ID: 561227
Sample Name: payment invoice.exe
Cookbook: default.jbs
Time: 09:13:51
Date: 27/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report payment invoice.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: NanoCore 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 6
AV Detection 6
E-Banking Fraud 6
System Summary 6
Stealing of Sensitive Information 6
Remote Access Functionality 6
Jbx Signature Overview 6
AV Detection 6
Networking 6
E-Banking Fraud 6
System Summary 6
Data Obfuscation 6
Hooking and other Techniques for Hiding and Protection 7
Malware Analysis System Evasion 7
HIPS / PFW / Operating System Protection Evasion 7
Stealing of Sensitive Information 7
Remote Access Functionality 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 11
World Map of Contacted IPs 12
Public IPs 12
Private 12
General Information 12
Warnings 13
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 13
IPs 13
Domains 14
ASNs 14
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 14
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe 14
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier 14
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log 15
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\payment invoice.exe.log 15
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat 15
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat 16
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin 16
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat 16
Static File Info 16
General 16
File Icon 17
Static PE Info 17
General 17
Entrypoint Preview 17
Data Directories 19
Sections 19

Resources 19
Imports 20
Version Infos 20
Network Behavior 20
Snort IDS Alerts 20
Network Port Distribution 21
TCP Packets 21
UDP Packets 23
DNS Queries 23
DNS Answers 24
Statistics 24
Behavior 24
System Behavior 25
Analysis Process: payment invoice.exePID: 6360, Parent PID: 5208 25
General 25
File Activities 25
File Created 25
File Written 25
File Read 26
Analysis Process: payment invoice.exePID: 3488, Parent PID: 6360 26
General 26
File Activities 27
File Created 27
File Deleted 28
File Written 28
File Read 30
Registry Activities 30
Key Value Created 30
Analysis Process: dhcpmon.exePID: 2100, Parent PID: 3472 30
General 31
File Activities 31
File Created 31
File Written 31
File Read 32
Analysis Process: dhcpmon.exePID: 6696, Parent PID: 2100 32
General 32
File Activities 33
File Created 33
File Read 33
Disassembly 34

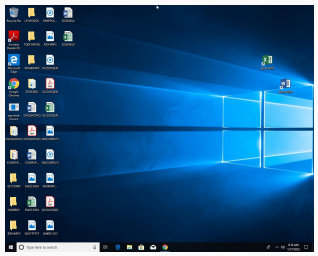
Windows Analysis Report

payment invoice.exe

Overview

General Information

Sample Name:	payment invoice.exe
Analysis ID:	561227
MD5:	1b42fbc89bc9f06..
SHA1:	7d7c025252a3fe..
SHA256:	fe3d1fe7f30a23c..
Tags:	exe NanoCore RAT
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

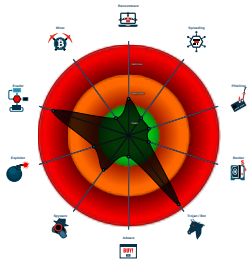
Nanocore

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Initial sample is a PE file and has a…

Classification



Process Tree

- **System is w10x64**
- payment invoice.exe (PID: 6360 cmdline: "C:\Users\user\Desktop\payment invoice.exe" MD5: 1B42FBC89BC9F06AD35424C85928D2F2)
  - payment invoice.exe (PID: 3488 cmdline: C:\Users\user\Desktop\payment invoice.exe MD5: 1B42FBC89BC9F06AD35424C85928D2F2)
- dhcpmon.exe (PID: 2100 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 1B42FBC89BC9F06AD35424C85928D2F2)
  - dhcpmon.exe (PID: 6696 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 1B42FBC89BC9F06AD35424C85928D2F2)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "c48b433d-6e7a-4320-ac18-2f1271be",
  "Group": "Default",
  "Domain1": "derarawfile10.ddns.net",
  "Domain2": "212.192.246250",
  "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.00000002.520173385.00000000052E0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
0000000B.00000002.520173385.00000000052E0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
0000000B.00000002.520173385.00000000052E0000.00000004.08000000.00040000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000F.00000000.349844025.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000F.00000000.349844025.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 71 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.payment invoice.exe.52e0000.20.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
11.2.payment invoice.exe.52e0000.20.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
11.2.payment invoice.exe.52e0000.20.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
15.2.dhcpmon.exe.2da9658.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
15.2.dhcpmon.exe.2da9658.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost

Click to see the 174 entries

Sigma Overview

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

System Summary

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

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)

Initial sample is a PE file and has a suspicious name

Executable has a suspicious name (potential lure to open the executable)

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

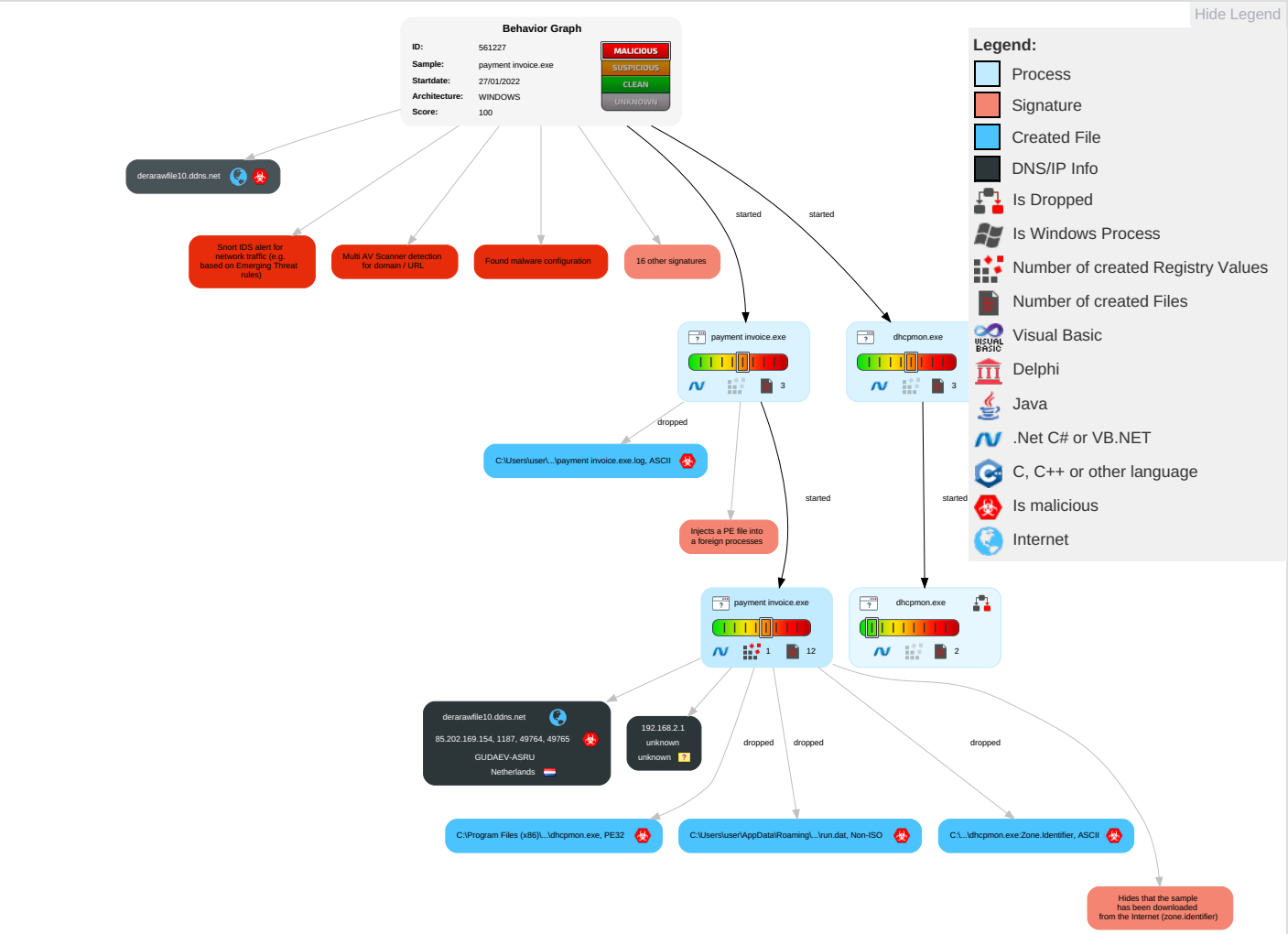
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	Path Interception	1 1 2 Process Injection	2 Masquerading	2 1 Input Capture	1 Query Registry	Remote Services	2 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 1 1 Security Software Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 2 Process Injection	NTDS	2 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	2 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	1 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 3 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact

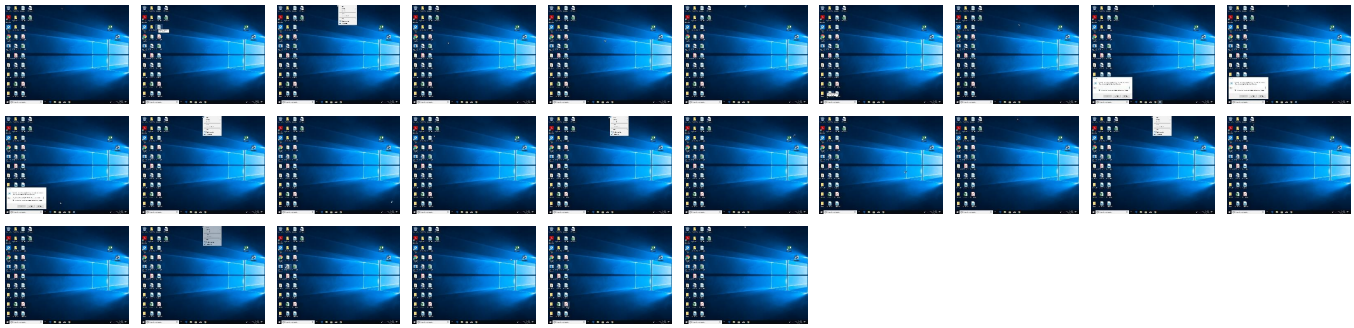
Behavior Graph



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
payment invoice.exe	15%	Metadefender		Browse
payment invoice.exe	40%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	
payment invoice.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	15%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	40%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.payment invoice.exe.52e0000.20.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Source	Detection	Scanner	Label	Link	Download
15.0.dhcpmon.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
11.2.payment invoice.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
11.0.payment invoice.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
15.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
15.0.dhcpmon.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
15.0.dhcpmon.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
15.0.dhcpmon.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
11.0.payment invoice.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
11.0.payment invoice.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
11.0.payment invoice.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
11.0.payment invoice.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
15.0.dhcpmon.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
derarawfile10.ddns.net	10%	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	
derarawfile10.ddns.net	10%	Virustotal		Browse
derarawfile10.ddns.net	100%	Avira URL Cloud	malware	
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	
212.192.246250	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	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.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
derarawfile10.ddns.net	85.202.169.154	true	true	• 10%, Virustotal, Browse	unknown

Contacted URLs

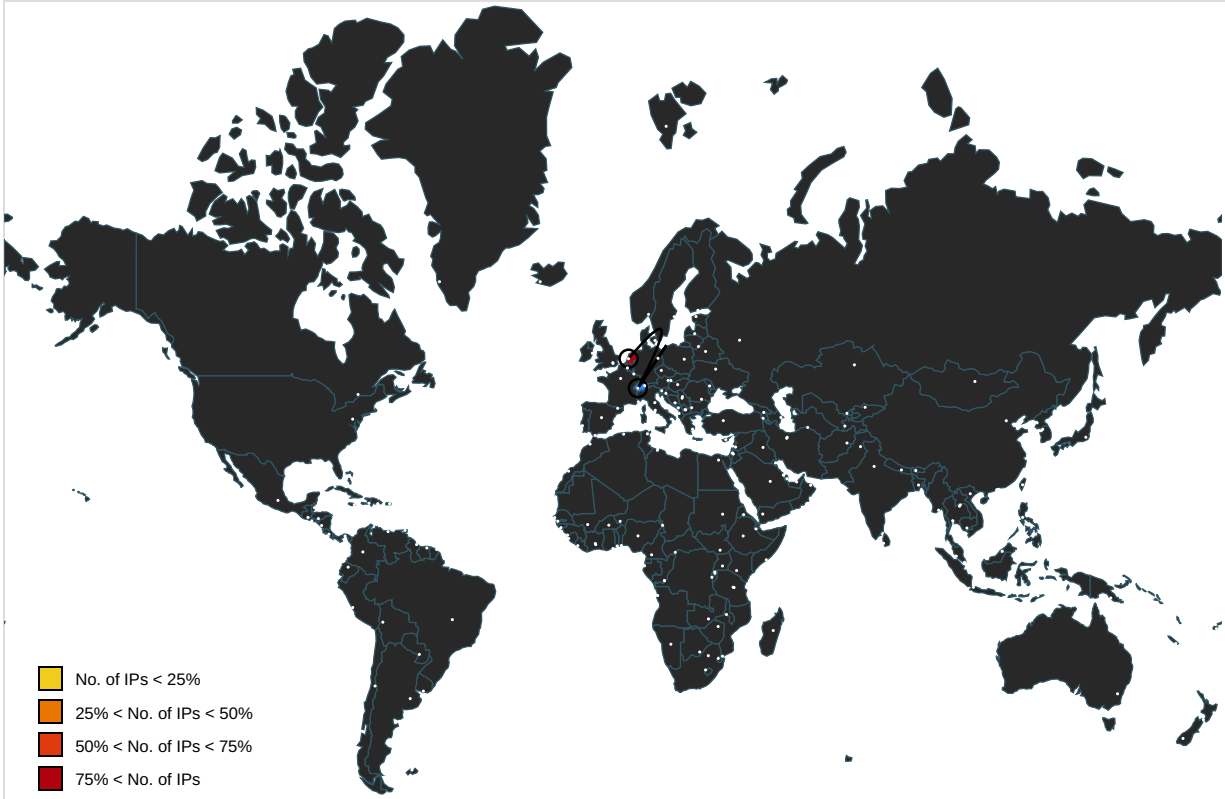
Name	Malicious	Antivirus Detection	Reputation
derarawfile10.ddns.net	true	• 10%, Virustotal, Browse • Avira URL Cloud: malware	unknown
212.192.246250	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	payment invoice.exe, 00000000.00000002.3 05994199.0000000006F52000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	payment invoice.exe, 00000000.00000002.3 05994199.0000000006F52000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	payment invoice.exe, 00000000.00000002.3 05994199.0000000006F52000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	payment invoice.exe, 00000000.00000002.3 05994199.0000000006F52000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	payment invoice.exe, 00000000.00000002.3 05994199.0000000006F52000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	payment invoice.exe, 00000000.00000002.3 05994199.0000000006F52000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.tiro.com	payment invoice.exe, 00000000.00000002.3 05994199.0000000006F52000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	payment invoice.exe, 00000000.00000002.3 05994199.0000000006F52000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	payment invoice.exe, 00000000.00000002.3 05994199.0000000006F52000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://google.com	payment invoice.exe, 0000000B.00000002.5 19394929.00000000043EB000.00000004.00000 800.00020000.00000000.sdmp, payment invoice.exe, 0000000B.00000002.519100489.00000000041E8 000.00000004.00000800.00020000.00000000.sdmp, payment invoice.exe, 0000000B.00000003.50147 8520.000000000452C000.00000004.00000800. 00020000.00000000.sdmp, payment invoice.exe, 0000000B.00000002.515719807.000000000296D000. 00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.coml	payment invoice.exe, 00000000.00000002.3 05994199.0000000006F52000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	payment invoice.exe, 00000000.00000002.3 05994199.0000000006F52000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	payment invoice.exe, 00000000.00000002.3 05994199.0000000006F52000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	payment invoice.exe, 00000000.00000002.3 05994199.0000000006F52000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	payment invoice.exe, 00000000.00000002.3 05994199.0000000006F52000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	payment invoice.exe, 00000000.00000002.3 05994199.0000000006F52000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	payment invoice.exe, 00000000.00000002.3 05994199.0000000006F52000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	payment invoice.exe, 00000000.00000002.3 05994199.0000000006F52000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	payment invoice.exe, 00000000.00000002.3 05994199.0000000006F52000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	payment invoice.exe, 00000000.00000002.3 05994199.0000000006F52000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/DPlease	payment invoice.exe, 00000000.00000002.3 05994199.0000000006F52000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	payment invoice.exe, 00000000.00000002.3 05994199.0000000006F52000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.fonts.com	payment invoice.exe, 00000000.00000002.3 05994199.0000000006F52000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	payment invoice.exe, 00000000.00000002.3 05994199.0000000006F52000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	payment invoice.exe, 00000000.00000002.3 05994199.0000000006F52000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	payment invoice.exe, 00000000.00000002.3 05994199.0000000006F52000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	payment invoice.exe, 00000000.00000002.3 05994199.0000000006F52000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
85.202.169.154	derarawfile10.ddns.net	Netherlands		209401	GUDAEV-ASRU	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	561227
Start date:	27.01.2022

Start time:	09:13:51
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	payment invoice.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:	21
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@14/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.2%) • Quality average: 75.3% • Quality standard deviation: 22.1%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- TCP Packets have been reduced to 100
- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): e12564.dspb.akamaiedge.net, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:15:11	API Interceptor	768x Sleep call for process: payment invoice.exe modified
09:15:22	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
09:15:34	API Interceptor	1x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\payment invoice.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	440832
Entropy (8bit):	7.8332758540402105
Encrypted:	false
SSDEEP:	12288:4Ba+qJhJbzR1+KOSjTzd3Bed/jtpBCQl:4U+MJJiyTz9Bed/Z
MD5:	1B42FBC89BC9F06AD35424C85928D2F2
SHA1:	7D7C025252A3FEDAE8959243268CB83741783D95
SHA-256:	FE3D1FE7F30A23C2F55A66E7BF38AA9094E512FB48B158B8023D3AE8DD99676D
SHA-512:	081EB918284FA0302585FFDEDAB13E2EE3CE42FD719FA4309CA7BF48273219F81CED197C6E98283F4E5A8E0D2D230BB745AC859482C6DCB577AF01527C890B32
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 15%, Browse • Antivirus: ReversingLabs, Detection: 40%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..... .....@.. ....@.....O..... ....H.....text...4.... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....xD..D.....Z.....(.....}.....{.....{....s....}.....(....*..0.....{.....+..*&...}....*...0.....+,...+...{..... (. .....X...{.....-....X...{.....-..{.....{.....[.Y.{.....[.Y.X(....{.....{.....[.Y.{.....[.O(....{.....{.....[.{.....[.Y.O(....{.....{.....[.{.....[.X(....*..0.....s....}.....(.....(.....{.....o.....(.....{.....o.....(.....{.....o.....(.....{.....o.....(

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

Process:	C:\Users\user\Desktop\payment invoice.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

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
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
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, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, 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\payment invoice.exe.log	
Process:	C:\Users\user\Desktop\payment invoice.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:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
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, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, 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\payment invoice.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C35(A5
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.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat

Process:	C:\Users\user\Desktop\payment invoice.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:wn:wn
MD5:	B8DCA36F2395AB86D4F647E118C92F1D
SHA1:	3D70475DDA94864D601F35B5E7A0E0CEDAA53E73
SHA-256:	F6D3CDD139D805A8231AB2C13183895EC6FF4C9310E30A1B2F64C40CB3163734
SHA-512:	11AC6E6DE38C5E3AE7C56CDB645BE45F78CB6B8B4BF7573C0B846C7117D0F4D290F9D7249F490D0EA7DFF89B3C5E67705224A35ABB2D616628CA35AD28E7C72
Malicious:	**true**
Reputation:	low
Preview:	.-X....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin

Process:	C:\Users\user\Desktop\payment invoice.exe
File Type:	data
Category:	modified
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671ECB
Malicious:	false
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\payment invoice.exe
File Type:	data
Category:	dropped
Size (bytes):	312480
Entropy (8bit):	**7.99946695108875**
Encrypted:	**true**
SSDEEP:	6144:2WYGDIDE+GJclEi5KjQpbL17IzzKJxw2mEhmTvpyD0i:+kIQ+EcFKjObdIA3mEhuvpyDd
MD5:	34CC720BAB9A243A96B008251C4541CA
SHA1:	B275C34B63ECA934EE8DD536B18D753203FC171A
SHA-256:	A63EAF4AE6032C446FDBABB4753851121BB6C03A1CF11749962BF501FF70DEB2
SHA-512:	FC4310B2A4478D04F82A3A1B8C4370442222B8F95EE2AD005FA9F0A638A85EE7E53F00B69027F0338A5A5AC9E42E4C6A5E33716115855567367E2E71D13346E4
Malicious:	false
Preview:	.<.#..!.nt.....I..N#....sb.....Q..O.v.qS.....AK.0.....7].S..K.|`k.....~a..,8..y.C+.3.Z.....;LZ.....y.QR..V..-.{".G.....g..]...R<]C`....Fak..{.....?.ViXd.....@k(Z.D...\..c...j.l5){HT....3.....Z...L.}).sH....m.H..._.)...w.@F.X,l.....h.....K.S..... ..*zi...{.:..y-.....Q.....E..~9.....n`ts..Tt.@..x*5..$.zv..1..n)...M..)....`.... ....`.....`.....8=y...Ry...r0J.9.....]$..,<.F;..B>..(....,\..{.....{...A..u.....Q.a..$..<..bP. xo.h...[.Y.ng...:.2..r.>....._..h.O:#c.Z.$..\.j.....Sb..8.....X...y.(.....W(...v....1"@N!A.8...d.RV..FmyYj.2....g.R..gaA."d..A..*..B2!.5./...u...c.cw..".p&5.A...%.....B.?3C.....z.tKv....=|.c.....h..\2_....H.{[K..$...4.... .I..Q.=...e..2Y..]..:.>.....c]....q.+G..'.J.....~...$1..R..{..D...5.y$..^...!(..C.0.<(..N...\....FGEi....X.oX.@W....(..-..@.....D.{._p...\.6..zv...n$f:.....e...p..:&*..8$ ./k....>Sd.....L,P.*<.c....ZK8C.B../'.....O.....Vz._0$.....OZ

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.8332758540402105

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	payment invoice.exe
File size:	440832
MD5:	1b42fbc89bc9f06ad35424c85928d2f2
SHA1:	7d7c025252a3fedae8959243268cb83741783d95
SHA256:	fe3d1fe7f30a23c2f55a66e7bf38aa9094e512fb48b158b8023d3ae8dd99676d
SHA512:	081eb918284fa0302585ffdedab13e2ee3ce42fd719fa4309ca7bf48273219f81ced197c6e98283f4e5a8e0d2d230bb745ac859482c6dcb577af01527c890b32
SSDEEP:	12288:4Ba+qJhJbzR1+KOSjTzd3Bed/jtpBCQl:4U+MJJiyTz9Bed/Z
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0..... .....@.. ....@ .....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x46cf2e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61F1E392 [Thu Jan 27 00:13:06 2022 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

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x6cedc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6e000	0x600	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x70000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x6cda4	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x6af34	0x6b000	False	0.905111437646	data	7.84083055635	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x6e000	0x600	0x600	False	0.430338541667	data	4.21802513151	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x70000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x6e090	0x36e	data		
RT_MANIFEST	0x6e410	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Overwolf 2021
Assembly Version	11.0.0.0
InternalName	ToStringHelperFu.exe
FileVersion	11.0.0.0
CompanyName	Overwolf LTD
LegalTrademarks	
Comments	
ProductName	Overwolf
ProductVersion	11.0.0.0
FileDescription	Overwolf
OriginalFilename	ToStringHelperFu.exe

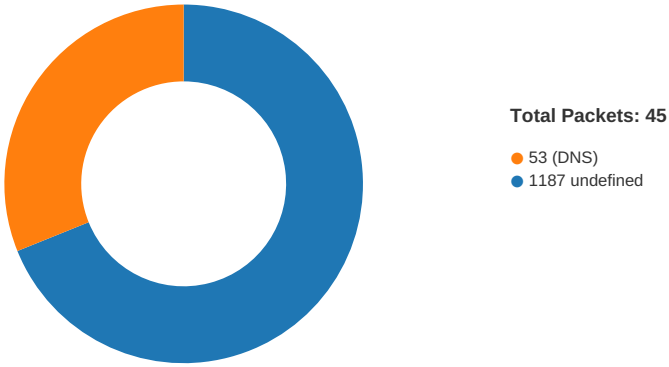
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/27/22-09:15:25.990304	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	65296	8.8.8.8	192.168.2.5
01/27/22-09:15:26.181080	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49764	1187	192.168.2.5	85.202.169.154
01/27/22-09:15:33.775371	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63183	8.8.8.8	192.168.2.5
01/27/22-09:15:33.843964	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49765	1187	192.168.2.5	85.202.169.154
01/27/22-09:15:42.593118	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49992	8.8.8.8	192.168.2.5
01/27/22-09:15:43.516050	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49772	1187	192.168.2.5	85.202.169.154
01/27/22-09:15:50.353088	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64345	8.8.8.8	192.168.2.5
01/27/22-09:15:50.382395	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49775	1187	192.168.2.5	85.202.169.154
01/27/22-09:15:57.272679	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54791	8.8.8.8	192.168.2.5
01/27/22-09:15:57.444999	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49782	1187	192.168.2.5	85.202.169.154
01/27/22-09:16:03.565006	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49784	1187	192.168.2.5	85.202.169.154
01/27/22-09:16:10.579898	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49785	1187	192.168.2.5	85.202.169.154
01/27/22-09:16:17.015587	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53813	8.8.8.8	192.168.2.5
01/27/22-09:16:17.044606	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49786	1187	192.168.2.5	85.202.169.154
01/27/22-09:16:24.558148	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49789	1187	192.168.2.5	85.202.169.154
01/27/22-09:16:30.817980	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49791	1187	192.168.2.5	85.202.169.154
01/27/22-09:16:37.432007	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49792	1187	192.168.2.5	85.202.169.154
01/27/22-09:16:44.534092	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59413	8.8.8.8	192.168.2.5
01/27/22-09:16:44.563709	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49793	1187	192.168.2.5	85.202.169.154
01/27/22-09:16:50.649072	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60516	8.8.8.8	192.168.2.5

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/27/22-09:16:50.677900	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49794	1187	192.168.2.5	85.202.169.154
01/27/22-09:16:56.908846	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49796	1187	192.168.2.5	85.202.169.154

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2022 09:15:25.998606920 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.026384115 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.026474953 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.181080103 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.225729942 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.270864964 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.388807058 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.416073084 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.416157007 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.496392012 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.696069956 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.772397995 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.819103003 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.819135904 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.819154978 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.819170952 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.819215059 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.819258928 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.847313881 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.847361088 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.847384930 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.847414970 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.847444057 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.847476006 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.847502947 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.847532988 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.847536087 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.847588062 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.879525900 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.879561901 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.879585981 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.879611015 CET	1187	49764	85.202.169.154	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2022 09:15:26.879631996 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.879656076 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.879679918 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.879703045 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.879709959 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.879725933 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.879728079 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.879745007 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.879749060 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.879774094 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.879797935 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.879803896 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.879821062 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.879844904 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.879846096 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.879868984 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.879918098 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.906546116 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.906582117 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.906608105 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.906632900 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.906657934 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.906683922 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.906709909 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.906730890 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.906733036 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.906755924 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.906780958 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.906790018 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.906805992 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.906817913 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.906831980 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.906857967 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.906858921 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.906887054 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.906913042 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.906938076 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.906939983 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.906965971 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.906970024 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.906992912 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.907015085 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.907016993 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.907043934 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.907071114 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.907094955 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.907097101 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.907124043 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.907124996 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.907157898 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.907185078 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.907195091 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.907211065 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.907233000 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.907236099 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.907262087 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.907289028 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.934036970 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.934067011 CET	1187	49764	85.202.169.154	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2022 09:15:26.934107065 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.934130907 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.934154034 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.934173107 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.934180975 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.934190035 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.934210062 CET	1187	49764	85.202.169.154	192.168.2.5
Jan 27, 2022 09:15:26.934210062 CET	49764	1187	192.168.2.5	85.202.169.154
Jan 27, 2022 09:15:26.934227943 CET	1187	49764	85.202.169.154	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2022 09:15:25.969337940 CET	65296	53	192.168.2.5	8.8.8.8
Jan 27, 2022 09:15:25.990303993 CET	53	65296	8.8.8.8	192.168.2.5
Jan 27, 2022 09:15:33.755445004 CET	63183	53	192.168.2.5	8.8.8.8
Jan 27, 2022 09:15:33.775371075 CET	53	63183	8.8.8.8	192.168.2.5
Jan 27, 2022 09:15:42.573765039 CET	49992	53	192.168.2.5	8.8.8.8
Jan 27, 2022 09:15:42.593117952 CET	53	49992	8.8.8.8	192.168.2.5
Jan 27, 2022 09:15:50.331999063 CET	64345	53	192.168.2.5	8.8.8.8
Jan 27, 2022 09:15:50.353087902 CET	53	64345	8.8.8.8	192.168.2.5
Jan 27, 2022 09:15:57.253832102 CET	54791	53	192.168.2.5	8.8.8.8
Jan 27, 2022 09:15:57.272679090 CET	53	54791	8.8.8.8	192.168.2.5
Jan 27, 2022 09:16:03.515331984 CET	50394	53	192.168.2.5	8.8.8.8
Jan 27, 2022 09:16:03.536154032 CET	53	50394	8.8.8.8	192.168.2.5
Jan 27, 2022 09:16:10.532634974 CET	58530	53	192.168.2.5	8.8.8.8
Jan 27, 2022 09:16:10.550066948 CET	53	58530	8.8.8.8	192.168.2.5
Jan 27, 2022 09:16:16.996191978 CET	53813	53	192.168.2.5	8.8.8.8
Jan 27, 2022 09:16:17.015587091 CET	53	53813	8.8.8.8	192.168.2.5
Jan 27, 2022 09:16:24.503495932 CET	57344	53	192.168.2.5	8.8.8.8
Jan 27, 2022 09:16:24.521217108 CET	53	57344	8.8.8.8	192.168.2.5
Jan 27, 2022 09:16:30.769622087 CET	59261	53	192.168.2.5	8.8.8.8
Jan 27, 2022 09:16:30.788856030 CET	53	59261	8.8.8.8	192.168.2.5
Jan 27, 2022 09:16:37.382241964 CET	57151	53	192.168.2.5	8.8.8.8
Jan 27, 2022 09:16:37.401635885 CET	53	57151	8.8.8.8	192.168.2.5
Jan 27, 2022 09:16:44.515067101 CET	59413	53	192.168.2.5	8.8.8.8
Jan 27, 2022 09:16:44.534091949 CET	53	59413	8.8.8.8	192.168.2.5
Jan 27, 2022 09:16:50.627748013 CET	60516	53	192.168.2.5	8.8.8.8
Jan 27, 2022 09:16:50.649071932 CET	53	60516	8.8.8.8	192.168.2.5
Jan 27, 2022 09:16:56.859551907 CET	65086	53	192.168.2.5	8.8.8.8
Jan 27, 2022 09:16:56.879015923 CET	53	65086	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2022 09:15:25.969337940 CET	192.168.2.5	8.8.8.8	0x5909	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)
Jan 27, 2022 09:15:33.755445004 CET	192.168.2.5	8.8.8.8	0xad7	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)
Jan 27, 2022 09:15:42.573765039 CET	192.168.2.5	8.8.8.8	0x4219	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)
Jan 27, 2022 09:15:50.331999063 CET	192.168.2.5	8.8.8.8	0xf8b4	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)
Jan 27, 2022 09:15:57.253832102 CET	192.168.2.5	8.8.8.8	0xf001	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)
Jan 27, 2022 09:16:03.515331984 CET	192.168.2.5	8.8.8.8	0x5d74	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)
Jan 27, 2022 09:16:10.532634974 CET	192.168.2.5	8.8.8.8	0xdc47	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)
Jan 27, 2022 09:16:16.996191978 CET	192.168.2.5	8.8.8.8	0x59d7	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)
Jan 27, 2022 09:16:24.503495932 CET	192.168.2.5	8.8.8.8	0xc8a9	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)

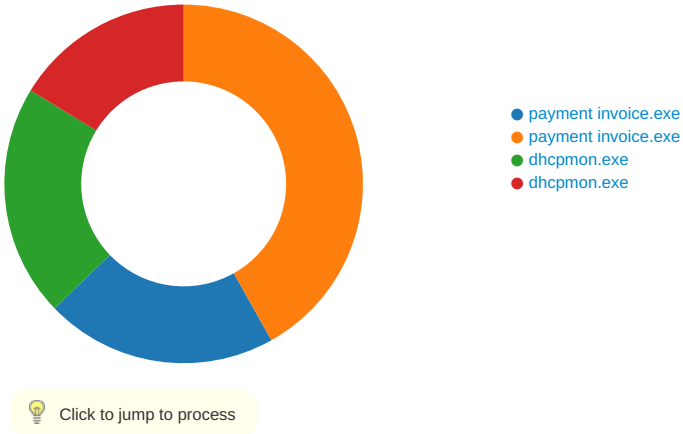
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2022 09:16:30.769622087 CET	192.168.2.5	8.8.8.8	0x8745	Standard query (0)	derarawfil e10.ddns.net	A (IP address)	IN (0x0001)
Jan 27, 2022 09:16:37.382241964 CET	192.168.2.5	8.8.8.8	0x4c8a	Standard query (0)	derarawfil e10.ddns.net	A (IP address)	IN (0x0001)
Jan 27, 2022 09:16:44.515067101 CET	192.168.2.5	8.8.8.8	0x502d	Standard query (0)	derarawfil e10.ddns.net	A (IP address)	IN (0x0001)
Jan 27, 2022 09:16:50.627748013 CET	192.168.2.5	8.8.8.8	0x3456	Standard query (0)	derarawfil e10.ddns.net	A (IP address)	IN (0x0001)
Jan 27, 2022 09:16:56.859551907 CET	192.168.2.5	8.8.8.8	0x5520	Standard query (0)	derarawfil e10.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2022 09:15:25.990303993 CET	8.8.8.8	192.168.2.5	0x5909	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)
Jan 27, 2022 09:15:33.775371075 CET	8.8.8.8	192.168.2.5	0xad7	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)
Jan 27, 2022 09:15:42.593117952 CET	8.8.8.8	192.168.2.5	0x4219	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)
Jan 27, 2022 09:15:50.353087902 CET	8.8.8.8	192.168.2.5	0xf8b4	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)
Jan 27, 2022 09:15:57.272679090 CET	8.8.8.8	192.168.2.5	0xf001	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)
Jan 27, 2022 09:16:03.536154032 CET	8.8.8.8	192.168.2.5	0x5d74	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)
Jan 27, 2022 09:16:10.550066948 CET	8.8.8.8	192.168.2.5	0xdc47	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)
Jan 27, 2022 09:16:17.015587091 CET	8.8.8.8	192.168.2.5	0x59d7	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)
Jan 27, 2022 09:16:24.521217108 CET	8.8.8.8	192.168.2.5	0xc8a9	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)
Jan 27, 2022 09:16:30.788856030 CET	8.8.8.8	192.168.2.5	0x8745	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)
Jan 27, 2022 09:16:37.401635885 CET	8.8.8.8	192.168.2.5	0x4c8a	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)
Jan 27, 2022 09:16:44.534091949 CET	8.8.8.8	192.168.2.5	0x502d	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)
Jan 27, 2022 09:16:50.649071932 CET	8.8.8.8	192.168.2.5	0x3456	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)
Jan 27, 2022 09:16:56.879015923 CET	8.8.8.8	192.168.2.5	0x5520	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: payment invoice.exe PID: **6360**, Parent PID: **5208**

General

Target ID:	0
Start time:	09:14:49
Start date:	27/01/2022
Path:	C:\Users\user\Desktop\payment invoice.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\payment invoice.exe"
Imagebase:	0xb40000
File size:	440832 bytes
MD5 hash:	1B42FBC89BC9F06AD35424C85928D2F2
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: 00000000.00000002.302169870.0000000002F11000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.302296870.0000000002FC5000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.302845784.0000000003F19000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.302845784.0000000003F19000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.302845784.0000000003F19000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E69CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E69CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\payment invoice.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E9AC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\payment invoice.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E9AC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E675705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E675705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E5D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E67CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E5D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E5D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E5D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E5D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E675705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E675705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C801B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C801B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C801B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C801B4F	ReadFile

Analysis Process: payment invoice.exe PID: **3488**, Parent PID: **6360**

General

Target ID:	11
Start time:	09:15:13
Start date:	27/01/2022
Path:	C:\Users\user\Desktop\payment invoice.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\payment invoice.exe
Imagebase:	0x4f0000
File size:	440832 bytes
MD5 hash:	1B42FBC89BC9F06AD35424C85928D2F2
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: 0000000B.00000002.520173385.00000000052E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.520173385.00000000052E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.520173385.00000000052E0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.521504626.0000000006AE0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.521504626.0000000006AE0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.519531866.000000000450B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.519531866.000000000450B000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.519880894.0000000004F30000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.519880894.0000000004F30000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.521530362.0000000006AF0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.521530362.0000000006AF0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000000.298590889.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.298590889.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.298590889.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.518735074.0000000003949000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.518735074.0000000003949000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.515620270.0000000002901000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000000.298920042.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.298920042.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.298920042.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000000.299236323.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.299236323.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.299236323.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.511296388.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.511296388.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.511296388.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000000.299557780.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.299557780.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.299557780.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.519394929.00000000043EB000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.519100489.00000000041E8000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.515719807.000000000296D000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 0000000B.00000003.501478520.000000000452C000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E69CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E69CF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C80BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C801E60	CreateFileW
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C80BEFF	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C80DD66	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C80DD66	CopyFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C80BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C80BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	10	6C801E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C801E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C801E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\payment invoice.exe:Zone.Identifier	success or wait	1	6C782935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	fd 2d 58 fd fd fd fd 48	-XH	success or wait	1	6C801B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	131072	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd fd fd 61 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 06 00 00 08 00 00 00 00 00 00 2e fd 06 00 00 20 00 00 00 fd 06 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 20 07 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELa0. @ @	success or wait	4	6C80DD66	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	6C80DD66	CopyFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	0	232	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd fd 26 15 fd fd 69 2b fd 49 63 28 31 fd 50 fd fd 50 fd 63 4c 54 fd fd 42 41 fd 62 fd fd 1b fd fd fd fd fd 34 68 fd 12 fd 74 fd 2b fd 07 5a 5c fd fd 20 fd 69 fd fd a4 fd fd 40 fd 33 fd fd 7b 0c fd 1c 67 72 76 2b 56 fd fd fd 42 19 0e fd 0d fd fd 15 5d fd 50 fd fd 16 57 fd 34 43 7d 75 4c 1e fd fd 0b fd 73 7e fd fd 46 04 fd fd 7d fd fd fd fd fd 00 45 fd fd fd fd fd fd 45 fd 14 fd 36 45 fd fd fd fd fd 7b 5f 05 18 7b fd 79 53 fd fd fd 37 fd fd 22 16 68 4b fd 21 03 78 fd 32 fd fd 69 e3 fd 7a 4a fd bb fd 20 fd fd fd fd 66 fd 67 3f fd 5f 0b fd fd fd 30 fd 3a 65 5b 37 77 7b 31 fd 21 fd 34 fd fd fd fd fd 26 fd	Gjh\3A5x&i+c(1PPcLTAb 4ht+Z\ i@ 3{grv+VB]PW4C}uLs~F} EE6E{{yS7"hK!x2izJ f? _0:e[7w{1!4&	success or wait	9	6C801B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	0	312480	fd 3c fd 23 83 fd 21 fd 6e 74 fd 17 fd fd 00 0e fd fd 17 49 db fd 4e 23 fd fd fd fd 73 62 fd 19 fd fd fd 51 1d fd 4f 13 76 fd 71 53 fd 09 06 fd 3a fd fd 41 4b fd 30 fd fd 09 fd fd 37 5d fd 53 1d 36 4b 0e 7c 60 6b fd 70 c0 e7 fd fd 7e 61 0c 0b 2c 38 13 1a 79 7f 43 2b 15 33 fd 5a c6 fd fd fd 13 fd 3b 4c 5a de fd fd fd fd 02 fd fd fd fd fd fd 01 79 fd 51 52 1c 02 56 fd fd 2d 0e 7b 22 fd 47 0a fd fd 18 fd 67 09 fd 5d fd ca fd 52 3c 5d 43 60 fd fd fd fd 46 61 6b fd bc 7b fd fd 1f 4c 58 3f 08 56 69 58 64 fd fd 01 fd fd 40 6b 28 5a fd 44 fd fd fd 5c d0 fd 63 fd fd 06 6a 7f 6c 35 29 7b 48 54 fd fd fd fd 33 fd fd fd fd 41 5a 01 fd fd 4c fd 7d 29 19 73 48 fd fd fd fd 6d fd 48 17 fd fd 5f fd 29 fd 17 fd	<#!ntIN#sbQOvqSAK07]SK\`k~a,8y C+3Z;LZyQRV-{"Gg]R<]C`Fak{?ViX d@k(ZD\cjl5) {HT3ZL})sHmH_)	success or wait	1	6C801B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	0	40	39 69 48 fd 1a c5 7d 5a cd 34 00 fd 66 0d 7e 61 fd fd fd 01 06 fd 0c fd 7e fd 7e fd fd fd fd 05 fd fd 33 fd 55 0b	9iH}Z4f~a~~3U	success or wait	1	6C801B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E675705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E675705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E5D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E67CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E5D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E5D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E5D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E5D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E675705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E675705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C801B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C801B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6E65D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6E65D72F	unknown
C:\Users\user\Desktop\payment invoice.exe	unknown	4096	success or wait	1	6E65D72F	unknown
C:\Users\user\Desktop\payment invoice.exe	unknown	512	success or wait	1	6E65D72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	6C80646A	RegSetValueExW

Analysis Process: dhcpmon.exe PID: **2100**, Parent PID: **3472**

General

Target ID:	14
Start time:	09:15:30
Start date:	27/01/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0x5c0000
File size:	440832 bytes
MD5 hash:	1B42FBC89BC9F06AD35424C85928D2F2
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: 0000000E.00000002.353630003.00000000029B1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000E.00000002.354462618.0000000002A65000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.361008995.00000000039B9000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.361008995.00000000039B9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.361008995.00000000039B9000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 15%, Metadefender, Browse • Detection: 40%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E69CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E69CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E9AC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E9AC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E675705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E675705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E5D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E67CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E5D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E5D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E5D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E5D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E675705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E675705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C801B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C801B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C801B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C801B4F	ReadFile

Analysis Process: dhcpmon.exe PID: **6696**, Parent PID: **2100**

General

Target ID:	15
Start time:	09:15:36
Start date:	27/01/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x8b0000
File size:	440832 bytes
MD5 hash:	1B42FBC89BC9F06AD35424C85928D2F2
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: 0000000F.00000000.349844025.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000000.349844025.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000000.349844025.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.380206809.0000000002D41000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.380206809.0000000002D41000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000000.349447069.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000000.349447069.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000000.349447069.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000000.350241950.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000000.350241950.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000000.350241950.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000000.350757246.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000000.350757246.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000000.350757246.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.380340638.0000000003D49000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.380340638.0000000003D49000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.379057501.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.379057501.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.379057501.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E69CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E69CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E675705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E675705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E5D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E67CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E5D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E5D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E5D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E5D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E675705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E675705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C801B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C801B4F	ReadFile

Disassembly

No disassembly