ID: 508724
Sample Name: CV.exe
Cookbook: default.jbs
Time: 14:59:11
Date: 25/10/2021
Version: 33.0.0 White Diamond

Table of Contents

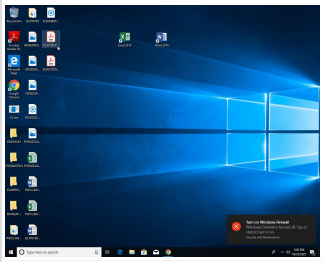
Windows Analysis Report CV.exe

Overview

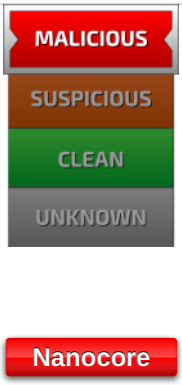
General Information

Sample Name:	CV.exe
Analysis ID:	508724
MD5:	5d9fed85f31d020..
SHA1:	df89b8bfedfd260…
SHA256:	9219aa9982516a..
Tags:	exe NanoCore
Infos:	

Most interesting Screenshot:



Detection



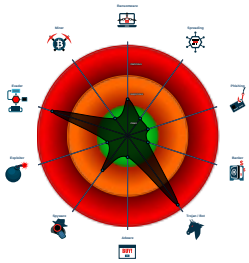
Nanocore

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…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…

Classification



Process Tree

- **System is w10x64**
- CV.exe (PID: 7020 cmdline: 'C:\Users\user\Desktop\CV.exe' MD5: 5D9FED85F31D020568F166E6291CBE7B)
  - CV.exe (PID: 7124 cmdline: C:\Users\user\Desktop\CV.exe MD5: 5D9FED85F31D020568F166E6291CBE7B)
- dhcpmon.exe (PID: 5512 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 5D9FED85F31D020568F166E6291CBE7B)
  - dhcpmon.exe (PID: 5300 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 5D9FED85F31D020568F166E6291CBE7B)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "baa1bd16-ba50-4743-8b51-41c36ee5",
  "Group": "Default",
  "Domain1": "kamuchehddhgfgf.ddns.net",
  "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": "8.8.4.453"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.349313749.0000000002E1 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000005.00000002.349313749.0000000002E1 1000.00000004.00000001.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 • 0x1b100:$e: KeepAlive • 0x23d91:$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:$j: #=q
00000000.00000002.304747743.000000000368 2000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.304713233.000000000366 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000004.00000002.337548650.0000000003E7 1000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x139c4d:$x1: NanoCore.ClientPluginHost • 0x16c46d:$x1: NanoCore.ClientPluginHost • 0x139c8a:$x2: IClientNetworkHost • 0x16c4aa:$x2: IClientNetworkHost • 0x13d7bd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcb w8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x16ffdd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 17 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.CV.exe.3667a98.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
5.2.dhcpmon.exe.3e595fe.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0x145e3:$x1: NanoCore.ClientPluginHost • 0x2d0af:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost • 0x14610:$x2: IClientNetworkHost • 0x2d0dc:$x2: IClientNetworkHost
5.2.dhcpmon.exe.3e595fe.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x145e3:$x2: NanoCore.ClientPluginHost • 0x2d0af:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0x156be:$s4: PipeCreated • 0x2e18a:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost • 0x145fd:$s5: IClientLoggingHost • 0x2d0c9:$s5: IClientLoggingHost
5.2.dhcpmon.exe.3e595fe.3.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
5.2.dhcpmon.exe.3e595fe.3.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xddf:$a: NanoCore • 0xe38:$a: NanoCore • 0xe75:$a: NanoCore • 0xeee:$a: NanoCore • 0x14599:$a: NanoCore • 0x145ae:$a: NanoCore • 0x145e3:$a: NanoCore • 0x2d065:$a: NanoCore • 0x2d07a:$a: NanoCore • 0x2d0af:$a: NanoCore • 0xe41:$b: ClientPlugin • 0xe7e:$b: ClientPlugin • 0x177c:$b: ClientPlugin • 0x1789:$b: ClientPlugin • 0x14355:$b: ClientPlugin • 0x14370:$b: ClientPlugin • 0x143a0:$b: ClientPlugin • 0x145b7:$b: ClientPlugin • 0x145ec:$b: ClientPlugin • 0x2ce21:$b: ClientPlugin • 0x2ce3c:$b: ClientPlugin
Click to see the 30 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

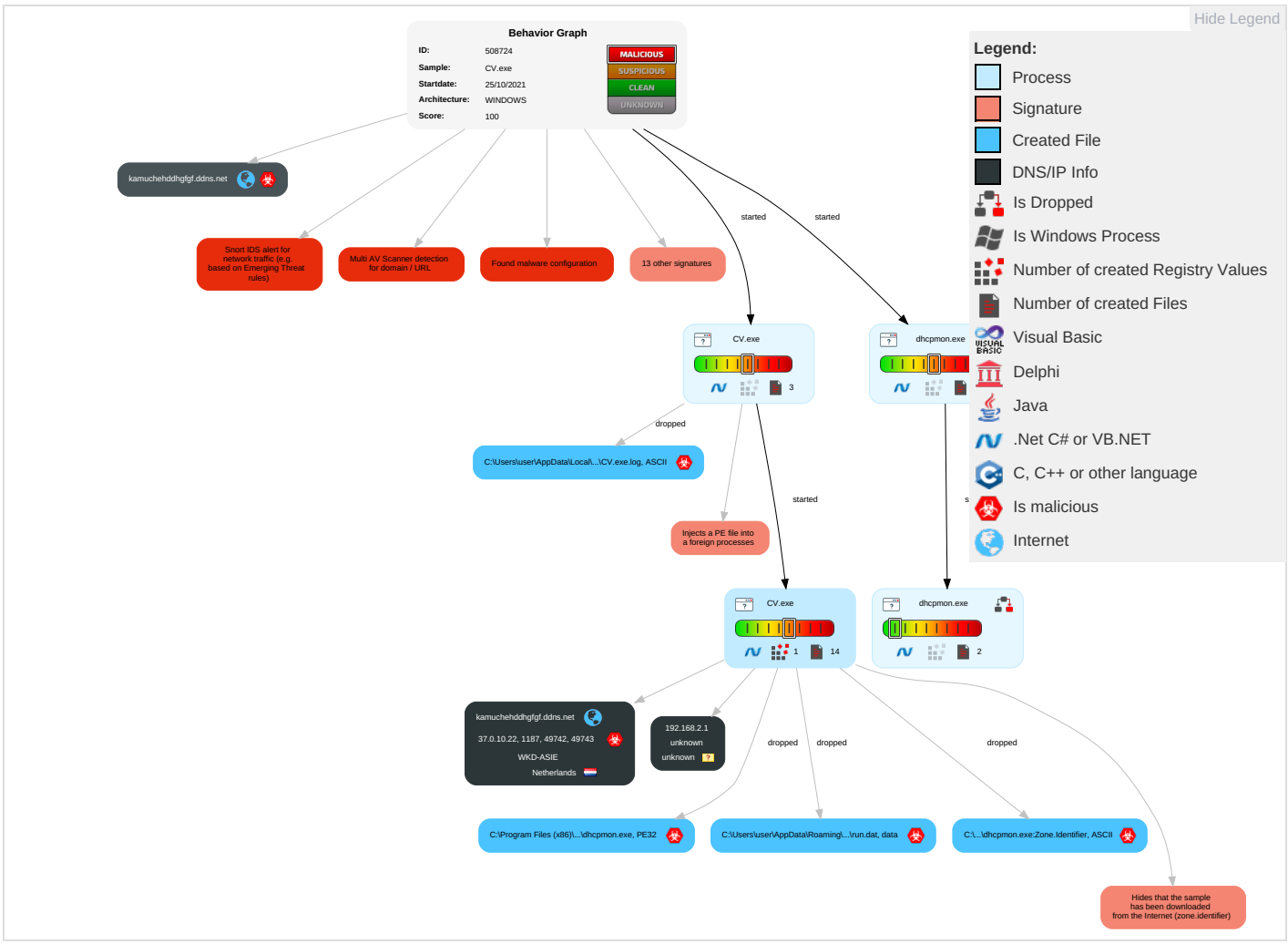
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control

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	Process Injection 1 1 2	Masquerading 2	Input Capture 2 1	Security Software Discovery 2 1 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	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
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 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)	Process Injection 1 1 2	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	Deobfuscate/Decode Files or Information 1	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

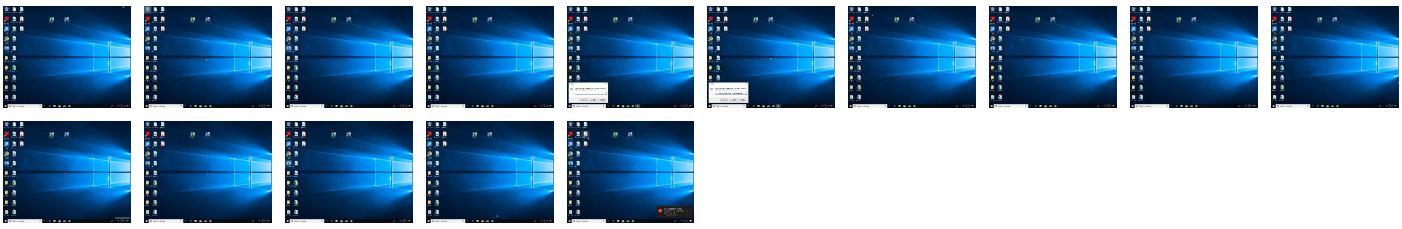
Behavior Graph



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	47%	Virustotal		Browse
CV.exe	56%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
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	56%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
kamuchehddhgfgf.ddns.net	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd#:	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdW:_L	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.fontbureau.comd9	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/W:_L	0%	Avira URL Cloud	safe	
http://www.carterandcone.comva	0%	URL Reputation	safe	
http://www.fontbureau.commsed	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/el-g	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.fontbureau.comepko	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.urwpp.de3=	0%	Avira URL Cloud	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	0%	URL Reputation	safe	
http://www.carterandcone.comcmf	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.carterandcone.com.128	0%	Avira URL Cloud	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.carterandcone.coma-eZ~	0%	Avira URL Cloud	safe	
http://www.fontbureau.comtota	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.sandoll.co.kr3~_L	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/L:	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/E:IL	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/W:_L	0%	Avira URL Cloud	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.tiro.com&=	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.goodfont.co.krm	0%	Avira URL Cloud	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.carterandcone.comnL	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comue	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.coma#:	0%	Avira URL Cloud	safe	
kamuchehddhgfgf.ddns.net	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr:~	0%	Avira URL Cloud	safe	
http://www.tiro.comlic	0%	URL Reputation	safe	
http://www.fontbureau.comzana	0%	Avira URL Cloud	safe	
http://www.carterandcone.comt	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/;:	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.goodfont.co.kry~	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cnRL%	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/x	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnva	0%	URL Reputation	safe	
http://www.fontbureau.comL:	0%	Avira URL Cloud	safe	
http://www.fontbureau.comldTF	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cne-d	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.fontbureau.comitud	0%	URL Reputation	safe	
http://www.fontbureau.comrsivo	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn//	0%	Avira URL Cloud	safe	
http://www.monotype.;9	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnl-nq	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kamuchehddhgfgf.ddns.net	37.0.10.22	true	true	• 8%, Virustotal, Browse	unknown

Contacted URLs

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

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
37.0.10.22	kamuchehddhgfgf.ddns.net	Netherlands		198301	WKD-ASIE	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	508724
Start date:	25.10.2021
Start time:	14:59:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 21s
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:	19
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@6/8@19/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.7% (good quality ratio 1.7%) • Quality average: 54% • Quality standard deviation: 42.8%
HCA Information:	• Successful, ratio: 97% • 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
15:00:13	API Interceptor	950x Sleep call for process: CV.exe modified
15:00:18	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
15:00:27	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
37.0.10.22	Debitnote-s3update.exe	Get hash	malicious	Browse	
	Purchase Order.exe	Get hash	malicious	Browse	
	Order.exe	Get hash	malicious	Browse	
	Order.exe	Get hash	malicious	Browse	
	My CV.exe	Get hash	malicious	Browse	
	Quote.exe	Get hash	malicious	Browse	
	Invoice and waybill.exe	Get hash	malicious	Browse	
	My Resume.exe	Get hash	malicious	Browse	
	Circular PSSB Parts Disc Credit Term (Dlr) Oct2021 (1).exe	Get hash	malicious	Browse	
	Circular PSSB Parts Disc Credit Term (Dlr) Oct2021 (1).exe	Get hash	malicious	Browse	
	Balance Payment.exe	Get hash	malicious	Browse	
	PURCHASE ORDER.exe	Get hash	malicious	Browse	
	Circular PSSB Parts Disc Credit Term (Dlr) s.exe	Get hash	malicious	Browse	
	T.T.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
kamuchehddhgfgf.ddns.net	Debitnote-s3update.exe	Get hash	malicious	Browse	• 37.0.10.22
	Order.exe	Get hash	malicious	Browse	• 37.0.10.22
	Order.exe	Get hash	malicious	Browse	• 37.0.10.22
	My CV.exe	Get hash	malicious	Browse	• 37.0.10.22
	Quote.exe	Get hash	malicious	Browse	• 37.0.10.22
	Invoice and waybill.exe	Get hash	malicious	Browse	• 37.0.10.22
	My Resume.exe	Get hash	malicious	Browse	• 37.0.10.22

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Circular PSSB Parts Disc Credit Term (Dlr) Oct2021 (1).exe	Get hash	malicious	Browse	• 37.0.10.22
	Circular PSSB Parts Disc Credit Term (Dlr) Oct2021 (1).exe	Get hash	malicious	Browse	• 37.0.10.22
	Balance Payment.exe	Get hash	malicious	Browse	• 37.0.10.22
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 37.0.10.22
	Circular PSSB Parts Disc Credit Term (Dlr) s.exe	Get hash	malicious	Browse	• 37.0.10.22
	T.T.exe	Get hash	malicious	Browse	• 37.0.10.22

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
WKD-ASIE	Debitnote-s3update.exe	Get hash	malicious	Browse	• 37.0.10.22
	SKypfeGItc.exe	Get hash	malicious	Browse	• 37.0.10.190
	Purchase Order.exe	Get hash	malicious	Browse	• 37.0.10.22
	HBC.exe	Get hash	malicious	Browse	• 37.0.10.15
	85QKQNr7mm.xlsx	Get hash	malicious	Browse	• 37.0.10.15
	AB948F038175411DC326A1AAD83DF48D6B656325 01551.exe	Get hash	malicious	Browse	• 37.0.8.235
	FC2E04D392AB5E508FDF6C90CE456BFD0AF6DEF1 F10A2.exe	Get hash	malicious	Browse	• 37.0.10.214
	3qZB2fO4lG.exe	Get hash	malicious	Browse	• 37.0.8.193
	365F984ABE68DDD398D7B749FB0E69B0F29DAF86 F0E3E.exe	Get hash	malicious	Browse	• 37.0.11.8
	CQUOTATION REQUEST4.scr.exe	Get hash	malicious	Browse	• 37.0.10.252
	gy6JsH7kJx.exe	Get hash	malicious	Browse	• 37.0.10.225
	About company.doc	Get hash	malicious	Browse	• 37.0.10.225
	SecuriteInfo.com.Virus.Win32.Save.a.26327.exe	Get hash	malicious	Browse	• 37.0.10.225
	ifCgoV9Ykq.exe	Get hash	malicious	Browse	• 37.0.10.225
	Agent_UDPRat.exe	Get hash	malicious	Browse	• 37.0.11.171
	Agent_UDPRat.exe	Get hash	malicious	Browse	• 37.0.11.171
	Order.exe	Get hash	malicious	Browse	• 37.0.10.22
	Order.exe	Get hash	malicious	Browse	• 37.0.10.22
	download.dat.exe	Get hash	malicious	Browse	• 37.0.10.13
	TA9015--AA-TA9015-000786-AA-TA9015--AA-TA9015.exe	Get hash	malicious	Browse	• 37.0.10.13

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):	707072
Entropy (8bit):	7.8156615612969675
Encrypted:	false
SSDEEP:	12288:iezTgmd4aCmp+SKpmH/dUytftlVyH7/i9flZ0lU3oEgUBFeg4XWq5m:iezTgmyjqfSM763t4gUBIg4v
MD5:	5D9FED85F31D020568F166E6291CBE7B
SHA1:	DF89B8BFEDFD260E648B3A8938B47DB6D2E1591C
SHA-256:	9219AA9982516A8454B770461ED85217CF3ADC6C2C2008B296720E3665B51E54
SHA-512:	0EB7B60FBBAACF29E0DDC98B776C50E5395214F75E048D61A6739C4552CD301E10CA8CC361E23762CAACFD07EBFD99058C302B5849FA7585D14614BAF39686 8
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 56%
Reputation:	low

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...0.ua..... ....@.. ....@.....K..... ....H.....text...$.... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....Z.....@.....0.....+.&. ....8U.....X. .....:D...&..(.... ....(....:-...&.. ....(...:....&...(....8>... .....E..... .....Y.....z...&...B...s...8u...& ....8.....(....?+... ....8.....(....9....& .....9....&8.....(..... ....8v...(..... ....(... ....8\...*...J+.&.....o....*.>+.&.....(....*:+.&.....o....*..+.&.. (....*>+.&.....(....*.+.&..*..+.&..*..0.....+.&..~.....eo.....

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
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

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Size (bytes):	232
Entropy (8bit):	7.117516745217376
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7V9Nhyleajl0fuONKcpMe5i:X4LEnybgCFCtvd7V9NYRj+GONKaMv
MD5:	CF55DF705B79F961ED069D8E84D2AF1C
SHA1:	574CDF36753CF356A25872BCCAA3CC6FFCD5D23F
SHA-256:	DF982E10764D21FCB1469EB6EA1175AC69544C68900B0DD8C79A0FE8A8F300F5
SHA-512:	518A037DF1D6FBC8A296DA5B96B67E073FB1F674090AFE3243E52A65B169DE35FC041C2C05F7EEF9EC74A0100A422E53B3D7D920E5ADF6CE42B82FE94244F5D E
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...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:T8n:Yn
MD5:	8B8C880350695864DF354F28F60894FD
SHA1:	0563D4B83527F6EAFB265CDABB8DF7DA25585E9B
SHA-256:	D1C3BC8F732DCA9A6C11BED615E42B2894AE6A626A70A0F521F82C5AB9291B5A
SHA-512:	ED162076CFF8CCEEE591FCC76EC298EF54B075D15CCB4A938C567DDD317EBCE968797ABDCE5B7288CCD57105DD112E950ECA82AA2DAE781BBFA153D63BC B563
Malicious:	**true**
Preview:	..8....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:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671E CB
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:	541579149843E1C08AEAA60DCC5C379D74D87BD7538B6E84D6476E79A65324BB023DFEE5E44F8BF1E794B94F83E5902FE84F4722CFEED37B1C426B97F4F4376
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.l.X...}w.".\-

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.8156615612969675
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	CV.exe
File size:	707072
MD5:	5d9fed85f31d020568f166e6291cbe7b
SHA1:	df89b8bfedfd260e648b3a8938b47db6d2e1591c
SHA256:	9219aa9982516a8454b770461ed85217cf3adc6c2c2008b296720e3665b51e54
SHA512:	0eb7b60fbbaacf29e0ddc98b776c50e5395214f75e048d61a6739c4552cd301e10ca8cc361e23762caacfd07ebfd99058c302b5849fa7585d14614baf3968638
SSDEEP:	12288:iezTgmd4aCmp+SKpmH/dUytftlVyH7/i9flZ0lU3oEgUBFeg4XWq5m:iezTgmyjqfSM763t4gUBIg4v
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...0.ua..... .....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4ade1e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61750C30 [Sun Oct 24 07:33:04 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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xabe24	0xac000	False	0.90768929415	data	7.82329709284	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xae000	0x5b0	0x600	False	0.423828125	data	4.09943837938	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb0000	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
10/25/21-15:00:18.610143	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58045	8.8.8.8	192.168.2.3
10/25/21-15:00:18.836746	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49742	1187	192.168.2.3	37.0.10.22
10/25/21-15:00:25.286725	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57459	8.8.8.8	192.168.2.3
10/25/21-15:00:25.447598	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49743	1187	192.168.2.3	37.0.10.22
10/25/21-15:00:33.199758	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54154	8.8.8.8	192.168.2.3
10/25/21-15:00:33.229011	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49746	1187	192.168.2.3	37.0.10.22
10/25/21-15:00:39.800881	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49747	1187	192.168.2.3	37.0.10.22
10/25/21-15:00:46.409065	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49748	1187	192.168.2.3	37.0.10.22
10/25/21-15:00:52.973691	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64021	8.8.8.8	192.168.2.3
10/25/21-15:00:53.003769	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49749	1187	192.168.2.3	37.0.10.22
10/25/21-15:00:59.564035	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49751	1187	192.168.2.3	37.0.10.22
10/25/21-15:01:06.817041	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49779	1187	192.168.2.3	37.0.10.22
10/25/21-15:01:13.608793	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49796	1187	192.168.2.3	37.0.10.22
10/25/21-15:01:20.781475	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49798	1187	192.168.2.3	37.0.10.22
10/25/21-15:01:26.772400	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57106	8.8.8.8	192.168.2.3
10/25/21-15:01:26.800869	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49799	1187	192.168.2.3	37.0.10.22
10/25/21-15:01:32.852409	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49823	1187	192.168.2.3	37.0.10.22
10/25/21-15:01:38.827127	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49825	1187	192.168.2.3	37.0.10.22
10/25/21-15:01:44.740049	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58058	8.8.8.8	192.168.2.3
10/25/21-15:01:44.771272	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49827	1187	192.168.2.3	37.0.10.22
10/25/21-15:01:50.676956	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49828	1187	192.168.2.3	37.0.10.22
10/25/21-15:01:56.589707	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51539	8.8.8.8	192.168.2.3
10/25/21-15:01:56.626994	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49829	1187	192.168.2.3	37.0.10.22
10/25/21-15:02:02.535309	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55393	8.8.8.8	192.168.2.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/25/21-15:02:02.564431	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49830	1187	192.168.2.3	37.0.10.22
10/25/21-15:02:08.926314	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49831	1187	192.168.2.3	37.0.10.22
10/25/21-15:02:14.881863	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63456	8.8.8.8	192.168.2.3
10/25/21-15:02:14.920037	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49832	1187	192.168.2.3	37.0.10.22

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 25, 2021 15:00:18.588891983 CEST	192.168.2.3	8.8.8.8	0x2572	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:00:25.265844107 CEST	192.168.2.3	8.8.8.8	0xddc5	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:00:33.179090977 CEST	192.168.2.3	8.8.8.8	0xb3c1	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:00:39.739573956 CEST	192.168.2.3	8.8.8.8	0x1748	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:00:46.357811928 CEST	192.168.2.3	8.8.8.8	0x1f29	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:00:52.953521967 CEST	192.168.2.3	8.8.8.8	0x197b	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:00:59.429028988 CEST	192.168.2.3	8.8.8.8	0x7254	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:01:06.766701937 CEST	192.168.2.3	8.8.8.8	0x3bed	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:01:13.559650898 CEST	192.168.2.3	8.8.8.8	0x2034	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:01:20.732178926 CEST	192.168.2.3	8.8.8.8	0xd849	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:01:26.752331018 CEST	192.168.2.3	8.8.8.8	0x2bea	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:01:32.805299044 CEST	192.168.2.3	8.8.8.8	0x2b1b	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:01:38.778913975 CEST	192.168.2.3	8.8.8.8	0x691	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:01:44.719530106 CEST	192.168.2.3	8.8.8.8	0x722f	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:01:50.603530884 CEST	192.168.2.3	8.8.8.8	0xbc8	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:01:56.568674088 CEST	192.168.2.3	8.8.8.8	0xae4f	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:02:02.515014887 CEST	192.168.2.3	8.8.8.8	0xe622	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:02:08.877588034 CEST	192.168.2.3	8.8.8.8	0xbe5	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)
Oct 25, 2021 15:02:14.861913919 CEST	192.168.2.3	8.8.8.8	0x3887	Standard query (0)	kamuchehdd hgfgf.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

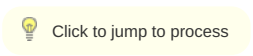
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 25, 2021 15:00:18.610142946 CEST	8.8.8.8	192.168.2.3	0x2572	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 15:00:25.286725044 CEST	8.8.8.8	192.168.2.3	0xddc5	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 25, 2021 15:00:33.199758053 CEST	8.8.8.8	192.168.2.3	0xb3c1	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 15:00:39.756234884 CEST	8.8.8.8	192.168.2.3	0x1748	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 15:00:46.376326084 CEST	8.8.8.8	192.168.2.3	0x1f29	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 15:00:52.973690987 CEST	8.8.8.8	192.168.2.3	0x197b	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 15:00:59.446767092 CEST	8.8.8.8	192.168.2.3	0x7254	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 15:01:06.785360098 CEST	8.8.8.8	192.168.2.3	0x3bed	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 15:01:13.577939034 CEST	8.8.8.8	192.168.2.3	0x2034	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 15:01:20.750567913 CEST	8.8.8.8	192.168.2.3	0xd849	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 15:01:26.772399902 CEST	8.8.8.8	192.168.2.3	0x2bea	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 15:01:32.823734999 CEST	8.8.8.8	192.168.2.3	0x2b1b	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 15:01:38.797635078 CEST	8.8.8.8	192.168.2.3	0x691	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 15:01:44.740048885 CEST	8.8.8.8	192.168.2.3	0x722f	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 15:01:50.622005939 CEST	8.8.8.8	192.168.2.3	0xbc8	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 15:01:56.589706898 CEST	8.8.8.8	192.168.2.3	0xae4f	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 15:02:02.535309076 CEST	8.8.8.8	192.168.2.3	0xe622	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 15:02:08.895885944 CEST	8.8.8.8	192.168.2.3	0xbe5	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)
Oct 25, 2021 15:02:14.881863117 CEST	8.8.8.8	192.168.2.3	0x3887	No error (0)	kamuchehdd hgfgf.ddns.net		37.0.10.22	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: CV.exe PID: 7020 Parent PID: 1464

General

Start time:	15:00:07
Start date:	25/10/2021
Path:	C:\Users\user\Desktop\CV.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\CV.exe'
Imagebase:	0xf50000
File size:	707072 bytes
MD5 hash:	5D9FED85F31D020568F166E6291CBE7B
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: 00000000.00000002.304747743.0000000003682000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.304713233.0000000003661000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.305068384.0000000004661000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.305068384.0000000004661000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.305068384.0000000004661000.00000004.00000001.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: 7124 Parent PID: 7020

General

Start time:	15:00:14
Start date:	25/10/2021
Path:	C:\Users\user\Desktop\CV.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\CV.exe
Imagebase:	0xd00000
File size:	707072 bytes
MD5 hash:	5D9FED85F31D020568F166E6291CBE7B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.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: 5512 Parent PID: 3352

General

Start time:	15:00:26
Start date:	25/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x740000
File size:	707072 bytes
MD5 hash:	5D9FED85F31D020568F166E6291CBE7B
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: 00000004.00000002.337548650.0000000003E71000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.337548650.0000000003E71000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.337548650.0000000003E71000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.336966221.0000000002E71000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.337007727.0000000002E92000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 56%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: dhcpmon.exe PID: 5300 Parent PID: 5512

General

Start time:	15:00:28
Start date:	25/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x770000
File size:	707072 bytes
MD5 hash:	5D9FED85F31D020568F166E6291CBE7B
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: 00000005.00000002.349313749.0000000002E11000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.349313749.0000000002E11000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.349379459.0000000003E11000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.349379459.0000000003E11000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.348554360.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.348554360.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.348554360.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis