.8	192.168.2.3
11/24/21-03:43:11.559225	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49742	1187	192.168.2.3	194.85.248.250
11/24/21-03:43:19.257828	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49743	1187	192.168.2.3	194.85.248.250
11/24/21-03:43:24.104401	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52806	8.8.8.8	192.168.2.3
11/24/21-03:43:43.590776	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53910	8.8.8.8	192.168.2.3
11/24/21-03:43:43.622080	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49747	1187	192.168.2.3	194.85.248.250
11/24/21-03:43:50.997879	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49763	1187	192.168.2.3	194.85.248.250

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/24/21-03:43:57.357526	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49786	1187	192.168.2.3	194.85.248.250
11/24/21-03:44:06.603088	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49788	1187	192.168.2.3	194.85.248.250
11/24/21-03:44:11.301772	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49794	1187	192.168.2.3	194.85.248.250
11/24/21-03:44:17.806794	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53777	8.8.8.8	192.168.2.3
11/24/21-03:44:20.840746	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49799	1187	192.168.2.3	194.85.248.250

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 24, 2021 03:43:08.191291094 CET	192.168.2.3	8.8.8.8	0x1cd2	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 03:43:19.204021931 CET	192.168.2.3	8.8.8.8	0x66ac	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 03:43:24.082745075 CET	192.168.2.3	8.8.8.8	0x6587	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 03:43:43.569127083 CET	192.168.2.3	8.8.8.8	0x6966	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 03:43:50.935333967 CET	192.168.2.3	8.8.8.8	0x9bd	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 03:43:57.308087111 CET	192.168.2.3	8.8.8.8	0x46e	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 03:44:03.538379908 CET	192.168.2.3	8.8.8.8	0xa1bf	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 03:44:11.241858959 CET	192.168.2.3	8.8.8.8	0x9e71	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 03:44:17.786855936 CET	192.168.2.3	8.8.8.8	0x8b0a	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 24, 2021 03:43:08.212325096 CET	8.8.8.8	192.168.2.3	0x1cd2	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 03:43:19.226371050 CET	8.8.8.8	192.168.2.3	0x66ac	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 03:43:24.104401112 CET	8.8.8.8	192.168.2.3	0x6587	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 03:43:43.590775967 CET	8.8.8.8	192.168.2.3	0x6966	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 03:43:50.955516100 CET	8.8.8.8	192.168.2.3	0x9bd	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 03:43:57.327816963 CET	8.8.8.8	192.168.2.3	0x46e	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 03:44:03.558403015 CET	8.8.8.8	192.168.2.3	0xa1bf	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 03:44:11.262809038 CET	8.8.8.8	192.168.2.3	0x9e71	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 03:44:17.806793928 CET	8.8.8.8	192.168.2.3	0x8b0a	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: CV.exe PID: 4020 Parent PID: 1744

General

Start time:	03:42:56
Start date:	24/11/2021
Path:	C:\Users\user\Desktop\CV.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\CV.exe"
Imagebase:	0x790000
File size:	431104 bytes
MD5 hash:	DE2D175988E8D0E1D9C37482FB37C66C
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: 00000000.00000002.290046292.0000000002E71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.290082065.0000000002E95000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.291903839.0000000003E71000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.291903839.0000000003E71000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.291903839.0000000003E71000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: CV.exe PID: 360 Parent PID: 4020

General

Start time:	03:43:02
Start date:	24/11/2021
Path:	C:\Users\user\Desktop\CV.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\CV.exe
Imagebase:	0x610000
File size:	431104 bytes
MD5 hash:	DE2D175988E8D0E1D9C37482FB37C66C
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: 00000005.00000000.287075484.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.287075484.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.287075484.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000000.287499193.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.287499193.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.287499193.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000000.288052990.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.288052990.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.288052990.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000000.286632471.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.286632471.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.286632471.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: dhcpmon.exe PID: 5628 Parent PID: 3352

General

Start time:	03:43:15
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:	0x240000
File size:	431104 bytes
MD5 hash:	DE2D175988E8D0E1D9C37482FB37C66C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000A.00000002.325873810.00000000029F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.328775816.00000000039F1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.328775816.00000000039F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.328775816.00000000039F1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000A.00000002.325943283.0000000002A17000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: dhcpmon.exe PID: 1664 Parent PID: 5628

General

Start time:	03:43:16
Start date:	24/11/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x10000
File size:	431104 bytes
MD5 hash:	DE2D175988E8D0E1D9C37482FB37C66C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: dhcpmon.exe PID: 5348 Parent PID: 5628

General

Start time:	03:43:17
Start date:	24/11/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x10000
File size:	431104 bytes
MD5 hash:	DE2D175988E8D0E1D9C37482FB37C66C
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: dhcpmon.exe PID: 7096 Parent PID: 5628

General

Start time:	03:43:19
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:	0xa40000
File size:	431104 bytes
MD5 hash:	DE2D175988E8D0E1D9C37482FB37C66C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000000.323309609.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000000.323309609.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000000.323309609.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000000.322328292.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000000.322328292.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000000.322328292.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.338892529.0000000003211000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.338892529.0000000003211000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.338928504.0000000004211000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.338928504.0000000004211000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000000.322810858.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000000.322810858.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000000.322810858.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000000.323801739.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000000.323801739.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000000.323801739.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.338247555.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.338247555.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.338247555.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: WMIADAP.exe PID: 7096 Parent PID: 2156

General

Start time:	03:45:01
Start date:	24/11/2021
Path:	C:\Windows\System32\wbem\WMIADAP.exe
Wow64 process (32bit):	
Commandline:	wmiadap.exe /F /T /R
Imagebase:	
File size:	177664 bytes
MD5 hash:	9783D0765F31980950445DFD40DB15DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

Code Analysis