ID: 527831
Sample Name: CV.exe
Cookbook: default.jbs
Time: 13:52:12
Date: 24/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

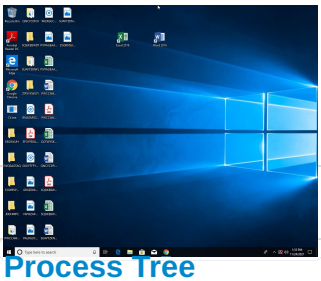
Windows Analysis Report CV.exe

Overview

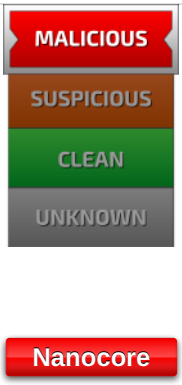
General Information

Sample Name:	CV.exe
Analysis ID:	527831
MD5:	d1edb7cd80f2034.
SHA1:	63c1bffd57bb0e4..
SHA256:	b186f6738901b0c.
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



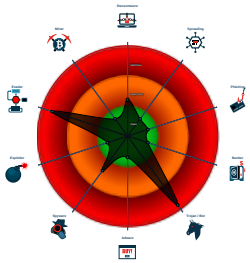
Nanocore

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Tries to detect sandboxes and other…
- Machine Learning detection for samp…

Classification



Process Tree

- **System is w10x64**
- CV.exe (PID: 2060 cmdline: "C:\Users\user\Desktop\CV.exe" MD5: D1EDB7CD80F20347FA00F25792241EA5)
  - CV.exe (PID: 5936 cmdline: C:\Users\user\Desktop\CV.exe MD5: D1EDB7CD80F20347FA00F25792241EA5)
  - CV.exe (PID: 1464 cmdline: C:\Users\user\Desktop\CV.exe MD5: D1EDB7CD80F20347FA00F25792241EA5)
- dhcpmon.exe (PID: 1096 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: D1EDB7CD80F20347FA00F25792241EA5)
  - dhcpmon.exe (PID: 5368 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: D1EDB7CD80F20347FA00F25792241EA5)
- **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
0000000F.00000002.355813819.00000000034D1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000F.00000002.355813819.00000000034D1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x238a7:$a: NanoCore • 0x23900:$a: NanoCore • 0x2393d:$a: NanoCore • 0x239b6:$a: NanoCore • 0x23909:$b: ClientPlugin • 0x23946:$b: ClientPlugin • 0x24244:$b: ClientPlugin • 0x24251:$b: ClientPlugin • 0x1b0fb:$e: KeepAlive • 0x23d91:$g: LogClientMessage • 0x23d11:$i: get_Connected • 0x158d9:$j: #=q • 0x15909:$j: #=q • 0x15945:$j: #=q • 0x1596d:$j: #=q • 0x1599d:$j: #=q • 0x159cd:$j: #=q • 0x159fd:$j: #=q • 0x15a2d:$j: #=q • 0x15a49:$j: #=q • 0x15a79:$j: #=q
00000000.00000002.301343560.000000000299 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
0000000C.00000000.297944815.000000000040 2000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000C.00000000.297944815.000000000040 2000.00000040.00000001.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.3107a18.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
0.2.CV.exe.3a064a0.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.CV.exe.3a064a0.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
0.2.CV.exe.3a064a0.2.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.CV.exe.3a064a0.2.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xe0f5:$a: NanoCore • 0xe105:$a: NanoCore • 0xe339:$a: NanoCore • 0xe34d:$a: NanoCore • 0xe38d:$a: NanoCore • 0xe154:$b: ClientPlugin • 0xe356:$b: ClientPlugin • 0xe396:$b: ClientPlugin • 0xe27b:$c: ProjectData • 0xec82:$d: DESCrypto • 0x1664e:$e: KeepAlive • 0x1463c:$g: LogClientMessage • 0x10837:$i: get_Connected • 0xefb8:$j: #=q • 0xefe8:$j: #=q • 0xf004:$j: #=q • 0xf034:$j: #=q • 0xf050:$j: #=q • 0xf06c:$j: #=q • 0xf09c:$j: #=q • 0xf0b8:$j: #=q
Click to see the 84 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 submitted file

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:

Snort IDS alert for network traffic (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

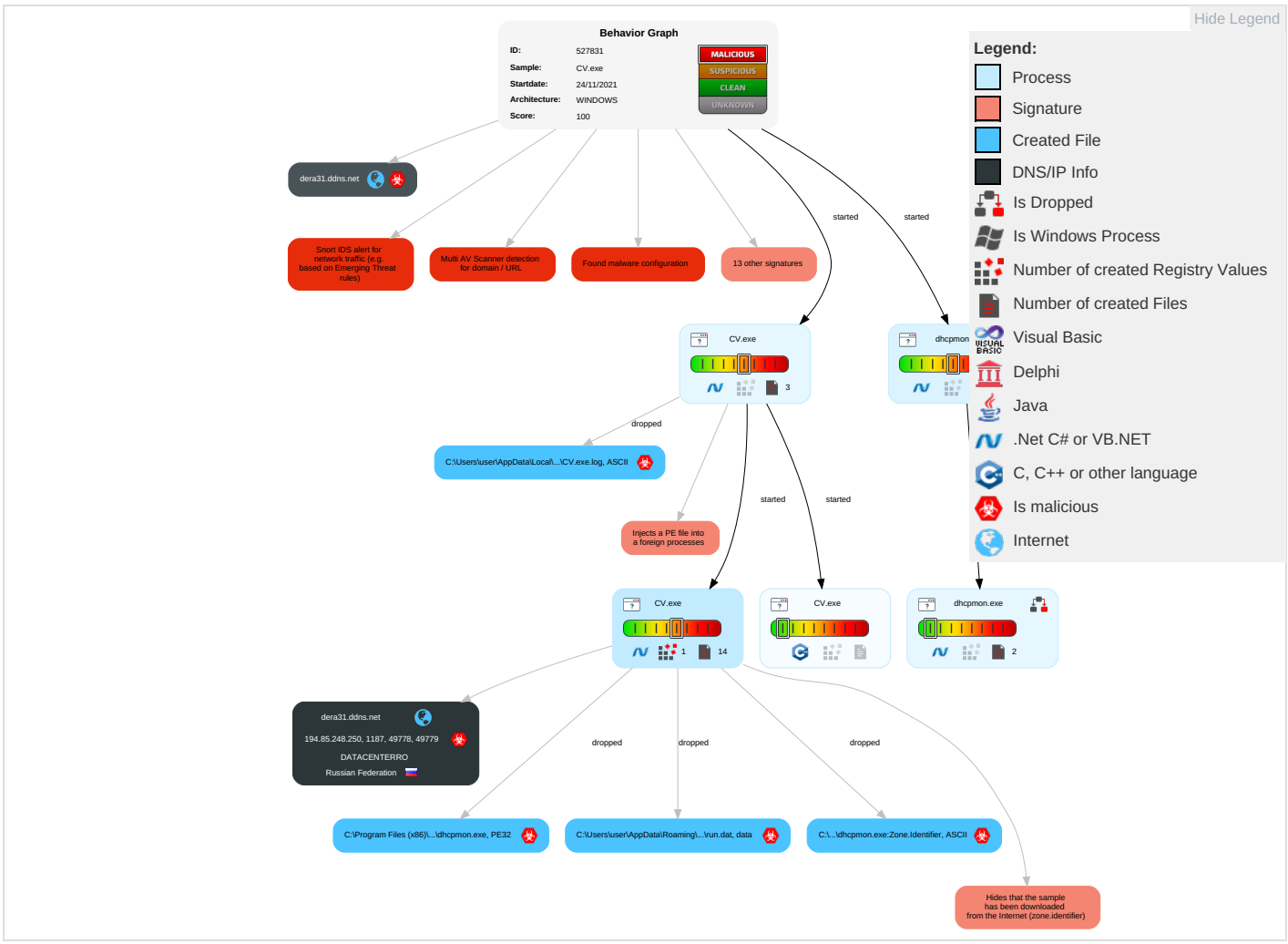
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Access Token Manipulation 1	Masquerading 2	Input Capture 2 1	Security Software Discovery 2 2 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
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	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 4 1	Security Account Manager	Virtualization/Sandbox Evasion 4 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1
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
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
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Timestomp 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

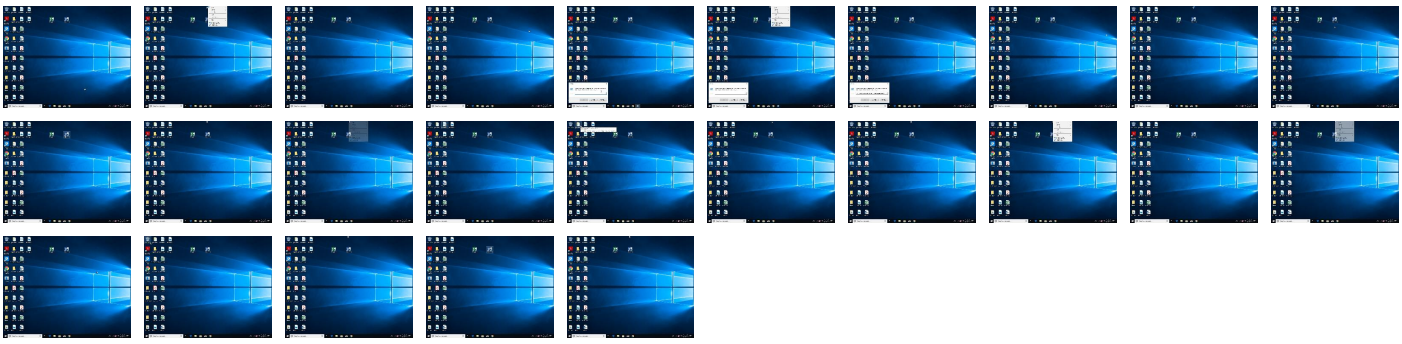
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
CV.exe	18%	ReversingLabs	ByteCode-MSIL.Trojan.Zilla	
CV.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:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	18%	ReversingLabs	ByteCode-MSIL.Trojan.Zilla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
15.0.dhcpmon.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.0.dhcpmon.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.0.dhcpmon.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.0.dhcpmon.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.0.CV.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.0.CV.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
12.0.CV.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.0.dhcpmon.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.0.CV.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.0.CV.exe.400000.12.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.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.comfi-f	0%	Avira URL Cloud	safe	
http://www.monotype.H	0%	Avira URL Cloud	safe	
http://www.carterandcone.comq	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/J	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/s	0%	Avira URL Cloud	safe	
http://www.carterandcone.comtud	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
dera31.ddns.net	0%	Avira URL Cloud	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comB.TTF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Vers	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comrsiva	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.commm	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.tiro.com(	0%	Avira URL Cloud	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	
195.133.18.211	0%	Avira URL Cloud	safe	
http://en.wikipK	0%	Avira URL Cloud	safe	
http://www.goodfont.co.krf	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnsq	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Vet	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
194.85.248.250	dera31.ddns.net	Russian Federation		35478	DATACENTERRO	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	527831
Start date:	24.11.2021
Start time:	13:52:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 33s
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:	31
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@8/8@20/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 3.4% (good quality ratio 2.7%) • Quality average: 61.8% • Quality standard deviation: 32.9%
HCA Information:	• Successful, ratio: 85% • 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
13:53:09	API Interceptor	896x Sleep call for process: CV.exe modified
13:53:18	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
13:53:27	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
194.85.248.250	INV.exe	Get hash	malicious	Browse	
	CV.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
dera31.ddns.net	INV.exe	Get hash	malicious	Browse	• 194.85.248.250
	CV.exe	Get hash	malicious	Browse	• 194.85.248.250
	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
DATACENTERRO	INV.exe	Get hash	malicious	Browse	• 194.85.248.250
	CV.exe	Get hash	malicious	Browse	• 194.85.248.250
	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

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):	608256
Entropy (8bit):	7.801754700760465
Encrypted:	false
SSDEEP:	12288:ZNtD00tT0tvUHZMzxSC3rZc9/iz0YhmeBJv3ej9KUrx9jgrv:3C0tqUESOrZ5game3Oj9fdGr
MD5:	D1EDB7CD80F20347FA00F25792241EA5
SHA1:	63C1BFFD57BB0E4CC32C53ECCCE4916FEA2AF18D
SHA-256:	B186F6738901B0CF5824A3E3789AF05342F414F30AD10D615A2B1A4203280627
SHA-512:	23A4AB61160F9C63E7FA1BCA39FBF7683297DF43CECBCEBE0A4990B7FD8135D249BF4AC8A13187A2AA04066B188F61F86614684B7A24DB87FF8EDB9992AF4714
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 18%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....z.....0..<.....[... ...`....@.. ..... ..@.....T[..O...`.....8[..... ....H.....text....;... ...<..... ..`.rsrc.....`.....>.....@..@.rel oc.....F.....@..B.....[.....H.....L.....y...h.....r...p}.....r...p(....}.....}.....(.....(.....*..0..f.....{....o....o.....r...p(....}.....+...{....o.....{.... ..o....&...X...{.....i....-..{....r!..po.....*...0.....{....o....(.....,..r#..p(....&..+[..{....o.....+=..o.....(.....,!.rU..p(....&.{....r!..po.....+....X...o....2...+..*...0.....r...p(....}.....{....(..... {.....s!.....o".....+U..{.....{....o#....o$...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:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

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

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\CV.exe
File Type:	data
Category:	modified
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:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:RTt:ht
MD5:	4495EBD38CC409948B11222A87339B62
SHA1:	7586E6C3CAD711FC3837B4064C14B741124C44B6
SHA-256:	8BF390A9F9ADBB0972125302C00F3328117DA280DDE757EEF3D01D215BE04369
SHA-512:	478925A733767D391B80A975021FB50DA33B235B2341CFDB39AC3F81D5F022AA6C014DB79936EDE918BEA040AF94F96739309690CAAE3BC086F7933EF044D5F8
Malicious:	**true**
Reputation:	low
Preview:	.Ww...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\CV.exe
File Type:	data
Category:	dropped
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\CV.exe
File Type:	data
Category:	dropped
Size (bytes):	412824
Entropy (8bit):	**7.999596596836973**
Encrypted:	**true**
SSDEEP:	12288:8I9gnTsbHFPV7iGQVIB8XBLeMb2qLB1rRxH:8QbHFxB8gMiQRxH
MD5:	C9DF8F232494E30402189920360F0907
SHA1:	F181CE82F56D624408AFD68FE82A6A9D77A23383
SHA-256:	ADA0DF11313089119C94406A8EF300442BC1F42ACFA44DF840F5FA9C732026C3
SHA-512:	5415791498 43E1C08AEAA60DCC5C379D74D87BD7538B6E84D6476E79A65324BB023DFEE5E44F8BF1E794B94F83E5902FE84F4722CFEED37B1C426B97F4F4376
Malicious:	false
Preview:	FF)d6...0...{..X$.E.v>..'9}G>W.S.K.....(..">b/(..m...d....G1.Fwf..1jr..2.i.K}..,.W....;;..y..U.b.O...1.kb...u...4.]7...D.W..Ci..k.U..+...%..D.[.W..6/.....j...w..4p...w...e...v..E...CV'.<... .YN.....t2.....p.k..6..[...N.l...Dg..L....O>.H...^..8Kifc....%...yX....e.....y.-O...%.....m_..v..5.A.3.8...A.;.\|.3p .yf('..Z.2Sv...Q.&.4...80.h....7u.a..~[....zr.V:cP:f..cy.f....F.b@.... ....Hu.fs.....b...l.V..u...p.p.h.S..'...*?.....5.JMa.....s,.<k.bo.V.)<.[R.-.....myP._Y.$...#dS....XN..IE.....Q..w.s`.....<.t....`.T<.....C.....<..e.....p&...F..{. ,nA..".m..$.H D`.:...g.....8...P@/PCxU8>{.....1\|_fX.....t.:.....X.\..<..._....7u...2.S2Rx...'../.4..0:P...i....DY..]....R....)..0F...M..w..f.....EV.T...v.r..D.K..Yuz \.K+.....y.`...<.!.C...R...C.. s:)..=vL..$}6..1...?A(DJ.....t..u..xg{.C$8..k.P0..f..D8..g.b..'es....pX..q..[..@32u..1.`.hy.B.*;.c.....w.....o...Z.s.d.$.j..!%v..2....{..P...CP.I.X...}w.".\-

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.801754700760465
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • 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% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	CV.exe
File size:	608256
MD5:	d1edb7cd80f20347fa00f25792241ea5
SHA1:	63c1bffd57bb0e4cc32c53eccce4916fea2af18d
SHA256:	b186f6738901b0cf5824a3e3789af05342f414f30ad10d615a2b1a4203280627
SHA512:	23a4ab61160f9c63e7fa1bca39fbf7683297df43cecbcebe0a4990b7fd8135d249bf4ac8a13187a2aa04066b188f61f86614684b7a24db87ff8edb9992af4714
SSDEEP:	12288:ZNtD00tT0tvUHZMzxSC3rZc9/iz0YhmeBJv3ej9KUrx9jgrv:3C0tqUESOrZ5game3Oj9fdGr
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....z.....0..<.....[... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x495ba6
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

General

Time Stamp:	0xD79B7A1C [Wed Aug 16 18:59:40 2084 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	0x93bbc	0x93c00	False	0.883513113367	data	7.81416898043	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x96000	0x61c	0x800	False	0.32958984375	data	3.44757176979	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x98000	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
11/24/21-13:53:17.975419	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49572	8.8.8.8	192.168.2.3
11/24/21-13:53:18.055737	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49778	1187	192.168.2.3	194.85.248.250
11/24/21-13:53:23.356626	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60823	8.8.8.8	192.168.2.3
11/24/21-13:53:23.388450	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49779	1187	192.168.2.3	194.85.248.250
11/24/21-13:53:28.253885	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49780	1187	192.168.2.3	194.85.248.250
11/24/21-13:53:32.911509	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55102	8.8.8.8	192.168.2.3
11/24/21-13:53:32.943821	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49781	1187	192.168.2.3	194.85.248.250
11/24/21-13:53:37.735223	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49784	1187	192.168.2.3	194.85.248.250
11/24/21-13:53:45.423244	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49785	1187	192.168.2.3	194.85.248.250
11/24/21-13:53:50.000725	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49786	1187	192.168.2.3	194.85.248.250
11/24/21-13:53:58.498083	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49788	1187	192.168.2.3	194.85.248.250
11/24/21-13:54:04.826647	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49789	1187	192.168.2.3	194.85.248.250
11/24/21-13:54:09.406079	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64367	8.8.8.8	192.168.2.3
11/24/21-13:54:09.438255	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49806	1187	192.168.2.3	194.85.248.250

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/24/21-13:54:15.518024	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55393	8.8.8.8	192.168.2.3
11/24/21-13:54:15.684471	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49825	1187	192.168.2.3	194.85.248.250
11/24/21-13:54:22.080250	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63456	8.8.8.8	192.168.2.3
11/24/21-13:54:22.124316	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49831	1187	192.168.2.3	194.85.248.250
11/24/21-13:54:28.169710	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58540	8.8.8.8	192.168.2.3
11/24/21-13:54:28.198987	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49833	1187	192.168.2.3	194.85.248.250
11/24/21-13:54:34.155830	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55108	8.8.8.8	192.168.2.3
11/24/21-13:54:34.218813	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49842	1187	192.168.2.3	194.85.248.250
11/24/21-13:54:41.244944	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49857	1187	192.168.2.3	194.85.248.250
11/24/21-13:54:47.179558	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49858	1187	192.168.2.3	194.85.248.250
11/24/21-13:54:54.239251	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49860	1187	192.168.2.3	194.85.248.250
11/24/21-13:55:00.250467	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49861	1187	192.168.2.3	194.85.248.250
11/24/21-13:55:06.162115	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49862	1187	192.168.2.3	194.85.248.250
11/24/21-13:55:12.785801	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49863	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 13:53:17.945394039 CET	192.168.2.3	8.8.8.8	0x36c2	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 13:53:23.335347891 CET	192.168.2.3	8.8.8.8	0x3fba	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 13:53:28.203588009 CET	192.168.2.3	8.8.8.8	0x6d40	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 13:53:32.891006947 CET	192.168.2.3	8.8.8.8	0xace7	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 13:53:37.682377100 CET	192.168.2.3	8.8.8.8	0xcad5	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 13:53:45.372145891 CET	192.168.2.3	8.8.8.8	0xbb0a	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 13:53:49.949804068 CET	192.168.2.3	8.8.8.8	0x78f2	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 13:53:57.280015945 CET	192.168.2.3	8.8.8.8	0x68a4	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 13:54:04.746898890 CET	192.168.2.3	8.8.8.8	0xa2b6	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 13:54:09.384938955 CET	192.168.2.3	8.8.8.8	0xf78d	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 13:54:15.495414019 CET	192.168.2.3	8.8.8.8	0x4b23	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 13:54:22.059016943 CET	192.168.2.3	8.8.8.8	0xd0aa	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 13:54:28.145822048 CET	192.168.2.3	8.8.8.8	0x3c50	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 13:54:34.134350061 CET	192.168.2.3	8.8.8.8	0xdc7a	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 13:54:41.195228100 CET	192.168.2.3	8.8.8.8	0x13ef	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 24, 2021 13:54:47.129384041 CET	192.168.2.3	8.8.8.8	0x2da7	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 13:54:54.160470963 CET	192.168.2.3	8.8.8.8	0x2883	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 13:55:00.192150116 CET	192.168.2.3	8.8.8.8	0xa977	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 13:55:06.110857964 CET	192.168.2.3	8.8.8.8	0x3def	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 13:55:12.701934099 CET	192.168.2.3	8.8.8.8	0xf76f	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 13:53:17.975419044 CET	8.8.8.8	192.168.2.3	0x36c2	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 13:53:23.356626034 CET	8.8.8.8	192.168.2.3	0x3fba	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 13:53:28.221946955 CET	8.8.8.8	192.168.2.3	0x6d40	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 13:53:32.911509037 CET	8.8.8.8	192.168.2.3	0xace7	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 13:53:37.703850031 CET	8.8.8.8	192.168.2.3	0xcad5	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 13:53:45.392890930 CET	8.8.8.8	192.168.2.3	0xbb0a	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 13:53:49.969712019 CET	8.8.8.8	192.168.2.3	0x78f2	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 13:53:57.299962044 CET	8.8.8.8	192.168.2.3	0x68a4	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 13:54:04.766309023 CET	8.8.8.8	192.168.2.3	0xa2b6	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 13:54:09.406079054 CET	8.8.8.8	192.168.2.3	0xf78d	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 13:54:15.518023968 CET	8.8.8.8	192.168.2.3	0x4b23	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 13:54:22.080250025 CET	8.8.8.8	192.168.2.3	0xd0aa	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 13:54:28.169709921 CET	8.8.8.8	192.168.2.3	0x3c50	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 13:54:34.155829906 CET	8.8.8.8	192.168.2.3	0xdc7a	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 13:54:41.215020895 CET	8.8.8.8	192.168.2.3	0x13ef	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 13:54:47.149298906 CET	8.8.8.8	192.168.2.3	0x2da7	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 13:54:54.178567886 CET	8.8.8.8	192.168.2.3	0x2883	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 13:55:00.212667942 CET	8.8.8.8	192.168.2.3	0xa977	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 13:55:06.130167961 CET	8.8.8.8	192.168.2.3	0x3def	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 13:55:12.723361969 CET	8.8.8.8	192.168.2.3	0xf76f	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: 2060 Parent PID: 5628

General

Start time:	13:53:02
Start date:	24/11/2021
Path:	C:\Users\user\Desktop\CV.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\CV.exe"
Imagebase:	0x2e0000
File size:	608256 bytes
MD5 hash:	D1EDB7CD80F20347FA00F25792241EA5
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: 00000000.00000002.301343560.0000000002991000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.301367377.00000000029AE000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.302046756.0000000003991000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.302046756.0000000003991000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.302046756.0000000003991000.00000004.00000001.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: 5936 Parent PID: 2060

General

Start time:	13:53:09
Start date:	24/11/2021
Path:	C:\Users\user\Desktop\CV.exe

Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\CV.exe
Imagebase:	0x3b0000
File size:	608256 bytes
MD5 hash:	D1EDB7CD80F20347FA00F25792241EA5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: CV.exe PID: 1464 Parent PID: 2060

General

Start time:	13:53:10
Start date:	24/11/2021
Path:	C:\Users\user\Desktop\CV.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\CV.exe
Imagebase:	0x740000
File size:	608256 bytes
MD5 hash:	D1EDB7CD80F20347FA00F25792241EA5
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: 0000000C.00000000.297944815.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000000.297944815.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000000.297944815.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000000.298501077.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000000.298501077.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000000.298501077.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000000.299111610.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000000.299111610.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000000.299111610.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000000.297385774.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000000.297385774.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000000.297385774.0000000000402000.00000040.00000001.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: 1096 Parent PID: 3352

General

Start time:	13:53:26
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:	0x960000
File size:	608256 bytes
MD5 hash:	D1EDB7CD80F20347FA00F25792241EA5
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: 0000000E.00000002.339696473.0000000003101000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.340507265.0000000004101000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.340507265.0000000004101000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.340507265.0000000004101000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000E.00000002.339762947.000000000311E000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 18%, ReversingLabs
Reputation:	low

File Activities — Show Windows behavior

File Created

File Written

File Read

Analysis Process: dhcpmon.exe PID: 5368 Parent PID: 1096

General

Start time:	13:53:28
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:	0xe70000
File size:	608256 bytes
MD5 hash:	D1EDB7CD80F20347FA00F25792241EA5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.355813819.00000000034D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.355813819.00000000034D1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000000.335021973.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000000.335021973.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000000.335021973.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.355853296.00000000044D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.355853296.00000000044D1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.352520108.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.352520108.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.352520108.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000000.336503359.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000000.336503359.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000000.336503359.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000000.335575660.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000000.335575660.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000000.335575660.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000000.337167425.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000000.337167425.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000000.337167425.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis