ID: 560096
Sample Name: Revised invoice.exe
Cookbook: default.jbs
Time: 06:22:42
Date: 26/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

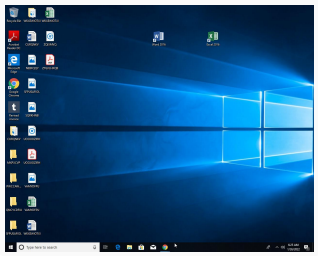
Windows Analysis Report

Revised invoice.exe

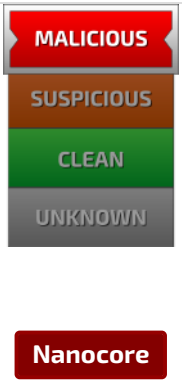
Overview

General Information

Sample Name:	Revised invoice.exe
Analysis ID:	560096
MD5:	4bab1b0e7bbb12.
SHA1:	2c6da100c498a0..
SHA256:	1a4032263b7f92..
Tags:	exe nanocore
Infos:	



Detection



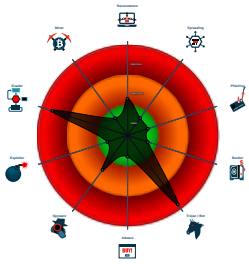
Nanocore

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 detection for URL or domain
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Initial sample is a PE file and has a…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- Revised invoice.exe (PID: 6272 cmdline: "C:\Users\user\Desktop\Revised invoice.exe" MD5: 4BAB1B0E7BBB12D6280A75EB3475B45B)
  - Revised invoice.exe (PID: 6692 cmdline: C:\Users\user\Desktop\Revised invoice.exe MD5: 4BAB1B0E7BBB12D6280A75EB3475B45B)
- dhcpmon.exe (PID: 2904 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 4BAB1B0E7BBB12D6280A75EB3475B45B)
  - dhcpmon.exe (PID: 5644 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 4BAB1B0E7BBB12D6280A75EB3475B45B)
- **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
0000000C.00000000.463093309.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000C.00000000.463093309.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000C.00000000.463093309.0000000000402000.00000040.00000400.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
0000000C.00000002.495569005.00000000040F9000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
0000000C.00000002.495569005.00000000040F9000.00000004.00000800.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	0x42f15:$a: NanoCore 0x42f6e:$a: NanoCore 0x42fab:$a: NanoCore 0x43024:$a: NanoCore 0x566cf:$a: NanoCore 0x566e4:$a: NanoCore 0x56719:$a: NanoCore 0x6f19b:$a: NanoCore 0x6f1b0:$a: NanoCore 0x6f1e5:$a: NanoCore 0x42f77:$b: ClientPlugin 0x42fb4:$b: ClientPlugin 0x438b2:$b: ClientPlugin 0x438bf:$b: ClientPlugin 0x5648b:$b: ClientPlugin 0x564a6:$b: ClientPlugin 0x564d6:$b: ClientPlugin 0x566ed:$b: ClientPlugin 0x56722:$b: ClientPlugin 0x6ef57:$b: ClientPlugin 0x6ef72:$b: ClientPlugin
Click to see the 55 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.dhcpmon.exe.413b136.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	0xe75:$x1: NanoCore.ClientPluginHost 0x145e3:$x1: NanoCore.ClientPluginHost 0x2d0af:$x1: NanoCore.ClientPluginHost 0xe8f:$x2: IClientNetworkHost 0x14610:$x2: IClientNetworkHost 0x2d0dc:$x2: IClientNetworkHost
12.2.dhcpmon.exe.413b136.4.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	0xe75:$x2: NanoCore.ClientPluginHost 0x145e3:$x2: NanoCore.ClientPluginHost 0x2d0af:$x2: NanoCore.ClientPluginHost 0x1261:$s3: PipeExists 0x1136:$s4: PipeCreated 0x156be:$s4: PipeCreated 0x2e18a:$s4: PipeCreated 0xeb0:$s5: IClientLoggingHost 0x145fd:$s5: IClientLoggingHost 0x2d0c9:$s5: IClientLoggingHost
12.2.dhcpmon.exe.413b136.4.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
12.2.dhcpmon.exe.413b136.4.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	0xddf:$a: NanoCore 0xe38:$a: NanoCore 0xe75:$a: NanoCore 0xeee:$a: NanoCore 0x14599:$a: NanoCore 0x145ae:$a: NanoCore 0x145e3:$a: NanoCore 0x2d065:$a: NanoCore 0x2d07a:$a: NanoCore 0x2d0af:$a: NanoCore 0xe41:$b: ClientPlugin 0xe7e:$b: ClientPlugin 0x177c:$b: ClientPlugin 0x1789:$b: ClientPlugin 0x14355:$b: ClientPlugin 0x14370:$b: ClientPlugin 0x143a0:$b: ClientPlugin 0x145b7:$b: ClientPlugin 0x145ec:$b: ClientPlugin 0x2ce21:$b: ClientPlugin 0x2ce3c:$b: ClientPlugin
4.2.Revised invoice.exe.29fca78.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	0xe75:$x1: NanoCore.ClientPluginHost 0xe8f:$x2: IClientNetworkHost
Click to see the 101 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 dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

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)

Initial sample is a PE file and has a suspicious name

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

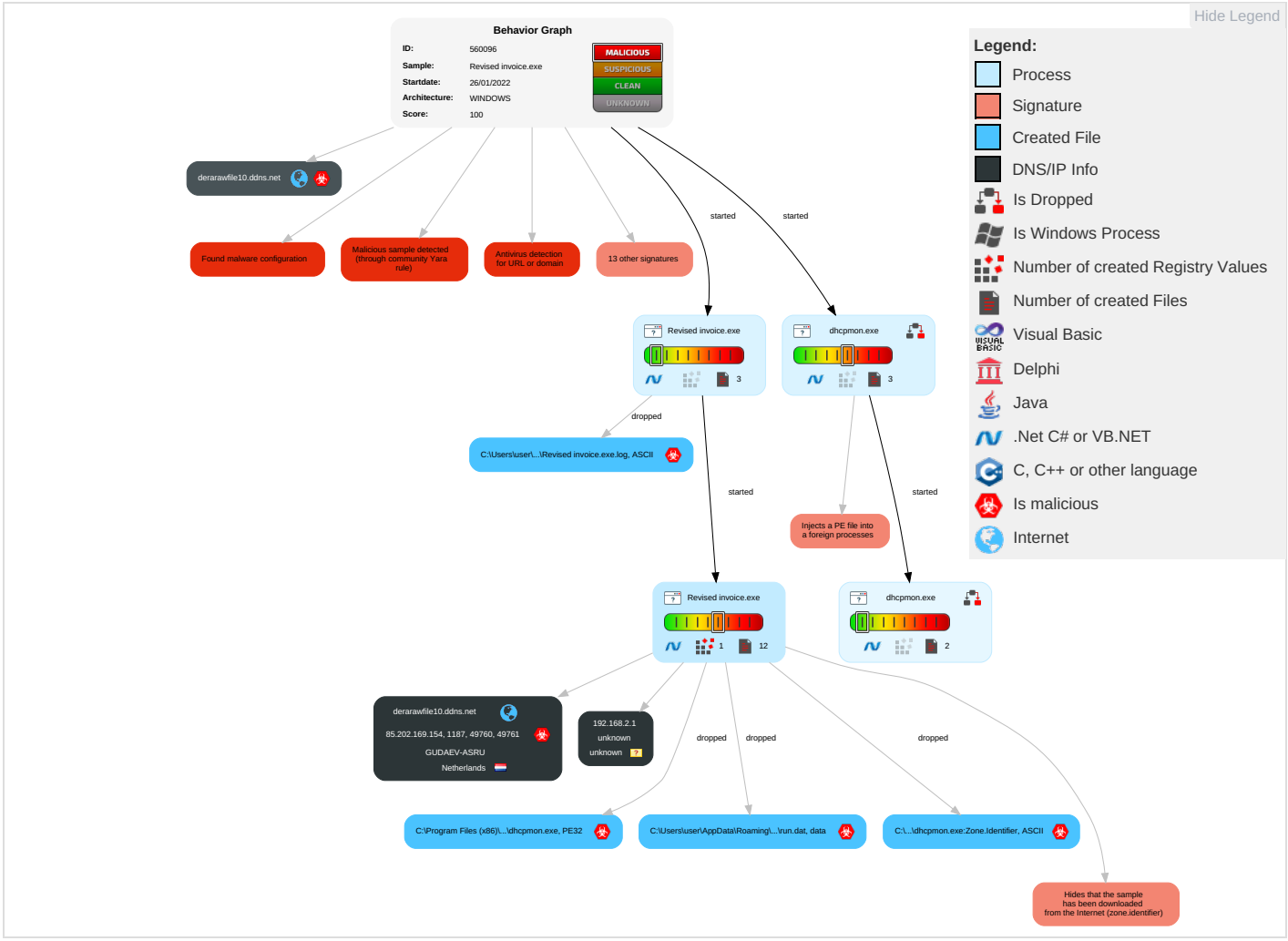
Detected Nanocore Rat

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	2 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

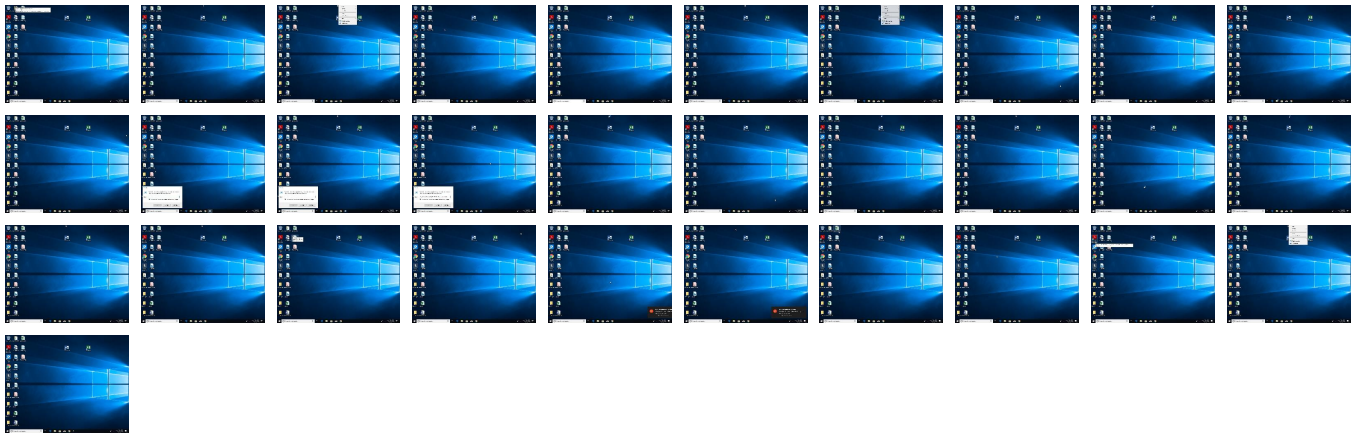
Behavior Graph



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
Revised invoice.exe	16%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	
Revised 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	23%	ReversingLabs	ByteCode-MSIL.Trojan.DarkStealerLoader	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.Revised invoice.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.Revised invoice.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
12.0.dhcpmon.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
4.0.Revised invoice.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
4.0.Revised invoice.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
12.0.dhcpmon.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
12.0.dhcpmon.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
4.0.Revised invoice.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
12.0.dhcpmon.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
12.0.dhcpmon.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File
4.2.Revised invoice.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSI L.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.carterandcone.comcr_	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com/	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnicrc	0%	Avira URL Cloud	safe	
http://www.carterandcone.comros	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.com#	0%	URL Reputation	safe	
http://www.carterandcone.comes	0%	URL Reputation	safe	
http://www.carterandcone.comx%	0%	Avira URL Cloud	safe	
http://www.monotype.f	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn-	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn;	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm2	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnr-c	0%	Avira URL Cloud	safe	
http://www.carterandcone.com-	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnno	0%	Avira URL Cloud	safe	
http://www.carterandcone.comes22	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sandoll.co.krs-c	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.carterandcone.comces00	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.urwpp.deoi	0%	URL Reputation	safe	
http://www.urwpp.de.	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kras	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sandoll.co.krn-uy1	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.comac	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.comF%	0%	Avira URL Cloud	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnh	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html#	0%	Avira URL Cloud	safe	
http://www.carterandcone.comic	0%	URL Reputation	safe	
http://www.sandoll.co.kr=	0%	Avira URL Cloud	safe	
http://www.urwpp.deoa&	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr8b1	0%	Avira URL Cloud	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.agfamonotype.	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn(ii)	0%	Avira URL Cloud	safe	
http://www.tiro.comlic	0%	URL Reputation	safe	
http://www.fontbureau.comica	0%	Avira URL Cloud	safe	
http://www.carterandcone.comi	0%	URL Reputation	safe	
derarawfile10.ddns.net	100%	Avira URL Cloud	malware	
http://www.carterandcone.comm	0%	URL Reputation	safe	
http://www.carterandcone.come-d	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.carterandcone.comint	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
212.192.246250	0%	Avira URL Cloud	safe	
http://www.carterandcone.comoaV2	0%	Avira URL Cloud	safe	
http://fontfabrik.comX2	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cnZ	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://fontfabrik.com#	0%	Avira URL Cloud	safe	
http://www.tiro.comg	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn//	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
derarawfile10.ddns.net	85.202.169.154	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
derarawfile10.ddns.net	true	• 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.carterandcone.comcr_	Revised invoice.exe, 00000000.00000003.367106783.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366650482.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366788242.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366932129.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	Revised invoice.exe, 00000000.00000002.4 10926933.0000000007502000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.com/	Revised invoice.exe, 00000000.00000003.3 53759018.0000000006212000.00000004.00000 800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cnicrc	Revised invoice.exe, 00000000.00000003.3 65408608.000000000622E000.00000004.00000 800.00020000.00000000.sdmp, Revised invoice.exe, 0 0000000.00000003.365576119.000000000622E 000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.36723 9507.000000000622B000.00000004.00000800. 00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.365760169.000000000622E000. 00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.365101107 .000000000622E000.00000004.00000800.0002 0000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366072624.00000000062 2E000.00000004.00000800.00020000.0000000 0.sdmp, Revised invoice.exe, 00000000.00000003.368 137719.000000000622B000.00000004.0000080 0.00020000.00000000.sdmp, Revised invoice.exe, 000 00000.00000003.367578995.000000000622B00 0.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.3647073 65.000000000622E000.00000004.00000800.00 020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.365908787.000000000 622E000.00000004.00000800.00020000.00000 000.sdmp, Revised invoice.exe, 00000000. 00000003.367106783.000000000622B000.0000 0004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.364867736.000 000000622E000.00000004.00000800.00020000 .00000000.sdmp, Revised invoice.exe, 00000000.0000 0003.366460308.000000000622B000.00000004 .00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.367422104.0000000 00622B000.00000004.00000800.00020000.000 00000.sdmp, Revised invoice.exe, 0000000 0.00000003.368054486.0000000006234000.00 000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.3 67728953.000000000622B000.00000004.00000 800.00020000.00000000.sdmp, Revised invoice.exe, 0 0000000.00000003.366332325.000000000622E 000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.36665 0482.000000000622B000.00000004.00000800. 00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366788242.000000000622B000. 00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.367876523 .000000000622B000.00000004.00000800.0002 0000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366932129.00000000062 2B000.00000004.00000800.00020000.0000000 0.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comros	Revised invoice.exe, 00000000.00000003.3 65408608.000000000622E000.00000004.00000 800.00020000.00000000.sdmp, Revised invoice.exe, 0 0000000.00000003.365576119.000000000622E 000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.36576 0169.000000000622E000.00000004.00000800. 00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366072624.000000000622E000. 00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.365908787 .000000000622E000.00000004.00000800.0002 0000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366460308.00000000062 2B000.00000004.00000800.00020000.0000000 0.sdmp, Revised invoice.exe, 00000000.00000003.366 332325.000000000622E000.00000004.0000080 0.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	Revised invoice.exe, 00000000.00000002.4 10926933.0000000007502000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Revised invoice.exe, 00000000.00000002.4 10926933.0000000007502000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.com#	Revised invoice.exe, 00000000.00000003.365408608.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.365101107.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.365255484.000000000622E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comes	Revised invoice.exe, 00000000.00000003.366650482.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366788242.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366932129.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Revised invoice.exe, 00000000.00000002.410926933.0000000007502000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comx%	Revised invoice.exe, 00000000.00000003.366460308.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersH0	Revised invoice.exe, 00000000.00000003.394089096.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.monotype.f	Revised invoice.exe, 00000000.00000003.372065578.0000000006231000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.372345940.0000000006231000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.372196965.0000000006231000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn-	Revised invoice.exe, 00000000.00000003.365408608.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.365101107.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.364707365.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.364867736.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.365255484.000000000622E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.tiro.com	Revised invoice.exe, 00000000.00000002.410926933.0000000007502000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn;	Revised invoice.exe, 00000000.00000003.363022467.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Revised invoice.exe, 00000000.00000003.394089096.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	Revised invoice.exe, 00000000.00000002.410926933.0000000007502000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://google.com	Revised invoice.exe, 00000004.00000002.619048568.0000000002A3D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.com	Revised invoice.exe, 00000000.00000003.365255484.000000000622E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm2	Revised invoice.exe, 00000000.00000003.387775919.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.389674141.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.387963973.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.388779559.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.389422039.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.388306201.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.388109557.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.389227415.000000000622C000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.388535003.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.389804972.000000000622C000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.387576262.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.389543097.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.388898410.000000000622C000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.389047637.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cnr-c	Revised invoice.exe, 00000000.00000003.364707365.000000000622E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.com-	Revised invoice.exe, 00000000.00000003.365576119.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.365760169.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366072624.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.365908787.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366460308.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366332325.000000000622E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cnno	Revised invoice.exe, 00000000.00000003.363022467.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comes22	Revised invoice.exe, 00000000.00000003.366932129.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	Revised invoice.exe, 00000000.00000002.410926933.0000000007502000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krs-c	Revised invoice.exe, 00000000.00000003.361679245.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	Revised invoice.exe, 00000000.00000002.410926933.0000000007502000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comces00	Revised invoice.exe, 00000000.00000003.365760169.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.365908787.000000000622E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/cThe	Revised invoice.exe, 00000000.00000002.410926933.0000000007502000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm	Revised invoice.exe, 00000000.00000003.387775919.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.387963973.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.388779559.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.388306201.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.388109557.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.388535003.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000002.410926933.0000000007502000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.387576262.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Revised invoice.exe, 00000000.00000003.356633716.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.356841100.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000002.410926933.0000000007502000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.356915572.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deoi	Revised invoice.exe, 00000000.00000003.374215463.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.373403063.000000000623100 0.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.374079868.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.373947160.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.373821747.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.373545548.000000000623100 0.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.373690092.0000000006230000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de.	Revised invoice.exe, 00000000.00000003.383925059.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.384255026.000000000623800 0.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.384447138.0000000006238000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.384106288.0000000006237000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.384524248.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kras	Revised invoice.exe, 00000000.00000003.361679245.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	Revised invoice.exe, 00000000.00000002.410926933.0000000007502000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ascendercorp.com/typedesigners.html	Revised invoice.exe, 00000000.00000003.369688026.0000000006233000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.370035509.0000000006233000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.369763768.0000000006233000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.369845471.0000000006233000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.370258143.0000000006233000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.krn-uy1	Revised invoice.exe, 00000000.00000003.361679245.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.361492036.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	Revised invoice.exe, 00000000.00000002.410926933.0000000007502000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Revised invoice.exe, 00000000.00000003.361679245.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000002.410926933.0000000007502000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.361492036.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comac	Revised invoice.exe, 00000000.00000003.365908787.000000000622E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	Revised invoice.exe, 00000000.00000002.410926933.0000000007502000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.de	Revised invoice.exe, 00000000.00000003.373403063.0000000006231000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.383925059.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.384255026.0000000006238000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.384447138.0000000006238000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.384106288.0000000006237000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.373545548.0000000006231000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.384668334.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.373690092.0000000006230000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.384524248.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Revised invoice.exe, 00000000.00000003.364707365.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.365908787.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.367106783.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.364867736.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366460308.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.367422104.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366332325.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000002.410926933.0000000007502000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366650482.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366788242.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366932129.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.365255484.000000000622E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comF%	Revised invoice.exe, 00000000.00000003.366072624.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366460308.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366332325.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366650482.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366788242.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366932129.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.como.	Revised invoice.exe, 00000000.00000003.367239507.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.368137719.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.367578995.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.367106783.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366460308.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.367422104.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.368054486.0000000006234000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.367728953.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366332325.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366650482.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366788242.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.367876523.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366932129.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersp	Revised invoice.exe, 00000000.00000003.374079868.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.come	Revised invoice.exe, 00000000.00000003.353759018.0000000006212000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	Revised invoice.exe, 00000000.00000002.410926933.0000000007502000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersn	Revised invoice.exe, 00000000.00000003.383733657.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cnh	Revised invoice.exe, 00000000.00000003.362696477.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.362926280.0000000006234000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ascendercorp.com/typedesigners.html#	Revised invoice.exe, 00000000.00000003.370879570.0000000006233000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.369688026.0000000006233000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.370035509.0000000006233000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.370392686.0000000006233000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.370542926.0000000006233000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.369763768.0000000006233000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.370742797.0000000006233000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.369845471.0000000006233000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.370258143.0000000006233000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comic	Revised invoice.exe, 00000000.00000003.365408608.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.365101107.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.364867736.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.365255484.000000000622E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sandoll.co.kr=	Revised invoice.exe, 00000000.00000003.361492036.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.urwpp.deoa&	Revised invoice.exe, 00000000.00000003.373403063.0000000006231000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.374079868.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.373947160.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.373821747.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.373545548.0000000006231000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.373690092.0000000006230000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	Revised invoice.exe, 00000000.00000002.410926933.0000000007502000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Revised invoice.exe, 00000000.00000002.406349724.0000000001A67000.00000004.00000020.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000002.410926933.0000000007502000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr8b1	Revised invoice.exe, 00000000.00000003.361679245.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.come	Revised invoice.exe, 00000000.00000003.365760169.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366072624.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.365908787.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.367106783.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366460308.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366332325.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366650482.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366788242.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366932129.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.agfamonotype.	Revised invoice.exe, 00000000.00000003.394245963.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000002.410670704.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.394510528.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.394372093.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.394089096.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlt	Revised invoice.exe, 00000000.00000003.380409949.000000000624E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/frere-jones.htmlefa	Revised invoice.exe, 00000000.00000003.377291056.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.377794899.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.378110058.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.377030811.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.377497410.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.377619595.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.377352983.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.377931382.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.377160989.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.zhongyicts.com.cn(ii)	Revised invoice.exe, 00000000.00000003.364707365.000000000622E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.tiro.comlic	Revised invoice.exe, 00000000.00000003.367239507.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.367106783.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comica	Revised invoice.exe, 00000000.00000002.406349724.0000000001A67000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comi	Revised invoice.exe, 00000000.00000003.367239507.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.367106783.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.367422104.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366650482.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366788242.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366932129.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.comm	Revised invoice.exe, 00000000.00000003.365760169.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366072624.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.365908787.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366460308.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366332325.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366650482.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366788242.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366932129.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.come-d	Revised invoice.exe, 00000000.00000003.366650482.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366788242.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.366932129.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	Revised invoice.exe, 00000000.00000003.365760169.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.365908787.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000002.410926933.0000000007502000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	Revised invoice.exe, 00000000.00000003.363910398.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.363989041.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.363760748.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.363384800.0000000006230000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.363563968.0000000006230000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Revised invoice.exe, 00000000.00000002.410926933.0000000007502000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comint	Revised invoice.exe, 00000000.00000003.365408608.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.365576119.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.365760169.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.365908787.000000000622E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn	Revised invoice.exe, 00000000.00000003.364432152.0000000006234000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.362696477.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.363910398.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.363022467.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.363989041.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.364707365.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.363760748.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.364867736.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.363384800.0000000006230000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.363563968.0000000006230000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000002.410926933.0000000007502000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.364542463.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.364298191.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.362926280.0000000006234000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Revised invoice.exe, 00000000.00000003.377056015.000000000624E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.377333224.000000000624E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.377181974.000000000624E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.377517366.000000000624E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000002.410926933.0000000007502000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.comoaV2	Revised invoice.exe, 00000000.00000003.367239507.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.367578995.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.367106783.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.367422104.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://fontfabrik.comX2	Revised invoice.exe, 00000000.00000003.356841100.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.356915572.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	Revised invoice.exe, 00000000.00000003.380642548.000000000624E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.380409949.000000000624E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.zhongyicts.com.cnZ	Revised invoice.exe, 00000000.00000003.364707365.000000000622E000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	Revised invoice.exe, 00000000.00000002.410926933.0000000007502000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.como	Revised invoice.exe, 00000000.00000002.406349724.0000000001A67000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cno.	Revised invoice.exe, 00000000.00000003.365408608.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.365576119.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.365760169.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.365101107.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.364707365.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.364867736.000000000622E000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.365255484.000000000622E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Revised invoice.exe, 00000000.00000002.410926933.0000000007502000.00000004.00000800.00020000.00000000.sdmp	false		high
http://fontfabrik.com#	Revised invoice.exe, 00000000.00000003.357972442.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.357162871.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.356996176.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.358148540.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.357338520.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.357778044.000000000622B000.00000004.00000800.00020000.00000000.sdmp, Revised invoice.exe, 00000000.00000003.357505167.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comg	Revised invoice.exe, 00000000.00000003.364201705.0000000001A6C000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/	Revised invoice.exe, 00000000.00000003.373947160.000000000622B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn//	Revised invoice.exe, 00000000.00000003.363384800.0000000006230000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: 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:	560096
Start date:	26.01.2022
Start time:	06:22:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Revised 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:	22
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@15/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 1.1% (good quality ratio 0.9%) • Quality average: 44.3% • Quality standard deviation: 30.1%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings

- 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, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, www.bing.com, client.wns.windows.com, fs.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, dual-a-0001.a-msedge.net, www-bing-com.dual-a-0001.a-msedge.net, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior 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.
- VT rate limit hit for: Revised invoice.exe

Simulations

Behavior and APIs

Time	Type	Description
06:24:04	API Interceptor	745x Sleep call for process: Revised invoice.exe modified
06:24:18	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
06:24:30	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\Revised invoice.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	825344
Entropy (8bit):	7.520494128006195
Encrypted:	false
SSDEEP:	24576:2P/qWxHh73mHLVtSsb+MCMaw2JgKhxFMIpydM3:2V4b+M5r2Jd5p
MD5:	4BAB1B0E7BBB12D6280A75EB3475B45B
SHA1:	2C6DA100C498A0862CAFC338B7570AD3714C716E
SHA-256:	1A4032263B7F92E02D65CAC6F7E483C1897DAFB8B9C47937758FEC3DA22F154C
SHA-512:	A52646B46F8BA8985F099C018090789E0482186631CDF31014248CACC31709FB8E70ACB390BAF9F82895488D789EB92AFCAF1980BB38D76505DE215B5F2DDAEI
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 23%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...X..a.....0.....v.... .....@.. ..@.....$...O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....X.....H.....<..... .....0..G.....r...p.....,.r...ps....z...(....(.....r...p.o....(....s....z.*.....-.....0..o.....s.... ..s.....~.....(.....o.....,.(.....o .....*...rW..p..o....(....(!.....,..o".....*..(.....-.....4B.....Za.....0..o.....s#.....o$....s%.....+.....J...r...p(&...o'...&...X....i.....-..o(.....&.r...p(!.....,..o".....*.....GO.....

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

Process:	C:\Users\user\Desktop\Revised 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\Revised invoice.exe.log

Process:	C:\Users\user\Desktop\Revised 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\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\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat

Process:	C:\Users\user\Desktop\Revised 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:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C35A5
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\Revised invoice.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:ph6:n6
MD5:	6C095DEF8EC05A7649A760E4872D3C3D
SHA1:	7F8A51E779662D2390F45376D3F293698E33973E
SHA-256:	70834C697DF69CA1B413876FC00EC4D002E32F0EFB68209496F81960BBA64B9B
SHA-512:	82A35B1F211AD3288B49EDDFA9A32EEEC2D31914C46F370F7F9AAAC3F9DB7A76B7B0EE5335862A5B5B6E1CCD1E1928F65F517B2F048C116866E6802839E7AF6
Malicious:	**true**
Preview:	..Y....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\Revised 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
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

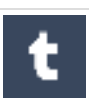
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\Revised invoice.exe
File Type:	data
Category:	dropped
Size (bytes):	312480
Entropy (8bit):	**7.99946695108875**
Encrypted:	**true**
SSDEEP:	6144:2WYGDIDE+GJclEi5KjQpbL17IzzKJxw2mEhmTvpyD0i:+kIQ+EcFKjObdIA3mEhuvpyDd
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):	7.520494128006195
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:	Revised invoice.exe
File size:	825344
MD5:	4bab1b0e7bbb12d6280a75eb3475b45b
SHA1:	2c6da100c498a0862cafc338b7570ad3714c716e
SHA256:	1a4032263b7f92e02d65cac6f7e483c1897dafb8b9c47937758fec3da22f154c
SHA512:	a52646b46f8ba8985f099c018090789e0482186631cdf31014248cacc31709fb8e70acb390baf9f82895488d789eb92afcaf1980bb38d76505de215b5f2ddaef
SSDEEP:	24576:2P/qWxHh73mHLVtSsb+MCMaw2JgKhxFMIpydM3:2V4b+M5r2Jd5p
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...X..a.....0.....v.... .....@.. .....@.....

File Icon



Icon Hash:	2c5231b95ab22408

Static PE Info

General

Entrypoint:	0x4ca076
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:	0x61F09658 [Wed Jan 26 00:31:20 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]
mov byte ptr [eax-2C754571h], ch
mov ecx, CFB1EDF5h
jmp far 82EBh : FBB5E4AAh
stc
nop
retf B5C9h
out DCh, eax
mov seg?, word ptr [edi-1F081154h]
retf EA8Eh
retf CE80h
lds ebp, fword ptr [ebp-7B2F3B49h]
xchg eax, ebx
aad F0h
jmp 00007F9F64DF062Ah
mov ah, 9Dh
int3
scasd
movsd
xchg eax, ebp
mov edx, 9DD28799h
jecxz 00007F9F64DF05F3h
mov edx, 0000CA90h
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xca024	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xcc000	0x11dc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xce000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
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	0xc80bc	0xc8200	False	0.701654971502	data	7.52802106198	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xcc000	0x11dc	0x1200	False	0.645616319444	data	6.54059849362	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xce000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xcc100	0xb3a	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xccc4c	0x14	data		
RT_VERSION	0xccc70	0x36c	data		
RT_MANIFEST	0xccfec	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

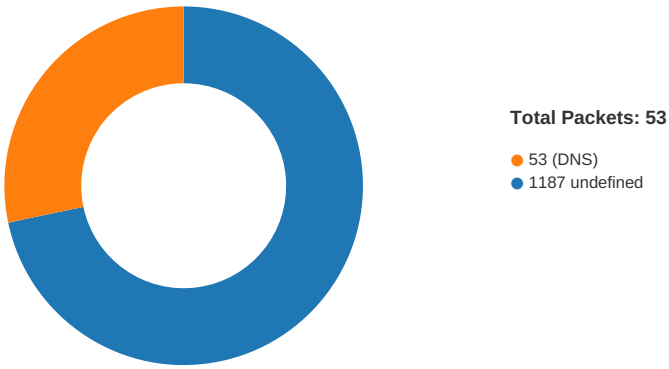
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2012
Assembly Version	1.5.0.0
InternalName	IIterat.exe
FileVersion	22.0.3.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	iiInfinityEngine Application
ProductVersion	22.0.3.0
FileDescription	iiInfinityEngine Application
OriginalFilename	IIterat.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/26/22-06:24:42.071716	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56023	8.8.8.8	192.168.2.6
01/26/22-06:24:48.449046	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60261	8.8.8.8	192.168.2.6
01/26/22-06:25:13.132016	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63745	8.8.8.8	192.168.2.6
01/26/22-06:25:19.830871	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50010	8.8.8.8	192.168.2.6
01/26/22-06:25:41.314592	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57574	8.8.8.8	192.168.2.6
01/26/22-06:26:18.057865	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60778	8.8.8.8	192.168.2.6

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 06:24:18.485788107 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:18.512763977 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:18.513204098 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:18.756021976 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:18.864753962 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:18.864942074 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:18.972136974 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:18.972227097 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:18.999602079 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.061052084 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.532491922 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.673132896 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.687484980 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.695467949 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.695513010 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.695539951 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.695554972 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.695573092 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.695601940 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.695612907 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.695621014 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.722363949 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.722410917 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.722448111 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.722481966 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.722481966 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.722515106 CET	1187	49760	85.202.169.154	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 06:24:19.722533941 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.722557068 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.722589970 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.722600937 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.722625017 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.722666979 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.749418974 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.749470949 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.749538898 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.749547958 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.749583006 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.749614954 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.749623060 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.749648094 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.749675989 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.749689102 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.749705076 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.749739885 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.749769926 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.749779940 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.749799967 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.749826908 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.749840975 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.749893904 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.749910116 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.749921083 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.749946117 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.749969006 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.749972105 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.750005960 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.776938915 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.776990891 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.777019978 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.777048111 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.777049065 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.777076960 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.777089119 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.777106047 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.777138948 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.777153015 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.777168989 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.777194977 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.777211905 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.777221918 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.777249098 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.777264118 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.777276039 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.777302027 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.777321100 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.777328968 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.777359009 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.777371883 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.777386904 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.777414083 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.777426004 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.777441025 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.777467966 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.777479887 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.777493954 CET	1187	49760	85.202.169.154	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 06:24:19.777519941 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.777534008 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.777546883 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.777573109 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.777596951 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.777605057 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.777633905 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.777648926 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.777658939 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.777681112 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.777698994 CET	49760	1187	192.168.2.6	85.202.169.154
Jan 26, 2022 06:24:19.777714014 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.777740955 CET	1187	49760	85.202.169.154	192.168.2.6
Jan 26, 2022 06:24:19.777754068 CET	49760	1187	192.168.2.6	85.202.169.154

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 06:24:17.996527910 CET	62044	53	192.168.2.6	8.8.8.8
Jan 26, 2022 06:24:18.015832901 CET	53	62044	8.8.8.8	192.168.2.6
Jan 26, 2022 06:24:25.421608925 CET	63791	53	192.168.2.6	8.8.8.8
Jan 26, 2022 06:24:25.440938950 CET	53	63791	8.8.8.8	192.168.2.6
Jan 26, 2022 06:24:32.777508020 CET	61346	53	192.168.2.6	8.8.8.8
Jan 26, 2022 06:24:32.796672106 CET	53	61346	8.8.8.8	192.168.2.6
Jan 26, 2022 06:24:42.050080061 CET	56023	53	192.168.2.6	8.8.8.8
Jan 26, 2022 06:24:42.071716070 CET	53	56023	8.8.8.8	192.168.2.6
Jan 26, 2022 06:24:48.430347919 CET	60261	53	192.168.2.6	8.8.8.8
Jan 26, 2022 06:24:48.449045897 CET	53	60261	8.8.8.8	192.168.2.6
Jan 26, 2022 06:24:55.326966047 CET	58336	53	192.168.2.6	8.8.8.8
Jan 26, 2022 06:24:55.346101999 CET	53	58336	8.8.8.8	192.168.2.6
Jan 26, 2022 06:25:02.217654943 CET	53781	53	192.168.2.6	8.8.8.8
Jan 26, 2022 06:25:02.235038042 CET	53	53781	8.8.8.8	192.168.2.6
Jan 26, 2022 06:25:08.164484978 CET	55299	53	192.168.2.6	8.8.8.8
Jan 26, 2022 06:25:08.183748960 CET	53	55299	8.8.8.8	192.168.2.6
Jan 26, 2022 06:25:13.111092091 CET	63745	53	192.168.2.6	8.8.8.8
Jan 26, 2022 06:25:13.132015944 CET	53	63745	8.8.8.8	192.168.2.6
Jan 26, 2022 06:25:19.809762001 CET	50010	53	192.168.2.6	8.8.8.8
Jan 26, 2022 06:25:19.830871105 CET	53	50010	8.8.8.8	192.168.2.6
Jan 26, 2022 06:25:26.769131899 CET	63816	53	192.168.2.6	8.8.8.8
Jan 26, 2022 06:25:26.788825035 CET	53	63816	8.8.8.8	192.168.2.6
Jan 26, 2022 06:25:34.897589922 CET	62208	53	192.168.2.6	8.8.8.8
Jan 26, 2022 06:25:34.917278051 CET	53	62208	8.8.8.8	192.168.2.6
Jan 26, 2022 06:25:41.295402050 CET	57574	53	192.168.2.6	8.8.8.8
Jan 26, 2022 06:25:41.314591885 CET	53	57574	8.8.8.8	192.168.2.6
Jan 26, 2022 06:25:46.075155973 CET	51818	53	192.168.2.6	8.8.8.8
Jan 26, 2022 06:25:46.094746113 CET	53	51818	8.8.8.8	192.168.2.6
Jan 26, 2022 06:26:18.036572933 CET	60778	53	192.168.2.6	8.8.8.8
Jan 26, 2022 06:26:18.057864904 CET	53	60778	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 26, 2022 06:24:17.996527910 CET	192.168.2.6	8.8.8.8	0x8e9c	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2022 06:24:25.421608925 CET	192.168.2.6	8.8.8.8	0xd6ac	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2022 06:24:32.777508020 CET	192.168.2.6	8.8.8.8	0xf5af	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2022 06:24:42.050080061 CET	192.168.2.6	8.8.8.8	0x1877	Standard query (0)	derarawfile10.ddns.net	A (IP address)	IN (0x0001)

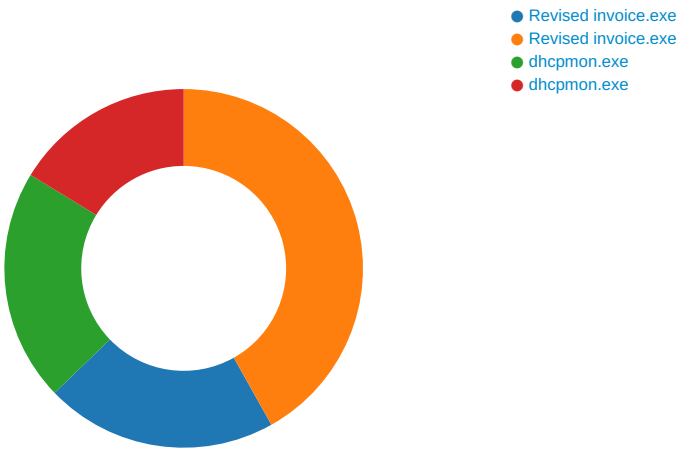
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 26, 2022 06:24:48.430347919 CET	192.168.2.6	8.8.8.8	0x92b4	Standard query (0)	derarawfil e10.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2022 06:24:55.326966047 CET	192.168.2.6	8.8.8.8	0x119c	Standard query (0)	derarawfil e10.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2022 06:25:02.217654943 CET	192.168.2.6	8.8.8.8	0xd9a6	Standard query (0)	derarawfil e10.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2022 06:25:08.164484978 CET	192.168.2.6	8.8.8.8	0xbbf0	Standard query (0)	derarawfil e10.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2022 06:25:13.111092091 CET	192.168.2.6	8.8.8.8	0x42ac	Standard query (0)	derarawfil e10.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2022 06:25:19.809762001 CET	192.168.2.6	8.8.8.8	0x890c	Standard query (0)	derarawfil e10.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2022 06:25:26.769131899 CET	192.168.2.6	8.8.8.8	0xdb32	Standard query (0)	derarawfil e10.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2022 06:25:34.897589922 CET	192.168.2.6	8.8.8.8	0x7daa	Standard query (0)	derarawfil e10.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2022 06:25:41.295402050 CET	192.168.2.6	8.8.8.8	0xc438	Standard query (0)	derarawfil e10.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2022 06:25:46.075155973 CET	192.168.2.6	8.8.8.8	0xa1b5	Standard query (0)	derarawfil e10.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2022 06:26:18.036572933 CET	192.168.2.6	8.8.8.8	0xd979	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 26, 2022 06:24:18.015832901 CET	8.8.8.8	192.168.2.6	0x8e9c	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)
Jan 26, 2022 06:24:25.440938950 CET	8.8.8.8	192.168.2.6	0xd6ac	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)
Jan 26, 2022 06:24:32.796672106 CET	8.8.8.8	192.168.2.6	0xf5af	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)
Jan 26, 2022 06:24:42.071716070 CET	8.8.8.8	192.168.2.6	0x1877	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)
Jan 26, 2022 06:24:48.449045897 CET	8.8.8.8	192.168.2.6	0x92b4	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)
Jan 26, 2022 06:24:55.346101999 CET	8.8.8.8	192.168.2.6	0x119c	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)
Jan 26, 2022 06:25:02.235038042 CET	8.8.8.8	192.168.2.6	0xd9a6	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)
Jan 26, 2022 06:25:08.183748960 CET	8.8.8.8	192.168.2.6	0xbbf0	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)
Jan 26, 2022 06:25:13.132015944 CET	8.8.8.8	192.168.2.6	0x42ac	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)
Jan 26, 2022 06:25:19.830871105 CET	8.8.8.8	192.168.2.6	0x890c	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)
Jan 26, 2022 06:25:26.788825035 CET	8.8.8.8	192.168.2.6	0xdb32	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)
Jan 26, 2022 06:25:34.917278051 CET	8.8.8.8	192.168.2.6	0x7daa	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)
Jan 26, 2022 06:25:41.314591885 CET	8.8.8.8	192.168.2.6	0xc438	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)
Jan 26, 2022 06:25:46.094746113 CET	8.8.8.8	192.168.2.6	0xa1b5	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)
Jan 26, 2022 06:26:18.057864904 CET	8.8.8.8	192.168.2.6	0xd979	No error (0)	derarawfil e10.ddns.net		85.202.169.154	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: Revised invoice.exe PID: **6272**, Parent PID: **5308**

General

Target ID:	0
Start time:	06:23:41
Start date:	26/01/2022
Path:	C:\Users\user\Desktop\Revised invoice.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Revised invoice.exe"
Imagebase:	0xf80000
File size:	825344 bytes
MD5 hash:	4BAB1B0E7BBB12D6280A75EB3475B45B
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: 00000000.00000002.408160026.0000000004319000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.408160026.0000000004319000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.408160026.0000000004319000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.406375161.0000000003311000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.406688531.00000000033CC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
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	6F11CF06	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	6F11CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Revised invoice.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6F42C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Revised 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	6F42C907	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	6F0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6F0F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6F0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6F0FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6F0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6F0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6F0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6F0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6F0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6F0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD81B4F	ReadFile

Analysis Process: Revised invoice.exe PID: **6692**, Parent PID: **6272**

General

Target ID:	4
Start time:	06:24:06
Start date:	26/01/2022
Path:	C:\Users\user\Desktop\Revised invoice.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Revised invoice.exe
Imagebase:	0x490000
File size:	825344 bytes
MD5 hash:	4BAB1B0E7BBB12D6280A75EB3475B45B
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: 00000004.00000002.617046851.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.617046851.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.617046851.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.619048568.0000000002A3D000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.402923457.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.402923457.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.402923457.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.402001244.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.402001244.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.402001244.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.402541996.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.402541996.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.402541996.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.403354659.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.403354659.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.403354659.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.618965452.00000000029D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
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	6F11CF06	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	6F11CF06	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	6CD8BEFF	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	6CD81E60	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	6CD8BEFF	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	6CD8DD66	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	6CD8DD66	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6CD8BEFF	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	6CD8BEFF	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	5	6CD81E60	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	6CD81E60	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	6CD81E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Revised invoice.exe:Zone.Identifier	success or wait	1	6CD02935	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	04 fd 59 fd fd fd fd 48	YH	success or wait	1	6CD81B4F	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	262144	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 58 fd fd 61 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 0c 00 00 14 00 00 00 00 00 00 76 fd 0c 00 00 20 00 00 00 fd 0c 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 00 0d 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.$PELXa0v @ @	success or wait	4	6CD8DD66	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	6CD8DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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	6CD81B4F	WriteFile
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	6CD81B4F	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	6CD81B4F	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	6F0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6F0F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6F0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6F0FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6F0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6F0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6F0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6F0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6F0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6F0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD81B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6F0DD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6F0DD72F	unknown
C:\Users\user\Desktop\Revised invoice.exe	unknown	4096	success or wait	1	6F0DD72F	unknown
C:\Users\user\Desktop\Revised invoice.exe	unknown	512	success or wait	1	6F0DD72F	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	6CD8646A	RegSetValueExW

Analysis Process: dhcpmon.exe PID: **2904**, Parent PID: **3440**

General

Target ID:	11
Start time:	06:24:26
Start date:	26/01/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0xcf0000
File size:	825344 bytes
MD5 hash:	4BAB1B0E7BBB12D6280A75EB3475B45B
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: 0000000B.00000002.470438107.000000000319C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000B.00000002.469694616.00000000030E1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.471522970.00000000040E9000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.471522970.00000000040E9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.471522970.00000000040E9000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 23%, 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	6F11CF06	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	6F11CF06	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	6F42C78D	CreateFileW

File Written

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	6F42C907	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	6F0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6F0F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6F0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6F0FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6F0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6F0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6F0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6F0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6F0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6F0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD81B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD81B4F	ReadFile

Analysis Process: dhcpmon.exe PID: **5644**, Parent PID: **2904**

General

Target ID:	12
Start time:	06:24:33
Start date:	26/01/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0xce0000
File size:	825344 bytes
MD5 hash:	4BAB1B0E7BBB12D6280A75EB3475B45B
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000000.463093309.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000000.463093309.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000000.463093309.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.495569005.00000000040F9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.495569005.00000000040F9000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000000.464915224.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000000.464915224.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000000.464915224.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.492933919.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.492933919.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.492933919.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000000.463837365.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000000.463837365.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000000.463837365.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000000.465799773.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000000.465799773.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000000.465799773.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.494722519.00000000030F1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.494722519.00000000030F1000.00000004.00000800.00020000.00000000.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	6F11CF06	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	6F11CF06	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	6F0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6F0F5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6F0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6F0FCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6F0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6F0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6F0503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6F0503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6F0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6F0F5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD81B4F	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	6CD81B4F	ReadFile

Disassembly

No disassembly