ID: 527765
Sample Name: INV.exe
Cookbook: default.jbs
Time: 11:39:21
Date: 24/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

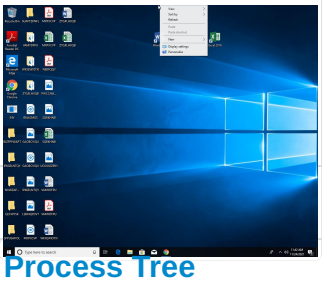
Windows Analysis Report INV.exe

Overview

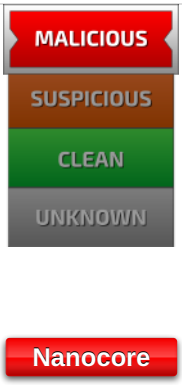
General Information

Sample Name:	INV.exe
Analysis ID:	527765
MD5:	9d64fa92ce93c24..
SHA1:	463c942e70fee74.
SHA256:	e6a01ce5b7532b..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



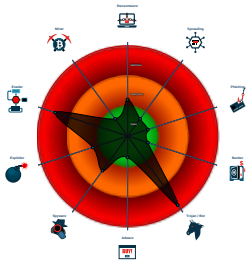
Nanocore

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for doma…
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- INV.exe (PID: 7072 cmdline: "C:\Users\user\Desktop\INV.exe" MD5: 9D64FA92CE93C242C09947E6A0A892A6)
  - INV.exe (PID: 6488 cmdline: C:\Users\user\Desktop\INV.exe MD5: 9D64FA92CE93C242C09947E6A0A892A6)
- dhcpmon.exe (PID: 5236 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 9D64FA92CE93C242C09947E6A0A892A6)
  - dhcpmon.exe (PID: 6988 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 9D64FA92CE93C242C09947E6A0A892A6)
- **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
0000000B.00000002.452804151.0000000002FE1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000B.00000002.452804151.0000000002FE1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x6943b:$a: NanoCore • 0x69494:$a: NanoCore • 0x694d1:$a: NanoCore • 0x6954a:$a: NanoCore • 0x6949d:$b: ClientPlugin • 0x694da:$b: ClientPlugin • 0x69dd8:$b: ClientPlugin • 0x69de5:$b: ClientPlugin • 0x5f093:$e: KeepAlive • 0x69925:$g: LogClientMessage • 0x698a5:$i: get_Connected • 0x59871:$j: #=q • 0x598a1:$j: #=q • 0x598dd:$j: #=q • 0x59905:$j: #=q • 0x59935:$j: #=q • 0x59965:$j: #=q • 0x59995:$j: #=q • 0x599c5:$j: #=q • 0x599e1:$j: #=q • 0x59a11:$j: #=q
0000000B.00000000.432448182.0000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000B.00000000.432448182.0000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
0000000B.00000000.432448182.000000000040 2000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	0xfcf5:$a: NanoCore 0xfd05:$a: NanoCore 0xff39:$a: NanoCore 0xff4d:$a: NanoCore 0xff8d:$a: NanoCore 0xfd54:$b: ClientPlugin 0xff56:$b: ClientPlugin 0xff96:$b: ClientPlugin 0xfe7b:$c: ProjectData 0x10882:$d: DESCrypto 0x1824e:$e: KeepAlive 0x1623c:$g: LogClientMessage 0x12437:$i: get_Connected 0x10bb8:$j: #=q 0x10be8:$j: #=q 0x10c04:$j: #=q 0x10c34:$j: #=q 0x10c50:$j: #=q 0x10c6c:$j: #=q 0x10c9c:$j: #=q 0x10cb8:$j: #=q
Click to see the 48 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.dhcpmon.exe.3b7fc20.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	0xe38d:$x1: NanoCore.ClientPluginHost 0xe3ca:$x2: IClientNetworkHost 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
8.2.dhcpmon.exe.3b7fc20.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	0xe105:$x1: NanoCore Client.exe 0xe38d:$x2: NanoCore.ClientPluginHost 0xf9c6:$s1: PluginCommand 0xf9ba:$s2: FileCommand 0x1086b:$s3: PipeExists 0x16622:$s4: PipeCreated 0xe3b7:$s5: IClientLoggingHost
8.2.dhcpmon.exe.3b7fc20.2.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
8.2.dhcpmon.exe.3b7fc20.2.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:$j: #=q
4.0.INV.exe.400000.8.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	0x1018d:$x1: NanoCore.ClientPluginHost 0x101ca:$x2: IClientNetworkHost 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 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

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for domain / URL

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Networking:

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)

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

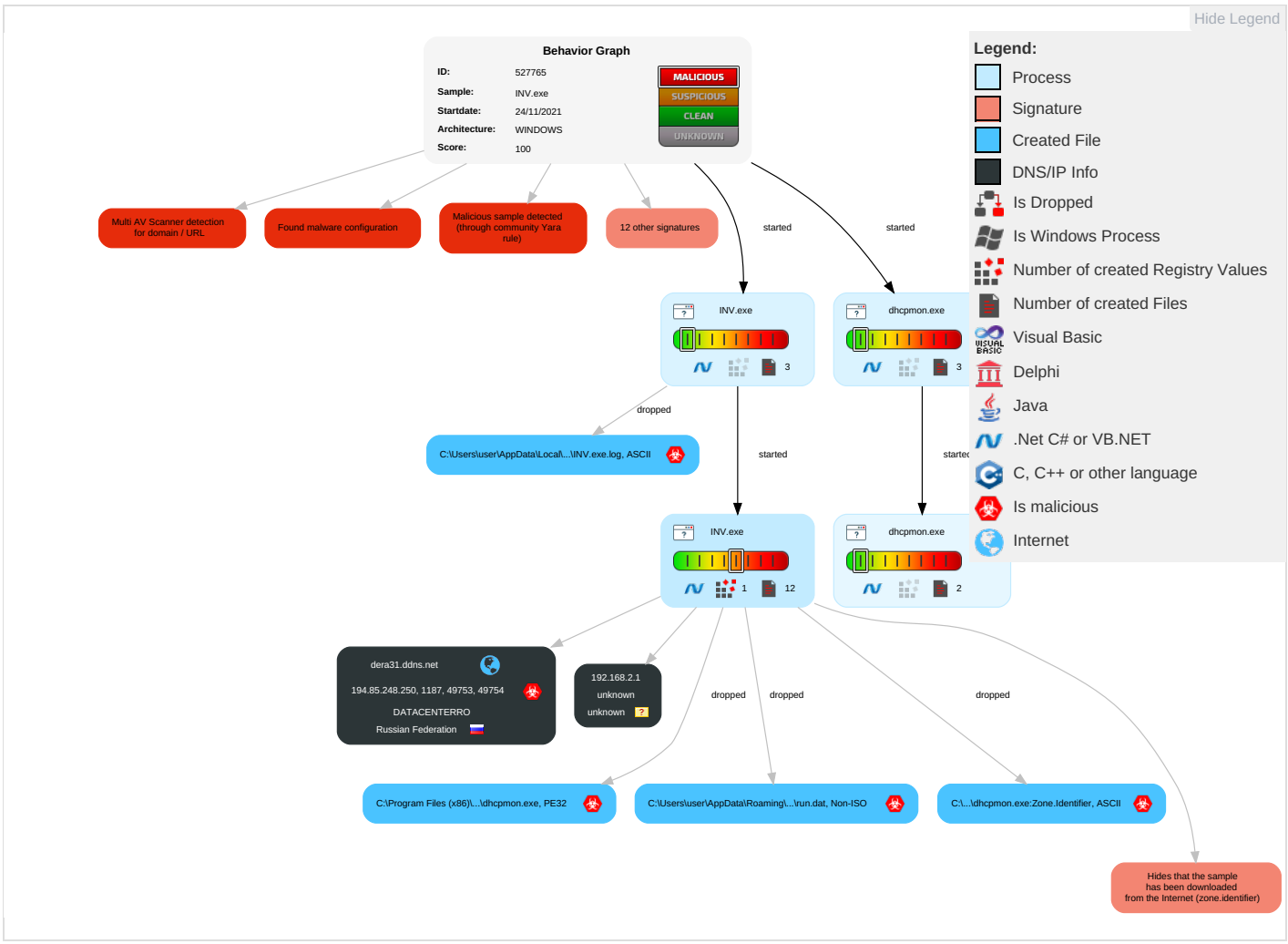
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Ne Eff
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 1 1	Masquerading 2	Input Capture 2 1	Query Registry 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Ea Ins Ne Co
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2 1 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Ex Re Ca
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Ex Tra Lo
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	Virtualization/Sandbox Evasion 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SI Sw
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Ma De Co
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jar De Se
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Ro Ac
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	Do Ins Pr

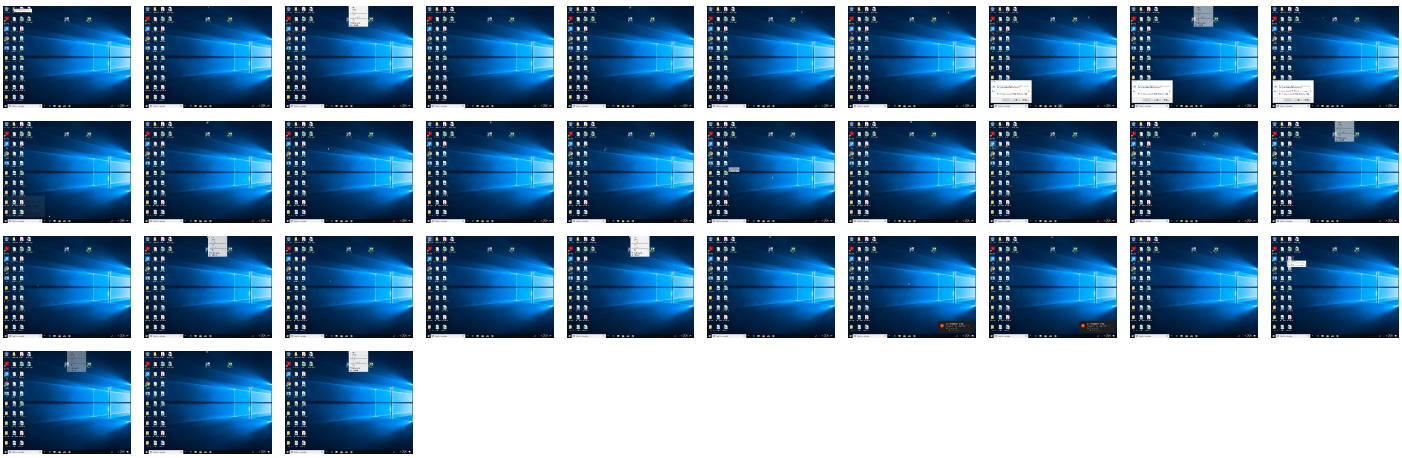
Behavior Graph



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
INV.exe	20%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	
INV.exe	100%	Avira	HEUR/AGEN.1141888	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Avira	HEUR/AGEN.1141888	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	20%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.0.dhcpmon.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.INV.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.INV.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.INV.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.dhcpmon.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.INV.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.INV.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
11.0.dhcpmon.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.dhcpmon.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.dhcpmon.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.2.dhcpmon.exe.400000.0.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.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
dera31.ddns.net	6%	Virustotal		Browse
dera31.ddns.net	0%	Avira URL Cloud	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.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.chinhdo.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
195.133.18.211	5%	Virustotal		Browse
195.133.18.211	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	• 6%, Virustotal, Browse • Avira URL Cloud: safe	unknown
195.133.18.211	true	• 5%, Virustotal, Browse • 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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	527765
Start date:	24.11.2021
Start time:	11:39:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	INV.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:	23
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@18/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.9% (good quality ratio 0.4%) • Quality average: 24.5% • Quality standard deviation: 32.6%
HCA Information:	• Successful, ratio: 92% • 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
11:40:33	API Interceptor	886x Sleep call for process: INV.exe modified
11:40:45	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
11:40:59	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	CV.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
dera31.ddns.net	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	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
	oGszHCs1c7	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\INV.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	553472
Entropy (8bit):	7.892995395638637
Encrypted:	false
SSDEEP:	12288:tOL/Mq/d/xj06PDRQtc0DEt1G2AjKVUhCX+U3/4sQ+5C5xw:tOLUm/mWDk+RA+qgXF/4sQ+U5

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
MD5:	9D64FA92CE93C242C09947E6A0A892A6
SHA1:	463C942E70FEE74AEF894C0DA58277C884D8C6BD
SHA-256:	E6A01CE5B7532B69A312FEE870B244D1DF1A6CAC00551981C850CE38EDC79AF5
SHA-512:	92AAA8E0BABD8B19264D9F4BAB511FEF60B64BC4E54E6D6F65010D4545F9D8670933A22121C0BA2EE54D61C66F63769BA971FD4C1F38CE6497CA8BB6DCCAE 1A
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: ReversingLabs, Detection: 20%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...f..a.....0..h.....>.... .....@.. ....@.....W..... ....H.....text...Df... ...h..... ..`.rsrc.....j.....@..@.reloc..... .....p.....@..B..... .....H.....X>...G.....o.....Ho.....?.....B..... 0.....*....0..... .... .".+a%....^E....F.....u.....\.....8.....i/. P*.$%+. .U.6%&+.....X. ..T#+..o..... uC..Z .0..a+..... ....Z .+!Da8o...s..... '..Z ..>-a8V..... ..>GZ #.wa8A...r...p(..... ..Z 3Z."a8#.....*...0.....r...p.

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\INV.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_v4.0_32\UsageLogs\INV.exe.log	
Process:	C:\Users\user\Desktop\INV.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0. 0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System. ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyT oken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.C onfiguration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\ 8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C: \Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0. 0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System. ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyT oken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.C onfiguration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\ 8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C: \Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\INV.exe
File Type:	data
Category:	dropped
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
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\INV.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:bnt:p
MD5:	B67F236CCBDD808687AB1ED303277371
SHA1:	A7F2A003B809BE7AEC847182F7A8E32E1A69927D
SHA-256:	54D51090990EA722925865E229CEC4ACA47400D75F98803D004B2E2F52E86247
SHA-512:	4F53EBEC74CF58ED08C623FE2ABD36000297C162EDDCD27D284A31E57E1AB3A0ECEE1DDA76B936C069CF869D40B6E84C4BFF03B122665DF912CA097CF091A BD2
Malicious:	**true**
Reputation:	low
Preview:	B.:L...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\INV.exe
File Type:	data
Category:	modified
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671E CB
Malicious:	false
Reputation:	moderate, very likely benign file
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\INV.exe
File Type:	data
Category:	dropped
Size (bytes):	315080
Entropy (8bit):	**7.999403263872478**
Encrypted:	**true**
SSDEEP:	6144:m8aeVE5MlgWfxwY/8uvJYRDMVpXUhXQrEBPgzC2D4Toqhs22DJM+iaPnW:mfwiMdxwYEYyWzw0TqC2kM+lnW
MD5:	981C80683A41E2D9DD9C297DAA691C54
SHA1:	7A1F5DDFFB3E630FE19E19F6AA923427DE72217B
SHA-256:	6C67B680BB9CF41F30C37D791D9EE52582977C1D9D5696FEAE1613FC0C5E2DBE
SHA-512:	72E4198AE2A65B7E1698925DF537CBA63A2877677C7C8FEA475E52B99E631272CFBEDCD5A4E1949EB7F8073C01229E89CCCD1ABBFD8832533346A6568750ADAE
Malicious:	false
Preview:	..f# ....)1*.....5....;.T..u.. .3.Xd... ....u(..._.V.{L..Y.8....~...S79.f0V...=.}...SJg|.lh.J..^Ge.....3h?n..:..r....,o."a.I....\..0Z.D.....^....[..f.I....@/_..".5+...I...J`./s..p-.....c..?...*.. .&.. ...>.Ye$=.pG.....9D...'7.w.a.[3.d.-..V..]..B.b.zA?..M..3...%A....K5@.. j.U.h.B....'...0."..u.V...d..c,r"..@9.9.>..cDgP~d9..St...{..24.s.'.....9.D..P4.....I...G..G5.....u.-2...z1[.....C..n.6.!..'.%@&.l4..P..rc+vq..C5B.b*..j.W,..T..z.....)BX4...>A.*~#..A....8..B....5....w....GC.....y.....7...?.T.....!.....7A.....C.3.....A.....hC..5'..42..zS.*2.m7....A.'/.R..X....}e...>.....}...n.A...4..?.P.l..n.0.l`...".d1.(e\|..f.....i.9.#...n..+..l....Xz.q...6".Hl...+...1^pgs...%.FR.T....(...=.rHX.d.9%...?..f?.Q.yi.D9/>....V..5.....q...nP'...S.Y.....pu.!..-..\..\|/....V.......NX...../.8..V.0.5`m$.{b..lw.K.3-..C3...-.2.Qb.....o...6z....`H...(..o.ag.-7../F..RoI..O#.u|.U.@....$;.....s.~.M...j?...q#.l..y..M.[../.....=T.....5HX.QJ...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.892995395638637
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	INV.exe
File size:	553472
MD5:	9d64fa92ce93c242c09947e6a0a892a6
SHA1:	463c942e70fee74aef894c0da58277c884d8c6bd
SHA256:	e6a01ce5b7532b69a312fee870b244d1df1a6cac0055198 1c850ce38edc79af5
SHA512:	92aaa8e0babd8b19264d9f4bab511fef60b64bc4e54e6d6 f65010d4545f9d8670933a22121c0ba2ee54d61c66f6376 9ba971fd4c1f38ce6497ca8bb6dccae61a
SSDEEP:	12288:tOL/Mq/d/xj06PDRQtc0DEt1G2AjKVUhCX+U3/4 sQ+5C5xw:tOLUm/mWDk+RA+qgXF/4sQ+U5
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...f. .a.....0..h.....>.... .....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x48863e
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:	0x619DE066 [Wed Nov 24 06:49:10 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x86644	0x86800	False	0.923913438081	data	7.90207517274	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8a000	0x600	0x600	False	0.455078125	data	4.26873788537	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8c000	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
11/24/21-11:40:43.693178	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	62044	8.8.8.8	192.168.2.6
11/24/21-11:40:55.238234	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49448	8.8.8.8	192.168.2.6
11/24/21-11:41:00.517317	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60342	8.8.8.8	192.168.2.6
11/24/21-11:41:11.773479	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58384	8.8.8.8	192.168.2.6
11/24/21-11:41:24.716787	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53781	8.8.8.8	192.168.2.6
11/24/21-11:41:36.939954	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50010	8.8.8.8	192.168.2.6
11/24/21-11:41:55.338434	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	62208	8.8.8.8	192.168.2.6
11/24/21-11:42:07.300908	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56628	8.8.8.8	192.168.2.6
11/24/21-11:42:14.530221	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60778	8.8.8.8	192.168.2.6
11/24/21-11:42:26.568735	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54683	8.8.8.8	192.168.2.6

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 24, 2021 11:40:43.669563055 CET	192.168.2.6	8.8.8.8	0xb92c	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 11:40:50.424350977 CET	192.168.2.6	8.8.8.8	0x60b7	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 11:40:55.217364073 CET	192.168.2.6	8.8.8.8	0x2f78	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 11:41:00.488914013 CET	192.168.2.6	8.8.8.8	0x673e	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 11:41:06.762356997 CET	192.168.2.6	8.8.8.8	0xe54e	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 11:41:11.752306938 CET	192.168.2.6	8.8.8.8	0x1451	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 11:41:17.746325970 CET	192.168.2.6	8.8.8.8	0x66aa	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 11:41:24.693977118 CET	192.168.2.6	8.8.8.8	0xe18e	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 11:41:30.877182961 CET	192.168.2.6	8.8.8.8	0x376c	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 11:41:36.918418884 CET	192.168.2.6	8.8.8.8	0x23c8	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 11:41:43.336577892 CET	192.168.2.6	8.8.8.8	0x1f37	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 11:41:49.437659025 CET	192.168.2.6	8.8.8.8	0x5e3f	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 11:41:55.319106102 CET	192.168.2.6	8.8.8.8	0xbb7d	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 11:42:02.210747957 CET	192.168.2.6	8.8.8.8	0x604e	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 11:42:07.276382923 CET	192.168.2.6	8.8.8.8	0xa6cf	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 11:42:14.507567883 CET	192.168.2.6	8.8.8.8	0x812b	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 11:42:20.570477009 CET	192.168.2.6	8.8.8.8	0xa47a	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 11:42:26.549261093 CET	192.168.2.6	8.8.8.8	0x909b	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 11:40:43.693177938 CET	8.8.8.8	192.168.2.6	0xb92c	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 11:40:50.444122076 CET	8.8.8.8	192.168.2.6	0x60b7	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 11:40:55.238234043 CET	8.8.8.8	192.168.2.6	0x2f78	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 11:41:00.517317057 CET	8.8.8.8	192.168.2.6	0x673e	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 11:41:06.782207966 CET	8.8.8.8	192.168.2.6	0xe54e	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 11:41:11.773478985 CET	8.8.8.8	192.168.2.6	0x1451	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 11:41:17.766179085 CET	8.8.8.8	192.168.2.6	0x66aa	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 11:41:24.716787100 CET	8.8.8.8	192.168.2.6	0xe18e	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 11:41:30.895451069 CET	8.8.8.8	192.168.2.6	0x376c	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 11:41:36.939954042 CET	8.8.8.8	192.168.2.6	0x23c8	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 24, 2021 11:41:43.356537104 CET	8.8.8.8	192.168.2.6	0x1f37	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 11:41:49.455307961 CET	8.8.8.8	192.168.2.6	0x5e3f	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 11:41:55.338433981 CET	8.8.8.8	192.168.2.6	0xbb7d	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 11:42:02.228897095 CET	8.8.8.8	192.168.2.6	0x604e	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 11:42:07.300908089 CET	8.8.8.8	192.168.2.6	0xa6cf	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 11:42:14.530220985 CET	8.8.8.8	192.168.2.6	0x812b	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 11:42:20.592962027 CET	8.8.8.8	192.168.2.6	0xa47a	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 24, 2021 11:42:26.568734884 CET	8.8.8.8	192.168.2.6	0x909b	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: INV.exe PID: 7072 Parent PID: 5084

General

Start time:	11:40:22
Start date:	24/11/2021
Path:	C:\Users\user\Desktop\INV.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\INV.exe"
Imagebase:	0xfd0000
File size:	553472 bytes
MD5 hash:	9D64FA92CE93C242C09947E6A0A892A6
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: 00000000.00000002.384059989.0000000003361000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.386415183.0000000004369000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.386415183.0000000004369000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.386415183.0000000004369000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: INV.exe PID: 6488 Parent PID: 7072

General

Start time:	11:40:34
Start date:	24/11/2021
Path:	C:\Users\user\Desktop\INV.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\INV.exe
Imagebase:	0x9c0000
File size:	553472 bytes
MD5 hash:	9D64FA92CE93C242C09947E6A0A892A6
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: 00000004.00000000.375140758.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.375140758.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.375140758.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.374658891.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.374658891.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.374658891.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.374169564.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.374169564.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.374169564.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.375865936.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.375865936.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.375865936.0000000000402000.00000040.00000001.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: 5236 Parent PID: 3440

General

Start time:	11:40:53
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:	0x470000
File size:	553472 bytes
MD5 hash:	9D64FA92CE93C242C09947E6A0A892A6
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: 00000008.00000002.440793413.0000000003A89000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.440793413.0000000003A89000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.440793413.0000000003A89000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000008.00000002.438460036.0000000002A81000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 20%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: dhcpmon.exe PID: 6988 Parent PID: 5236

General

Start time:	11:41:01
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:	0xbe0000
File size:	553472 bytes
MD5 hash:	9D64FA92CE93C242C09947E6A0A892A6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.452804151.0000000002FE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.452804151.0000000002FE1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000000.432448182.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.432448182.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.432448182.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000000.435107271.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.435107271.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.435107271.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.452888597.0000000003FE9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.452888597.0000000003FE9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.451682758.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.451682758.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.451682758.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000000.434333489.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.434333489.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.434333489.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000000.433501662.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.433501662.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.433501662.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis