ID: 385253
Sample Name: JQEl8bosea.exe
Cookbook: default.jbs
Time: 09:04:00
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

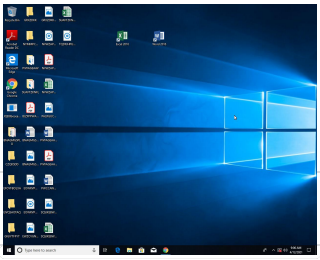
Analysis Report JQEl8bosea.exe

Overview

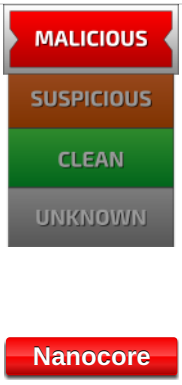
General Information

Sample Name:	JQEl8bosea.exe
Analysis ID:	385253
MD5:	ee9441f85d018a8.
SHA1:	39ac1d077fd01d0.
SHA256:	e7f54cadf8756bb..
Tags:	exe NanoCore nVpn RAT
Infos:	

Most interesting Screenshot:



Detection

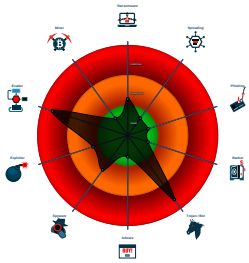


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…

Classification



Startup

- **System is w10x64**
- JQEl8bosea.exe (PID: 5988 cmdline: 'C:\Users\user\Desktop\JQEl8bosea.exe' MD5: EE9441F85D018A87729276EEA46BF51E)
  - schtasks.exe (PID: 5860 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\kpCKXquWbB' /XML 'C:\Users\user\AppData\Local\Temp\tmpF04A.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3440 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 4120 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe MD5: 71369277D09DA0830C8C59F9E22BB23A)
- dhcpmon.exe (PID: 4920 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 2212 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "f57d5a77-8670-45ef-b736-5f3a07b6",
  "Group": "Addora",
  "Domain1": "79.134.225.30",
  "Domain2": "nassiru1155.ddns.net",
  "Port": 1144,
  "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
00000004.00000002.491651474.00000000054A0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
00000004.00000002.491651474.00000000054A0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
00000004.00000002.491651474.00000000054A0000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000004.00000002.491511601.00000000051F0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000004.00000002.491511601.00000000051F0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.JQEl8bosea.exe.42b14c8.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.JQEl8bosea.exe.42b14c8.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
0.2.JQEl8bosea.exe.42b14c8.2.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
0.2.JQEl8bosea.exe.42b14c8.2.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xe0f5:$a: NanoCore • 0xe105:$a: NanoCore • 0xe339:$a: NanoCore • 0xe34d:$a: NanoCore • 0xe38d:$a: NanoCore • 0xe154:$b: ClientPlugin • 0xe356:$b: ClientPlugin • 0xe396:$b: ClientPlugin • 0xe27b:$c: ProjectData • 0xec82:$d: DESCrypto • 0x1664e:$e: KeepAlive • 0x1463c:$g: LogClientMessage • 0x10837:$i: get_Connected • 0xefb8:$j: #=q • 0xefe8:$j: #=q • 0xf004:$j: #=q • 0xf034:$j: #=q • 0xf050:$j: #=q • 0xf06c:$j: #=q • 0xf09c:$j: #=q • 0xf0b8:$j: #=q
4.2.RegSvcs.exe.51f0000.7.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
Click to see the 33 entries				

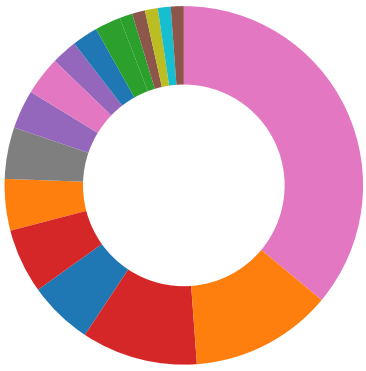
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Networking:

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

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:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

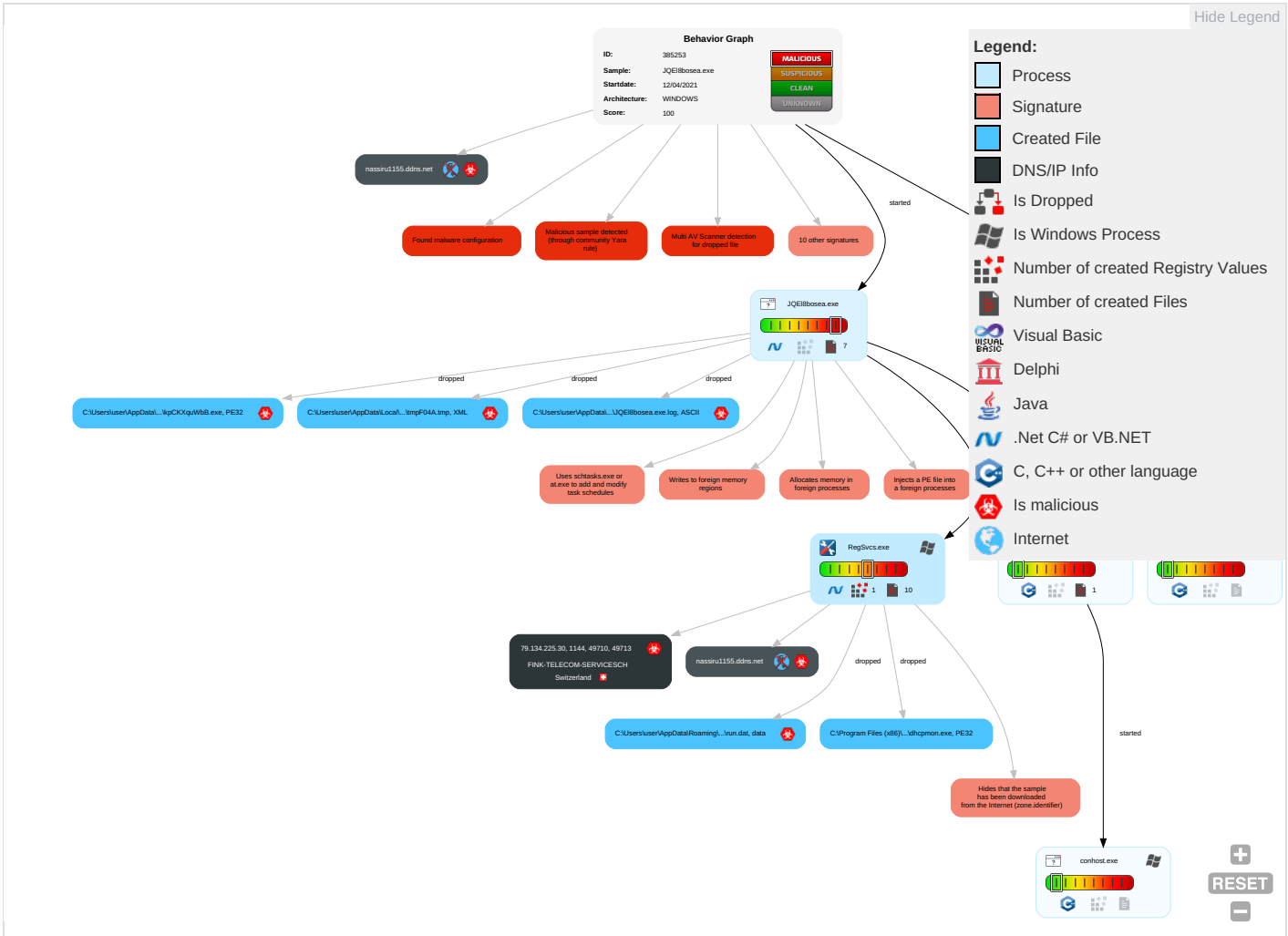
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1	Input Capture 2 1	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 3 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 3	Security Account Manager	System Information Discovery 1 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Security Software Discovery 2 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 2	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 3 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 3 1 2	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

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
JQEI8bosea.exe	36%	Virustotal		Browse
JQEI8bosea.exe	38%	ReversingLabs	Win32.Trojan.Injuke	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\kpCKXquWbB.exe	38%	ReversingLabs	Win32.Trojan.Injuke	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.2.RegSvcs.exe.54a0000.9.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.tiro.com;	0%	Avira URL Cloud	safe	
nassiru1155.ddns.net	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnS	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnU	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://weather.gc.ca/astro/seeing_e.html)	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.comH	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnH	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/a	0%	Avira URL Cloud	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/seb&	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comT	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.fonts.comicV	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/ana	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comlda	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/W	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/W	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/W	0%	URL Reputation	safe	
http://www.sandoll.co.kre	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
79.134.225.30	0%	Avira URL Cloud	safe	
http://www.fonts.comX	0%	URL Reputation	safe	
http://www.fonts.comX	0%	URL Reputation	safe	
http://www.fonts.comX	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/x	0%	Avira URL Cloud	safe	
http://www.fonts.comY	0%	Avira URL Cloud	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn0	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/rpor	0%	Avira URL Cloud	safe	
http://fontfabrik.com;	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.sandoll.co.krim	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
nassiru1155.ddns.net	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
nassiru1155.ddns.net	true	• Avira URL Cloud: safe	unknown
79.134.225.30	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

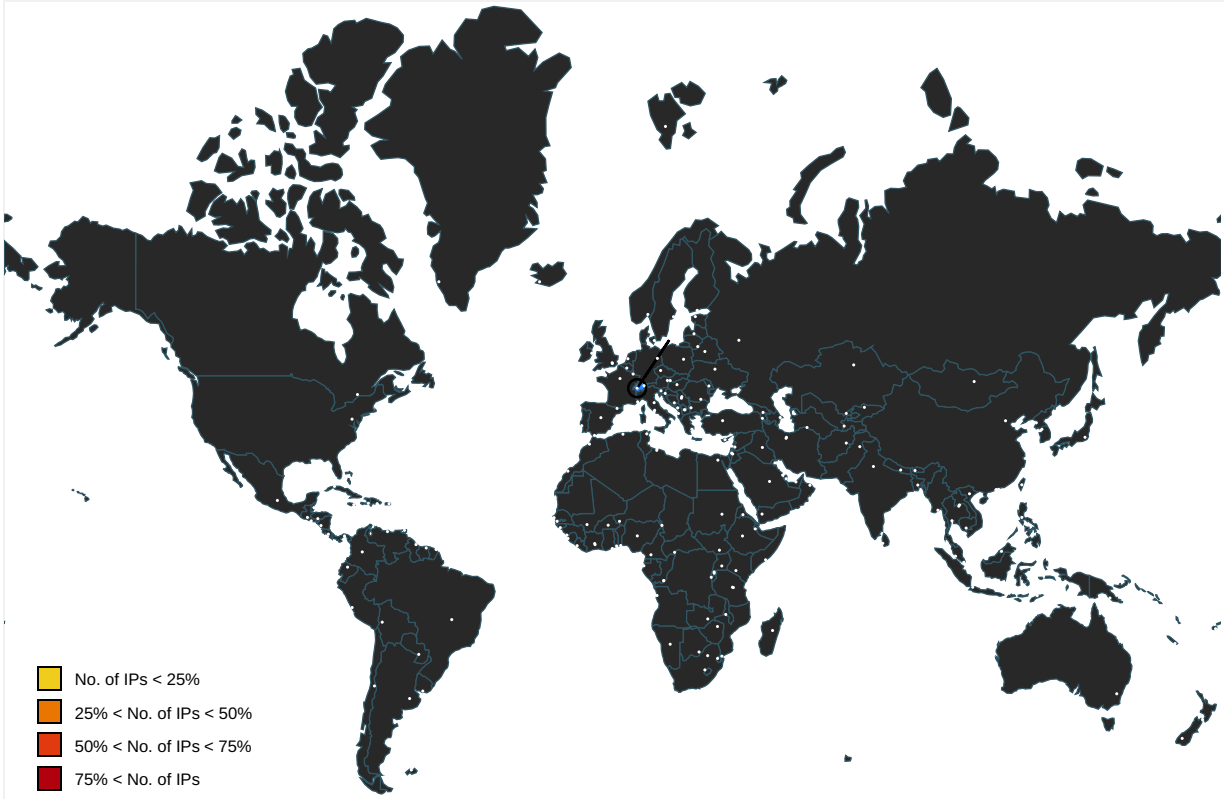
Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.com;	JQEl8bosea.exe, 00000000.00000003.212611532.000000000553B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	JQEl8bosea.exe, 00000000.00000002.252143925.00000000067B2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	JQEl8bosea.exe, 00000000.00000002.252143925.00000000067B2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	JQEl8bosea.exe, 00000000.00000002.252143925.00000000067B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	JQEl8bosea.exe, 00000000.00000002.252143925.00000000067B2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnS	JQEl8bosea.exe, 00000000.00000003.213729213.0000000005524000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnU	JQEl8bosea.exe, 00000000.00000003.213713304.000000000555D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	JQEl8bosea.exe, 00000000.00000002.252143925.00000000067B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://weather.gc.ca/astro/seeing_e.html)	JQEl8bosea.exe	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	JQEl8bosea.exe, 00000000.00000002.252143925.00000000067B2000.00000004.00000001.sdmp, JQEl8bosea.exe, 00000000.00000003.216554923.0000000005529000.00000004.00000001.sdmp, JQEl8bosea.exe, 00000000.00000003.216951988.000000000552D000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	JQEl8bosea.exe, 00000000.00000002.252143925.00000000067B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.comH	JQEl8bosea.exe, 00000000.00000003.212277776.000000000553B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnH	JQEl8bosea.exe, 00000000.00000003.213713304.000000000555D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	JQEl8bosea.exe, 00000000.00000002.248068269.000000000318D000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.com	JQEl8bosea.exe, 00000000.00000002.252143925.00000000067B2000.00000004.00000001.sdmp, JQEl8bosea.exe, 00000000.00000003.212277776.000000000553B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	JQEl8bosea.exe, 00000000.00000002.252143925.00000000067B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	JQEl8bosea.exe, 00000000.00000002.252143925.00000000067B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	JQEl8bosea.exe, 00000000.00000002.252143925.00000000067B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	JQEl8bosea.exe, 00000000.00000002.252143925.00000000067B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/a	JQEl8bosea.exe, 00000000.00000003.214865832.0000000005524000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comic	JQEl8bosea.exe, 00000000.00000003.212362251.000000000553B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/seb&	JQEl8bosea.exe, 00000000.00000003.214865832.0000000005524000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.comT	JQEl8bosea.exe, 00000000.00000003.212277776.000000000553B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp//	JQEl8bosea.exe, 00000000.00000003.214865832.0000000005524000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.comicV	JQEl8bosea.exe, 00000000.00000003.212402814.000000000553B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/ana	JQEl8bosea.exe, 00000000.00000003.214865832.0000000005524000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	JQEl8bosea.exe, 00000000.00000002.252143925.00000000067B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comlda	JQEl8bosea.exe, 00000000.00000003.239821285.0000000005520000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	JQEl8bosea.exe, 00000000.00000002.252143925.00000000067B2000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	JQEl8bosea.exe, 00000000.00000002.252143925.00000000067B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	JQEl8bosea.exe, 00000000.00000002.252143925.00000000067B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	JQEl8bosea.exe, 00000000.00000002.252143925.00000000067B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	JQEl8bosea.exe, 00000000.00000002.252143925.00000000067B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designerst	JQEl8bosea.exe, 00000000.00000003.216554923.0000000005529000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	JQEl8bosea.exe, 00000000.00000002.252143925.00000000067B2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	JQEl8bosea.exe, 00000000.00000002.252143925.00000000067B2000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/W	JQEl8bosea.exe, 00000000.00000003.214865832.0000000005524000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.kre	JQEl8bosea.exe, 00000000.00000003.213255283.0000000005529000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	JQEl8bosea.exe, 00000000.00000003.214865832.0000000005524000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.coma	JQEl8bosea.exe, 00000000.00000003.239821285.0000000005520000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comX	JQEl8bosea.exe, 00000000.00000003.212381432.000000000553B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/x	JQEl8bosea.exe, 00000000.00000003.214865832.0000000005524000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comY	JQEl8bosea.exe, 00000000.00000003.212402814.000000000553B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://en.w	JQEl8bosea.exe, 00000000.00000003.212000825.000000000148D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	JQEl8bosea.exe, 00000000.00000002.252143925.00000000067B2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	JQEl8bosea.exe, 00000000.00000003.213883793.0000000005524000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	JQEl8bosea.exe, 00000000.00000002.252143925.00000000067B2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn	JQEl8bosea.exe, 00000000.00000003.213713304.000000000555D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn0	JQEl8bosea.exe, 00000000.00000003.213713304.000000000555D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	JQEl8bosea.exe, 00000000.00000002.252143925.00000000067B2000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/s	JQEl8bosea.exe, 00000000.00000003.214865832.0000000005524000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/rpor	JQEl8bosea.exe, 00000000.00000003.214865832.0000000005524000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://fontfabrik.com;	JQEl8bosea.exe, 00000000.00000003.212590409.000000000553B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/	JQEl8bosea.exe, 00000000.00000003.214865832.0000000005524000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krim	JQEl8bosea.exe, 00000000.00000003.213255283.0000000005529000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	JQEl8bosea.exe, 00000000.00000002.252143925.00000000067B2000.00000004.00000001.sdmp, JQEl8bosea.exe, 00000000.00000003.216951988.000000000552D000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.30	unknown	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	385253
Start date:	12.04.2021
Start time:	09:04:00
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 9m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	JQEl8bosea.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:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@8/8@36/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 3.4% (good quality ratio 2.2%) • Quality average: 41.1% • Quality standard deviation: 34.8%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 104.42.151.234, 184.30.24.56, 20.50.102.62, 104.43.139.144, 20.54.26.129, 13.88.21.125, 20.82.210.154, 92.122.213.247, 92.122.213.194, 168.61.161.212, 52.255.188.83 • Excluded domains from analysis (whitelisted): fs.microsoft.com, arc.msn.com.nsatc.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:04:56	API Interceptor	1x Sleep call for process: JQEl8bosea.exe modified
09:05:06	API Interceptor	946x Sleep call for process: RegSvcs.exe modified
09:05:09	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.30	YfceI5MZX4.exe	Get hash	malicious	Browse	
	SOL2021-03-14-NETC-NI-21-049-CEVA INV.xlsx	Get hash	malicious	Browse	
	TSskTqG9V9.exe	Get hash	malicious	Browse	
	Files Specification.xlsx	Get hash	malicious	Browse	
	J62DQ7fO0b.exe	Get hash	malicious	Browse	
	oE6O5K1emC.exe	Get hash	malicious	Browse	
	AIC7VMxudf.exe	Get hash	malicious	Browse	
	Payment Confirmation.exe	Get hash	malicious	Browse	
	JOIN.exe	Get hash	malicious	Browse	
	Itinerary.pdf.exe	Get hash	malicious	Browse	
	vVH0wIFYFd.exe	Get hash	malicious	Browse	
	GWee9QSphp.exe	Get hash	malicious	Browse	
	s7pnYY2USl.jar	Get hash	malicious	Browse	
	s7pnYY2USl.jar	Get hash	malicious	Browse	
	SecuriteInfo.com.BehavesLike.Win32.Generic.dc.exe	Get hash	malicious	Browse	
	Import and Export Regulation.xlsx	Get hash	malicious	Browse	
	BBdzKOGQ36.exe	Get hash	malicious	Browse	
	BL.exe	Get hash	malicious	Browse	
	Payment Invoice.exe	Get hash	malicious	Browse	
	Payment Invoice.pdf.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	YfceI5MZX4.exe	Get hash	malicious	Browse	• 79.134.225.30
	SOL2021-03-14-NETC-NI-21-049-CEVA INV.xlsx	Get hash	malicious	Browse	• 79.134.225.30
	OjAJYVQ7iK.exe	Get hash	malicious	Browse	• 79.134.225.112
	TSskTqG9V9.exe	Get hash	malicious	Browse	• 79.134.225.30
	Files Specification.xlsx	Get hash	malicious	Browse	• 79.134.225.30
	J62DQ7fO0b.exe	Get hash	malicious	Browse	• 79.134.225.30
	oE6O5K1emC.exe	Get hash	malicious	Browse	• 79.134.225.30
	zunUbtZ2Y3.exe	Get hash	malicious	Browse	• 79.134.225.40
	EASTERS.exe	Get hash	malicious	Browse	• 79.134.225.118
	LIST OF POEA DELISTED AGENCIES.pdf.exe	Get hash	malicious	Browse	• 79.134.225.9
	AWB.pdf.exe	Get hash	malicious	Browse	• 79.134.225.102
	AIC7VMxudf.exe	Get hash	malicious	Browse	• 79.134.225.30
	9mm case for ROYAL METAL INDUSTRIES 3milmonth Specification drawings.exe	Get hash	malicious	Browse	• 79.134.225.21
	PO50164.exe	Get hash	malicious	Browse	• 79.134.225.79
	Fast color scan to a PDFfile_1_20210331084231346.pdf.exe	Get hash	malicious	Browse	• 79.134.225.102
	n7dIHuG3v6.exe	Get hash	malicious	Browse	• 79.134.225.92
	F6JT4fXIAQ.exe	Get hash	malicious	Browse	• 79.134.225.92
	order_inquiry2094.xls.exe	Get hash	malicious	Browse	• 79.134.225.102
	5H957qLghX.exe	Get hash	malicious	Browse	• 79.134.225.25
	yBio5dWAOl.exe	Get hash	malicious	Browse	• 79.134.225.7

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	YfceI5MZX4.exe	Get hash	malicious	Browse	
	TSskTqG9V9.exe	Get hash	malicious	Browse	
	oE6O5K1emC.exe	Get hash	malicious	Browse	
	GS_ PO NO.1862021.exe	Get hash	malicious	Browse	
	wDIaJji4Vv.exe	Get hash	malicious	Browse	
	cJtVGjtNGZ.exe	Get hash	malicious	Browse	
	Bilansno placanje.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Inject4.9647.20479.exe	Get hash	malicious	Browse	
	wnIPBdB5OF.exe	Get hash	malicious	Browse	
	Delivery Form C.exe	Get hash	malicious	Browse	
	h6uc8EaDQX.exe	Get hash	malicious	Browse	
	3aDHivUqWtumbXb.exe	Get hash	malicious	Browse	
	fMy120EQiT6NaRd.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Bulz.394792.29952.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.578.18498.exe	Get hash	malicious	Browse	
	sfTZCyMKuC.exe	Get hash	malicious	Browse	
	y9Rtu1cnBk.exe	Get hash	malicious	Browse	
	lxli7b5j6A.exe	Get hash	malicious	Browse	
	nq0aCrCXyE.exe	Get hash	malicious	Browse	
	73SriHObnQ.exe	Get hash	malicious	Browse	

Created / dropped Files

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

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	3.7515815714465193
Encrypted:	false
SSDEEP:	384:BOj9Y8/gS7SDriLGKq1MHR5U4Ag6ihJSxUCR1rgCPKabK2t0X5P7DZ+JgWSW72uw:B+gSAdN1MH3HAFRJngW2u
MD5:	71369277D09DA0830C8C59F9E22BB23A
SHA1:	37F9781314F0F6B7E9CB529A573F2B1C8DE9E93F
SHA-256:	D4527B7AD2FC4778CC5BE8709C95AEA44EAC0568B367EE14F7357D72898C3698
SHA-512:	2F470383E3C796C4CF212EC280854DBB9E7E8C8010CE6857E58F8E7066D7516B7CD7039BC5C0F547E1F5C7F9F2287869ADFFB2869800B08B2982A88BE96E9FB
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: YfceI5MZX4.exe, Detection: malicious, Browse • Filename: TSskTqG9V9.exe, Detection: malicious, Browse • Filename: oE6O5K1emC.exe, Detection: malicious, Browse • Filename: GS_ PO NO.1862021.exe, Detection: malicious, Browse • Filename: wDIaJji4Vv.exe, Detection: malicious, Browse • Filename: cJtVGjtNGZ.exe, Detection: malicious, Browse • Filename: Bilansno placanje.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.Inject4.9647.20479.exe, Detection: malicious, Browse • Filename: wnIPBdB5OF.exe, Detection: malicious, Browse • Filename: Delivery Form C.exe, Detection: malicious, Browse • Filename: h6uc8EaDQX.exe, Detection: malicious, Browse • Filename: 3aDHivUqWtumbXb.exe, Detection: malicious, Browse • Filename: fMy120EQiT6NaRd.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Variant.Bulz.394792.29952.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.PackedNET.578.18498.exe, Detection: malicious, Browse • Filename: sfTZCyMKuC.exe, Detection: malicious, Browse • Filename: y9Rtu1cnBk.exe, Detection: malicious, Browse • Filename: lxli7b5j6A.exe, Detection: malicious, Browse • Filename: nq0aCrCXyE.exe, Detection: malicious, Browse • Filename: 73SriHObnQ.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....{Z.....P... .....k.. .....@.. .....[.. ..@.....k..K..... k..... ....H.....text....K... ...P..... ..`.rsrc.....`.....@..@.rel oc.....p.....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\JQEl8bosea.exe.log	
Process:	C:\Users\user\Desktop\JQEl8bosea.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	664
Entropy (8bit):	5.288448637977022
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk70U2xANlW3ANv:MLF20NaL3z2p29hJ5g522rW2xAi3A9
MD5:	B1DB55991C3DA14E35249AEA1BC357CA
SHA1:	0DD2D91198FDEF296441B12F1A906669B279700C
SHA-256:	34D3E48321D5010AD2BD1F3F0B728077E4F5A7F70D66FA36B57E5209580B6BDC
SHA-512:	BE38A31888C9C2F8047FA9C99672CB985179D325107514B7500DDA9523AE3E1D20B45EACC4E6C8A5D096360D0FBB98A120E63F38FFE324DF8A0559F6890CC80
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages _v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Wind ows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\3577 4dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	120
Entropy (8bit):	5.016405576253028
Encrypted:	false
SSDEEP:	3:QHXMKaoWglAFXMWA2yTMGfsbNXLVd49Am12MFuAvOAsDeieVyn:Q3LawlAFXMWTyAGCFLIP12MUAvvrs
MD5:	50DEC1858E13F033E6DCA3CBFAD5E8DE
SHA1:	79AE1E9131B0FAF215B499D2F7B4C595AA120925
SHA-256:	14A557E226E3BA8620BB3A70035E1E316F1E9FB5C9E8F74C07110EE90B8D8AE4
SHA-512:	1BD73338DF685A5B57B0546E102ECFDEE65800410D6F77845E50456AC70DE72929088AF19B59647F01CBA7A5ACFB399C52D9EF2402A9451366586862EF88E7BF
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\tmpF04A.tmp	
Process:	C:\Users\user\Desktop\JQEl8bosea.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1643
Entropy (8bit):	5.199158359933081
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBNtn:cbh47TlNQ//rydbz9l3YODOLNdq3Z
MD5:	0332FB0ECA98F3379EA70E0DCFB31755
SHA1:	D5CCC3D9197CC94A045264E66618B2E62B5030BF
SHA-256:	A054F9074E3CD2A1A0E69802B4A44B36D3E74608420D771C7751E0E5C0445FE1
SHA-512:	FD9620E67FD8C5BDAD87B27EE7AB9B46BAA25AF75212FEF6C1008D9A753013C7FEB6832DFD14731E958D40A6B985E32A91824C19978AABA6E0E4744E81FC54 6
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:SaYP:STP
MD5:	2B990DD15E7EE3B13B7510FF9B651732
SHA1:	FA99254167129BBF23A26C368AB212620318241C
SHA-256:	C0F06C2B67C7A246395B93DF896F5BCE7A969758791900E8923EDF88C45D1538
SHA-512:	1DEFD199274B2E83B0322ADD30DC28A98162ADA8EE0DB20905ED0C7F1CF4CC28F280A899386F449874094896C5F7F93DF69F094606534B633EB171B432F85F0E
Malicious:	**true**
Reputation:	low
Preview:	N......H

C:\Users\user\AppData\Roaming\kpCKXquWbB.exe	
Process:	C:\Users\user\Desktop\JQEl8bosea.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	859648
Entropy (8bit):	7.4818373211026685
Encrypted:	false
SSDEEP:	24576:0IlGqB4X8QkYwpzEE96ok2WEcCXUlcIrGl:0PqBO9kYwpjQ59EcNvrGl
MD5:	EE9441F85D018A87729276EEA46BF51E
SHA1:	39AC1D077FD01D0D77AC41CD016849D86E3BE383
SHA-256:	E7F54CADF8756BBA15B8E5AFBCF005C42A83494E91F460B046549C58DB2CE9AF
SHA-512:	578E7C51FD6F4680DB244EEA7E0D701F19E3595243301DD081EB14608F455905E567C40924A5868E5856E162A4AAA27D34C1EC882F079AF12DA46A65346CFC35
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 38%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...`xs`.....P.....1... ...@....@.. ....@.....H1..S....@..x.....`..... ..... ..H.....text..... ..... ..`.rsrc...x....@.....@..@.rel oc.....`.....@..B.....1.....H.....>..p.....9.....c.....3\|.....C7X..<N.j.,.A...rK.%...%..o.xd...N.....YL.N.E..1.p.P.....u...Q.....S.H...'... v.z..%.iE;p2.1A..;.....?u.....o.=...o.J_....@_...}..cA..:.....ZF<..A.Gf U..KG.q.Y...q.....F..i0.+...."..?-.....U8.I.h.....p.....`.1....$;.[i[...M....>].nu..`.^.C....7.w~i.<..a...H..0:...s..rel .oR.#..dW....M.H.b...;)-..G&~.....$.....'_...y..A..`.Bg.t.`...wd.D.'.d.2_.j.m.(H:..|.....a..\..IR.

C:\Users\user\AppData\Roaming\kpCKXquWbB.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\JQEl8bosea.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1145
Entropy (8bit):	4.462201512373672
Encrypted:	false
SSDEEP:	24:zKLXkzPDObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0zPDQntKKH1MqJC
MD5:	46EBEB88876A00A52CC37B1F8E0D0438
SHA1:	5E5DB352F964E5F398301662FF558BD905798A65
SHA-256:	D65BD5A6CC112838AFE8FA70BF61FD13C1313BCE3EE3E76C50E454D7B581238B
SHA-512:	E713E6F304A469FB71235C598BC7E2C6F8458ABC61DAF3D1F364F66579CAFA4A7F3023E585BDA552FB400009E7805A8CA0311A50D5EDC9C2AD2D067772A071E E

\Device\ConDrv	
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 2.0.50727.8922..Copyright (c) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [options] AssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp Expect an existing application... /tlb:<tlbfile> Filename for the exported type library... /appname:<name> Use the specified name for the target application... /parname:<name> Use the specified name or id for the target partition... /extlb Use an existing type library... /reconfig Reconfigure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo Suppress logo output... /quiet Suppress logo output and success output...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.4818373211026685
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:	JQEl8bosea.exe
File size:	859648
MD5:	ee9441f85d018a87729276eea46bf51e
SHA1:	39ac1d077fd01d0d77ac41cd016849d86e3be383
SHA256:	e7f54cadf8756bba15b8e5afbcf005c42a83494e91f460b046549c58db2ce9af
SHA512:	578e7c51fd6f4680db244eea7e0d701f19e3595243301dd081eb14608f455905e567c40924a5868e5856e162a4aaa27d34c1ec882f079af12da46a65346cfc35
SSDEEP:	24576:0llGqB4X8QkYwpzEE96ok2WEcCXUlcIrGl:0PqBO9kYwpjQ59EcNvrGl
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...`xs`.....P.....1... ...@....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d319e
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:	0x60737860 [Sun Apr 11 22:29:52 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
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	0xd3148	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd4000	0x678	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd6000	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	0xd11a4	0xd1200	False	0.765971729304	data	7.48975303645	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xd4000	0x678	0x800	False	0.34326171875	data	3.62838077268	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd6000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xd40a0	0x3e8	data		
RT_MANIFEST	0xd4488	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

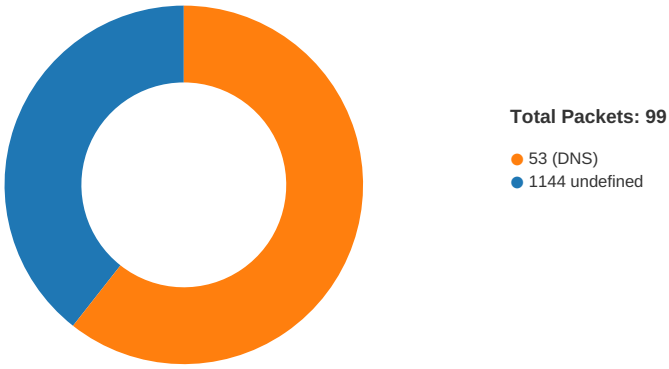
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright CodeUnit 2007
Assembly Version	2007.8.28.1
InternalName	TimeZoneInfoOptions.exe
FileVersion	2007.08.28.1
CompanyName	CodeUnit
LegalTrademarks	
Comments	Image Size Standardiser
ProductName	Image Size Standardiser
ProductVersion	2007.08.28.1
FileDescription	Image Size Standardiser
OriginalFilename	TimeZoneInfoOptions.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:05:08.009278059 CEST	49710	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:05:08.080837965 CEST	1144	49710	79.134.225.30	192.168.2.3
Apr 12, 2021 09:05:08.647866964 CEST	49710	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:05:08.720879078 CEST	1144	49710	79.134.225.30	192.168.2.3
Apr 12, 2021 09:05:09.335364103 CEST	49710	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:05:09.406732082 CEST	1144	49710	79.134.225.30	192.168.2.3
Apr 12, 2021 09:05:13.446739912 CEST	49713	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:05:13.520921946 CEST	1144	49713	79.134.225.30	192.168.2.3
Apr 12, 2021 09:05:14.038883924 CEST	49713	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:05:14.114413023 CEST	1144	49713	79.134.225.30	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:05:14.742053032 CEST	49713	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:05:14.817647934 CEST	1144	49713	79.134.225.30	192.168.2.3
Apr 12, 2021 09:05:18.823410988 CEST	49717	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:05:18.897607088 CEST	1144	49717	79.134.225.30	192.168.2.3
Apr 12, 2021 09:05:19.398766994 CEST	49717	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:05:19.473529100 CEST	1144	49717	79.134.225.30	192.168.2.3
Apr 12, 2021 09:05:19.976931095 CEST	49717	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:05:20.051358938 CEST	1144	49717	79.134.225.30	192.168.2.3
Apr 12, 2021 09:05:37.026592016 CEST	49721	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:05:37.100876093 CEST	1144	49721	79.134.225.30	192.168.2.3
Apr 12, 2021 09:05:37.650227070 CEST	49721	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:05:37.724369049 CEST	1144	49721	79.134.225.30	192.168.2.3
Apr 12, 2021 09:05:38.353410006 CEST	49721	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:05:38.427665949 CEST	1144	49721	79.134.225.30	192.168.2.3
Apr 12, 2021 09:05:42.433402061 CEST	49722	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:05:42.507603884 CEST	1144	49722	79.134.225.30	192.168.2.3
Apr 12, 2021 09:05:43.041419983 CEST	49722	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:05:43.115433931 CEST	1144	49722	79.134.225.30	192.168.2.3
Apr 12, 2021 09:05:43.650800943 CEST	49722	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:05:43.724935055 CEST	1144	49722	79.134.225.30	192.168.2.3
Apr 12, 2021 09:05:47.730827093 CEST	49723	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:05:47.805217981 CEST	1144	49723	79.134.225.30	192.168.2.3
Apr 12, 2021 09:05:48.354260921 CEST	49723	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:05:48.428258896 CEST	1144	49723	79.134.225.30	192.168.2.3
Apr 12, 2021 09:05:48.932670116 CEST	49723	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:05:49.006992102 CEST	1144	49723	79.134.225.30	192.168.2.3
Apr 12, 2021 09:06:06.153006077 CEST	49737	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:06:06.224319935 CEST	1144	49737	79.134.225.30	192.168.2.3
Apr 12, 2021 09:06:06.730801105 CEST	49737	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:06:06.802294016 CEST	1144	49737	79.134.225.30	192.168.2.3
Apr 12, 2021 09:06:07.307180882 CEST	49737	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:06:07.378699064 CEST	1144	49737	79.134.225.30	192.168.2.3
Apr 12, 2021 09:06:11.389211893 CEST	49739	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:06:11.460561037 CEST	1144	49739	79.134.225.30	192.168.2.3
Apr 12, 2021 09:06:11.965631008 CEST	49739	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:06:12.037117958 CEST	1144	49739	79.134.225.30	192.168.2.3
Apr 12, 2021 09:06:12.543792963 CEST	49739	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:06:12.615716934 CEST	1144	49739	79.134.225.30	192.168.2.3
Apr 12, 2021 09:06:16.623855114 CEST	49741	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:06:16.698028088 CEST	1144	49741	79.134.225.30	192.168.2.3
Apr 12, 2021 09:06:17.203367949 CEST	49741	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:06:17.279762983 CEST	1144	49741	79.134.225.30	192.168.2.3
Apr 12, 2021 09:06:17.794704914 CEST	49741	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:06:17.868786097 CEST	1144	49741	79.134.225.30	192.168.2.3
Apr 12, 2021 09:06:34.883342028 CEST	49746	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:06:34.955228090 CEST	1144	49746	79.134.225.30	192.168.2.3
Apr 12, 2021 09:06:35.467572927 CEST	49746	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:06:35.538976908 CEST	1144	49746	79.134.225.30	192.168.2.3
Apr 12, 2021 09:06:36.045739889 CEST	49746	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:06:36.117404938 CEST	1144	49746	79.134.225.30	192.168.2.3
Apr 12, 2021 09:06:40.126153946 CEST	49752	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:06:40.197599888 CEST	1144	49752	79.134.225.30	192.168.2.3
Apr 12, 2021 09:06:40.702719927 CEST	49752	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:06:40.773889065 CEST	1144	49752	79.134.225.30	192.168.2.3
Apr 12, 2021 09:06:41.280670881 CEST	49752	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:06:41.353643894 CEST	1144	49752	79.134.225.30	192.168.2.3
Apr 12, 2021 09:06:45.360275030 CEST	49753	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:06:45.431485891 CEST	1144	49753	79.134.225.30	192.168.2.3
Apr 12, 2021 09:06:45.937397003 CEST	49753	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:06:46.008747101 CEST	1144	49753	79.134.225.30	192.168.2.3
Apr 12, 2021 09:06:46.515945911 CEST	49753	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:06:46.587429047 CEST	1144	49753	79.134.225.30	192.168.2.3
Apr 12, 2021 09:07:03.423558950 CEST	49754	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:07:03.494982958 CEST	1144	49754	79.134.225.30	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:07:04.001144886 CEST	49754	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:07:04.072335958 CEST	1144	49754	79.134.225.30	192.168.2.3
Apr 12, 2021 09:07:04.580198050 CEST	49754	1144	192.168.2.3	79.134.225.30
Apr 12, 2021 09:07:04.651410103 CEST	1144	49754	79.134.225.30	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:04:43.708234072 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:04:43.759792089 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 12, 2021 09:05:10.820460081 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:05:10.869189024 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 12, 2021 09:05:12.593740940 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:05:12.642627954 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 12, 2021 09:05:17.730418921 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:05:17.789083958 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 12, 2021 09:05:21.365081072 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:05:21.413697958 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 12, 2021 09:05:24.121512890 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:05:24.184250116 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 12, 2021 09:05:24.188559055 CEST	53195	53	192.168.2.3	8.8.4.4
Apr 12, 2021 09:05:24.249919891 CEST	53	53195	8.8.4.4	192.168.2.3
Apr 12, 2021 09:05:24.291443110 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:05:24.353029013 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 12, 2021 09:05:28.483140945 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:05:28.540317059 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 12, 2021 09:05:28.544827938 CEST	49563	53	192.168.2.3	8.8.4.4
Apr 12, 2021 09:05:28.602058887 CEST	53	49563	8.8.4.4	192.168.2.3
Apr 12, 2021 09:05:28.642529011 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:05:28.702318907 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 12, 2021 09:05:31.859446049 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:05:31.908154011 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 12, 2021 09:05:32.790673971 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:05:32.848016977 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 12, 2021 09:05:32.852798939 CEST	58823	53	192.168.2.3	8.8.4.4
Apr 12, 2021 09:05:32.909949064 CEST	53	58823	8.8.4.4	192.168.2.3
Apr 12, 2021 09:05:32.941808939 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:05:32.990444899 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 12, 2021 09:05:47.768928051 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:05:47.839797020 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 12, 2021 09:05:53.051625013 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:05:53.109354973 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 12, 2021 09:05:53.112921000 CEST	53034	53	192.168.2.3	8.8.4.4
Apr 12, 2021 09:05:53.161513090 CEST	53	53034	8.8.4.4	192.168.2.3
Apr 12, 2021 09:05:53.304538965 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:05:53.364343882 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 12, 2021 09:05:54.289810896 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:05:54.338396072 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 12, 2021 09:05:56.014453888 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:05:56.063127041 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 12, 2021 09:05:57.506633043 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:05:57.566809893 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 12, 2021 09:05:57.570873976 CEST	58987	53	192.168.2.3	8.8.4.4
Apr 12, 2021 09:05:57.621113062 CEST	53	58987	8.8.4.4	192.168.2.3
Apr 12, 2021 09:05:57.731434107 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:05:57.788477898 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 12, 2021 09:05:58.570832968 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:05:58.619451046 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 12, 2021 09:05:58.883003950 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:05:58.934390068 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 12, 2021 09:06:01.866025925 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:06:01.924539089 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 12, 2021 09:06:01.927740097 CEST	64938	53	192.168.2.3	8.8.4.4
Apr 12, 2021 09:06:01.988298893 CEST	53	64938	8.8.4.4	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 09:06:02.031160116 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:06:02.082571983 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 12, 2021 09:06:03.813141108 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:06:03.871764898 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 12, 2021 09:06:05.643884897 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:06:05.692625046 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 12, 2021 09:06:07.051897049 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:06:07.100792885 CEST	53	56130	8.8.8.8	192.168.2.3
Apr 12, 2021 09:06:15.542005062 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:06:15.590805054 CEST	53	56338	8.8.8.8	192.168.2.3
Apr 12, 2021 09:06:17.418521881 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:06:17.467186928 CEST	53	59420	8.8.8.8	192.168.2.3
Apr 12, 2021 09:06:18.798449993 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:06:18.847286940 CEST	53	58784	8.8.8.8	192.168.2.3
Apr 12, 2021 09:06:21.918689013 CEST	63978	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:06:21.975641966 CEST	53	63978	8.8.8.8	192.168.2.3
Apr 12, 2021 09:06:22.010214090 CEST	62938	53	192.168.2.3	8.8.4.4
Apr 12, 2021 09:06:22.070168972 CEST	53	62938	8.8.4.4	192.168.2.3
Apr 12, 2021 09:06:22.100982904 CEST	55708	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:06:22.157732964 CEST	53	55708	8.8.8.8	192.168.2.3
Apr 12, 2021 09:06:26.204421997 CEST	56803	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:06:26.261703968 CEST	53	56803	8.8.8.8	192.168.2.3
Apr 12, 2021 09:06:26.265151024 CEST	57145	53	192.168.2.3	8.8.4.4
Apr 12, 2021 09:06:26.322006941 CEST	53	57145	8.8.4.4	192.168.2.3
Apr 12, 2021 09:06:26.364600897 CEST	55359	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:06:26.413167953 CEST	53	55359	8.8.8.8	192.168.2.3
Apr 12, 2021 09:06:30.485357046 CEST	58306	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:06:30.533978939 CEST	53	58306	8.8.8.8	192.168.2.3
Apr 12, 2021 09:06:30.681742907 CEST	64124	53	192.168.2.3	8.8.4.4
Apr 12, 2021 09:06:30.738754034 CEST	53	64124	8.8.4.4	192.168.2.3
Apr 12, 2021 09:06:30.771049976 CEST	49361	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:06:30.819739103 CEST	53	49361	8.8.8.8	192.168.2.3
Apr 12, 2021 09:06:33.615156889 CEST	63150	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:06:33.666977882 CEST	53	63150	8.8.8.8	192.168.2.3
Apr 12, 2021 09:06:34.751358032 CEST	53279	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:06:34.802962065 CEST	53	53279	8.8.8.8	192.168.2.3
Apr 12, 2021 09:06:35.169784069 CEST	56881	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:06:35.218888044 CEST	53	56881	8.8.8.8	192.168.2.3
Apr 12, 2021 09:06:36.387805939 CEST	53642	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:06:36.439663887 CEST	53	53642	8.8.8.8	192.168.2.3
Apr 12, 2021 09:06:37.013063908 CEST	55667	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:06:37.085361958 CEST	53	55667	8.8.8.8	192.168.2.3
Apr 12, 2021 09:06:37.192425013 CEST	54833	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:06:37.249574900 CEST	53	54833	8.8.8.8	192.168.2.3
Apr 12, 2021 09:06:38.487384081 CEST	62476	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:06:38.535991907 CEST	53	62476	8.8.8.8	192.168.2.3
Apr 12, 2021 09:06:50.626095057 CEST	49705	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:06:50.674719095 CEST	53	49705	8.8.8.8	192.168.2.3
Apr 12, 2021 09:06:50.706913948 CEST	61477	53	192.168.2.3	8.8.4.4
Apr 12, 2021 09:06:50.758378029 CEST	53	61477	8.8.4.4	192.168.2.3
Apr 12, 2021 09:06:50.779200077 CEST	61633	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:06:50.839865923 CEST	53	61633	8.8.8.8	192.168.2.3
Apr 12, 2021 09:06:54.879085064 CEST	55949	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:06:54.936000109 CEST	53	55949	8.8.8.8	192.168.2.3
Apr 12, 2021 09:06:54.941035986 CEST	57601	53	192.168.2.3	8.8.4.4
Apr 12, 2021 09:06:54.998331070 CEST	53	57601	8.8.4.4	192.168.2.3
Apr 12, 2021 09:06:55.037755013 CEST	49342	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:06:55.089405060 CEST	53	49342	8.8.8.8	192.168.2.3
Apr 12, 2021 09:06:59.118042946 CEST	56253	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:06:59.175786972 CEST	53	56253	8.8.8.8	192.168.2.3
Apr 12, 2021 09:06:59.305886984 CEST	49667	53	192.168.2.3	8.8.4.4
Apr 12, 2021 09:06:59.354918003 CEST	53	49667	8.8.4.4	192.168.2.3
Apr 12, 2021 09:06:59.358638048 CEST	55439	53	192.168.2.3	8.8.8.8
Apr 12, 2021 09:06:59.416088104 CEST	53	55439	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 09:05:24.121512890 CEST	192.168.2.3	8.8.8.8	0x9039	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:24.188559055 CEST	192.168.2.3	8.8.4.4	0x184a	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:24.291443110 CEST	192.168.2.3	8.8.8.8	0x7b79	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:28.483140945 CEST	192.168.2.3	8.8.8.8	0x5ba5	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:28.544827938 CEST	192.168.2.3	8.8.4.4	0xd1fa	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:28.642529011 CEST	192.168.2.3	8.8.8.8	0xef9b	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:32.790673971 CEST	192.168.2.3	8.8.8.8	0x1a62	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:32.852798939 CEST	192.168.2.3	8.8.4.4	0x9b6	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:32.941808939 CEST	192.168.2.3	8.8.8.8	0x8ba4	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:53.051625013 CEST	192.168.2.3	8.8.8.8	0x2d5a	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:53.112921000 CEST	192.168.2.3	8.8.4.4	0x88d6	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:53.304538965 CEST	192.168.2.3	8.8.8.8	0x3dbb	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:57.506633043 CEST	192.168.2.3	8.8.8.8	0x2af8	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:57.570873976 CEST	192.168.2.3	8.8.4.4	0xd560	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:57.731434107 CEST	192.168.2.3	8.8.8.8	0xec73	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:01.866025925 CEST	192.168.2.3	8.8.8.8	0xf2ec	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:01.927740097 CEST	192.168.2.3	8.8.4.4	0x6780	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:02.031160116 CEST	192.168.2.3	8.8.8.8	0x95fc	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:21.918689013 CEST	192.168.2.3	8.8.8.8	0x7982	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:22.010214090 CEST	192.168.2.3	8.8.4.4	0x1a01	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:22.100982904 CEST	192.168.2.3	8.8.8.8	0x24f4	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:26.204421997 CEST	192.168.2.3	8.8.8.8	0x2dda	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:26.265151024 CEST	192.168.2.3	8.8.4.4	0xb8ae	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:26.364600897 CEST	192.168.2.3	8.8.8.8	0x98b3	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:30.485357046 CEST	192.168.2.3	8.8.8.8	0xbcd1	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:30.681742907 CEST	192.168.2.3	8.8.4.4	0x3ef4	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:30.771049976 CEST	192.168.2.3	8.8.8.8	0x2db3	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:50.626095057 CEST	192.168.2.3	8.8.8.8	0xefb1	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:50.706913948 CEST	192.168.2.3	8.8.4.4	0xfa35	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:50.779200077 CEST	192.168.2.3	8.8.8.8	0xc1d4	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:54.879085064 CEST	192.168.2.3	8.8.8.8	0xfdff	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:54.941035986 CEST	192.168.2.3	8.8.4.4	0xf3ab	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:55.037755013 CEST	192.168.2.3	8.8.8.8	0xf1c	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:59.118042946 CEST	192.168.2.3	8.8.8.8	0x44a6	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:59.305886984 CEST	192.168.2.3	8.8.4.4	0x6e36	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:59.358638048 CEST	192.168.2.3	8.8.8.8	0x83d7	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

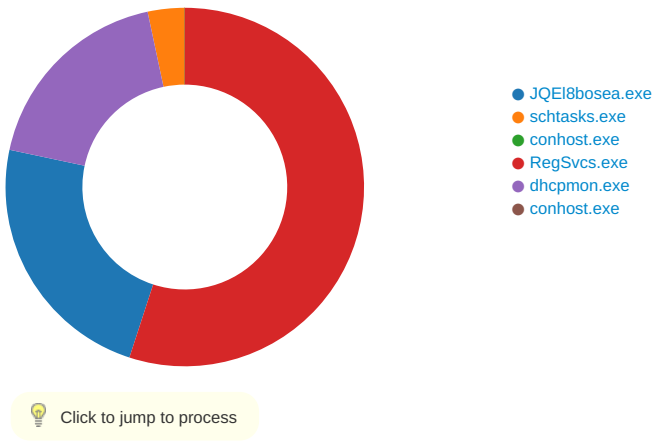
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 09:05:24.184250116 CEST	8.8.8.8	192.168.2.3	0x9039	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:24.249919891 CEST	8.8.4.4	192.168.2.3	0x184a	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:24.353029013 CEST	8.8.8.8	192.168.2.3	0x7b79	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:28.540317059 CEST	8.8.8.8	192.168.2.3	0x5ba5	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:28.602058887 CEST	8.8.4.4	192.168.2.3	0xd1fa	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:28.702318907 CEST	8.8.8.8	192.168.2.3	0xef9b	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:32.848016977 CEST	8.8.8.8	192.168.2.3	0x1a62	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:32.909949064 CEST	8.8.4.4	192.168.2.3	0x9b6	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:32.990444899 CEST	8.8.8.8	192.168.2.3	0x8ba4	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:53.109354973 CEST	8.8.8.8	192.168.2.3	0x2d5a	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:53.161513090 CEST	8.8.4.4	192.168.2.3	0x88d6	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:53.364343882 CEST	8.8.8.8	192.168.2.3	0x3dbb	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:57.566809893 CEST	8.8.8.8	192.168.2.3	0x2af8	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:57.621113062 CEST	8.8.4.4	192.168.2.3	0xd560	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:05:57.788477898 CEST	8.8.8.8	192.168.2.3	0xec73	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:01.924539089 CEST	8.8.8.8	192.168.2.3	0xf2ec	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:01.988298893 CEST	8.8.4.4	192.168.2.3	0x6780	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:02.082571983 CEST	8.8.8.8	192.168.2.3	0x95fc	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:21.975641966 CEST	8.8.8.8	192.168.2.3	0x7982	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:22.070168972 CEST	8.8.4.4	192.168.2.3	0x1a01	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:22.157732964 CEST	8.8.8.8	192.168.2.3	0x24f4	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:26.261703968 CEST	8.8.8.8	192.168.2.3	0x2dda	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:26.322006941 CEST	8.8.4.4	192.168.2.3	0xb8ae	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:26.413167953 CEST	8.8.8.8	192.168.2.3	0x98b3	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:30.533978939 CEST	8.8.8.8	192.168.2.3	0xbcd1	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 09:06:30.738754034 CEST	8.8.4.4	192.168.2.3	0x3ef4	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:30.819739103 CEST	8.8.8.8	192.168.2.3	0x2db3	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:50.674719095 CEST	8.8.8.8	192.168.2.3	0xefb1	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:50.758378029 CEST	8.8.4.4	192.168.2.3	0xfa35	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:50.839865923 CEST	8.8.8.8	192.168.2.3	0xc1d4	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:54.936000109 CEST	8.8.8.8	192.168.2.3	0xfdff	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:54.998331070 CEST	8.8.4.4	192.168.2.3	0xf3ab	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:55.089405060 CEST	8.8.8.8	192.168.2.3	0xf1c	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:59.175786972 CEST	8.8.8.8	192.168.2.3	0x44a6	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:59.354918003 CEST	8.8.4.4	192.168.2.3	0x6e36	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 09:06:59.416088104 CEST	8.8.8.8	192.168.2.3	0x83d7	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: JQEl8bosea.exe PID: 5988 Parent PID: 5732

General

Start time:	09:04:51
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\JQEl8bosea.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\JQEl8bosea.exe'
Imagebase:	0x960000
File size:	859648 bytes
MD5 hash:	EE9441F85D018A87729276EEA46BF51E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.248068269.000000000318D000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.248908706.0000000004219000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.248908706.0000000004219000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.248908706.0000000004219000.00000004.00000001.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	72FB60AC	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	72FB60AC	unknown
C:\Users\user\AppData\Roaming\kpCKXquWbB.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	2CD182C	CopyFileW
C:\Users\user\AppData\Roaming\kpCKXquWbB.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	2CD182C	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpF04A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	111B2F8	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\JQEl8bosea.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF04A.tmp	success or wait	1	2CD24F2	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\kpCKXquWbB.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 60 78 73 60 00 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 12 0d 00 00 0a 00 00 00 00 00 00 9e 31 0d 00 00 20 00 00 00 40 0d 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 80 0d 00 00 02 00 00 00 00 00 00 02 00 40 85 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.... $.......PE..L...`xs`.......... ....P.............1... ...@....@.. ....@................	success or wait	4	2CD182C	CopyFileW
C:\Users\user\AppData\Roaming\kpCKXquWbB.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	2CD182C	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpF04A.tmp	unknown	1643	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	2CD21AF	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\JQEl8bosea.exe.log	unknown	664	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 23 5c 63 64 37 63 37 34 66 63 65 32 61 30 65 61 62 37 32 63 64 32 35 63 62 65 34 62 62 36 31 36 31 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: schtasks.exe PID: 5860 Parent PID: 5988

General

Start time:	09:05:03
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\kpCKXquWbB' /XML 'C:\Users\user\AppData\Local\Temp\tmpF04A.tmp'
Imagebase:	0xa60000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF04A.tmp	unknown	2	success or wait	1	A6AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpF04A.tmp	unknown	1644	success or wait	1	A6ABD9	ReadFile

Analysis Process: conhost.exe PID: 3440 Parent PID: 5860

General

Start time:	09:05:04
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 4120 Parent PID: 5988

General

Start time:	09:05:04
Start date:	12/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Imagebase:	0x580000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
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: 00000004.00000002.491651474.00000000054A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.491651474.00000000054A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.491651474.00000000054A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.491511601.00000000051F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.491511601.00000000051F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.490406341.0000000003B67000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.490406341.0000000003B67000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.478005278.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.478005278.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.478005278.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	moderate

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	72FB60AC	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	72FB60AC	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	4E907A1	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	4E9089B	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	4E907A1	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	4E90B20	CopyFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	4E907A1	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	4E907A1	CreateDirectoryW
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	72FB60AC	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	72FB60AC	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	unknown	8	4e a3 10 bd cc fd d8 48	N.....H	success or wait	1	4E90A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	32768	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 cf ce 7b 5a 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 08 00 00 50 00 00 00 20 00 00 00 00 00 00 de 6b 00 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 00 00 00 10 00 00 00 b1 5b 01 00 03 00 40 05 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....$.......PE..L.....{Z.................P... ....k...........@.. ....[....@................................	success or wait	1	4E90B20	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	4E90A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	success or wait	1	4E90A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	end of file	1	4E90A53	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7308BF06	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	4E90C12	RegSetValueExW

Analysis Process: dhcpmon.exe PID: 4920 Parent PID: 3388

General

Start time:	09:05:17
Start date:	12/04/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x680000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

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	72FB60AC	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	72FB60AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	F7A53F	WriteFile
\Device\ConDrv	unknown	145	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 53 65 72 76 69 63 65 73 20 49 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 56 65 72 73 69 6f 6e 20 32 2e 30 2e 35 30 37 32 37 2e 38 39 32 32 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) .NET Framework Services Installation Utility Version 2.0.50727.8922..Copyright (c) Microsoft Corporation. All rights reserved.....	success or wait	1	F7A53F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	256	55 53 41 47 45 3a 20 72 65 67 73 76 63 73 2e 65 78 65 20 5b 6f 70 74 69 6f 6e 73 5d 20 41 73 73 65 6d 62 6c 79 4e 61 6d 65 0d 0a 4f 70 74 69 6f 6e 73 3a 0d 0a 20 20 20 20 2f 3f 20 6f 72 20 2f 68 65 6c 70 20 20 20 20 20 20 44 69 73 70 6c 61 79 20 74 68 69 73 20 75 73 61 67 65 20 6d 65 73 73 61 67 65 2e 0d 0a 20 20 20 20 2f 66 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 46 69 6e 64 20 6f 72 20 63 72 65 61 74 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 28 64 65 66 61 75 6c 74 29 2e 0d 0a 20 20 20 20 2f 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 43 72 65 61 74 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 2c 20 65 72 72 6f 72 20 69 66 20 69 74 20 61 6c 72 65 61 64 79 20 65 78 69 73 74 73 2e 0d 0a 20 20 20 20 2f 65 78 61 70 70 20	USAGE: regsvcs.exe [options] A ssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target applicat ion, error if it already exist s... /exapp	success or wait	3	F7A53F	WriteFile
\Device\ConDrv	unknown	232	53 75 70 70 72 65 73 73 20 6c 6f 67 6f 20 6f 75 74 70 75 74 2e 0d 0a 20 20 20 20 2f 71 75 69 65 74 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 53 75 70 70 72 65 73 73 20 6c 6f 67 6f 20 6f 75 74 70 75 74 20 61 6e 64 20 73 75 63 63 65 73 73 20 6f 75 74 70 75 74 2e 0d 0a 20 20 20 20 2f 63 6f 6d 70 6f 6e 6c 79 20 20 20 20 20 20 20 20 43 6f 6e 66 69 67 75 72 65 20 63 6f 6d 70 6f 6e 65 6e 74 73 20 6f 6e 6c 79 2c 20 6e 6f 20 6d 65 74 68 6f 64 73 20 6f 72 20 69 6e 74 65 72 66 61 63 65 73 2e 0d 0a 20 20 20 20 2f 61 70 70 64 69 72 3a 3c 70 61 74 68 3e 20 20 53 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 72 6f 6f 74 20 64 69 72 65 63 74 6f 72 79 20 74 6f 20 73 70 65 63 69 66 69 65 64 20 70 61 74 68 2e 0d 0a 0d 0a	Suppress logo output... /quiet Suppress logo output and success output... /componly Configure components only, no methods or inte rfaces... /appdir:<path> Set application root directory to specified path.....	success or wait	1	F7A53F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	unknown	120	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 45 6e 74 65 72 70 72 69 73 65 53 65 72 76 69 63 65 73 2c 20 56 65 72 73 69 6f 6e 3d 32 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: conhost.exe PID: 2212 Parent PID: 4920

General

Start time:	09:05:19
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis