ID: 385233
Sample Name: YfceI5MZX4.exe
Cookbook: default.jbs
Time: 08:41:27
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

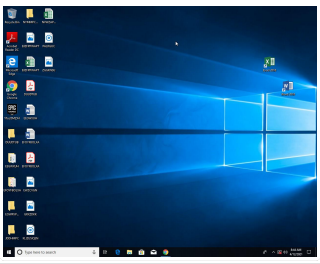
Analysis Report YfceI5MZX4.exe

Overview

General Information

Sample Name:	YfceI5MZX4.exe
Analysis ID:	385233
MD5:	a3cbeb3e732b11..
SHA1:	ebb41b49de8f1b0.
SHA256:	e006460ad1e34d..
Tags:	exe NanoCore nVpn RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

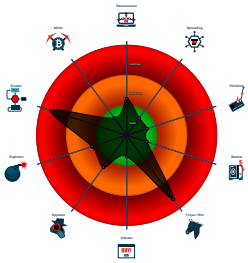
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- 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…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- YfceI5MZX4.exe (PID: 6136 cmdline: 'C:\Users\user\Desktop\YfceI5MZX4.exe' MD5: A3CBEB3E732B11954572B3EE6755242C)
  - schtasks.exe (PID: 5564 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\gmSlQSien' /XML 'C:\Users\user\AppData\Local\Temp\tmp7762.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 2908 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 5996 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe MD5: 71369277D09DA0830C8C59F9E22BB23A)
- dhcpmon.exe (PID: 6464 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 6472 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
00000005.00000002.500274474.0000000003FB B000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000005.00000002.500274474.0000000003FB B000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xf3e5:$a: NanoCore • 0xf43e:$a: NanoCore • 0xf47b:$a: NanoCore • 0xf4f4:$a: NanoCore • 0x22b9f:$a: NanoCore • 0x22bb4:$a: NanoCore • 0x22be9:$a: NanoCore • 0x3b66b:$a: NanoCore • 0x3b680:$a: NanoCore • 0x3b6b5:$a: NanoCore • 0xf447:$b: ClientPlugin • 0xf484:$b: ClientPlugin • 0xfd82:$b: ClientPlugin • 0xfd8f:$b: ClientPlugin • 0x2295b:$b: ClientPlugin • 0x22976:$b: ClientPlugin • 0x229a6:$b: ClientPlugin • 0x22bbd:$b: ClientPlugin • 0x22bf2:$b: ClientPlugin • 0x3b427:$b: ClientPlugin • 0x3b442:$b: ClientPlugin
00000005.00000002.492901504.000000000040 2000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJlLdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000005.00000002.492901504.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.492901504.000000000040 2000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.YfceI5MZX4.exe.3b51e28.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x429ad:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x429ea:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x4651d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.YfceI5MZX4.exe.3b51e28.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x42725:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x429ad:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x43fe6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x43fda:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x44e8b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x4ac42:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost • 0x429d7:$s5: IClientLoggingHost
0.2.YfceI5MZX4.exe.3b51e28.3.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.YfceI5MZX4.exe.3b51e28.3.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0x42715:$a: NanoCore • 0x42725:$a: NanoCore • 0x42959:$a: NanoCore • 0x4296d:$a: NanoCore • 0x429ad:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x42774:$b: ClientPlugin • 0x42976:$b: ClientPlugin • 0x429b6:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x4289b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x432a2:$d: DESCrypto • 0x1844e:$e: KeepAlive
5.2.RegSvcs.exe.3fd2a65.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0x23c50:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost • 0x23c7d:$x2: IClientNetworkHost
Click to see the 33 entries				

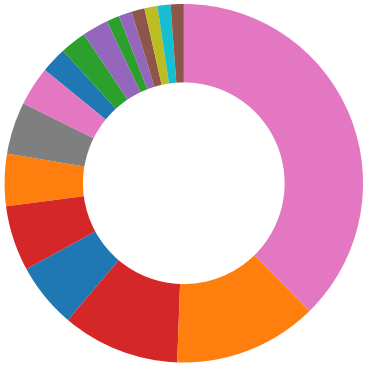
Sigma Overview

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

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

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:

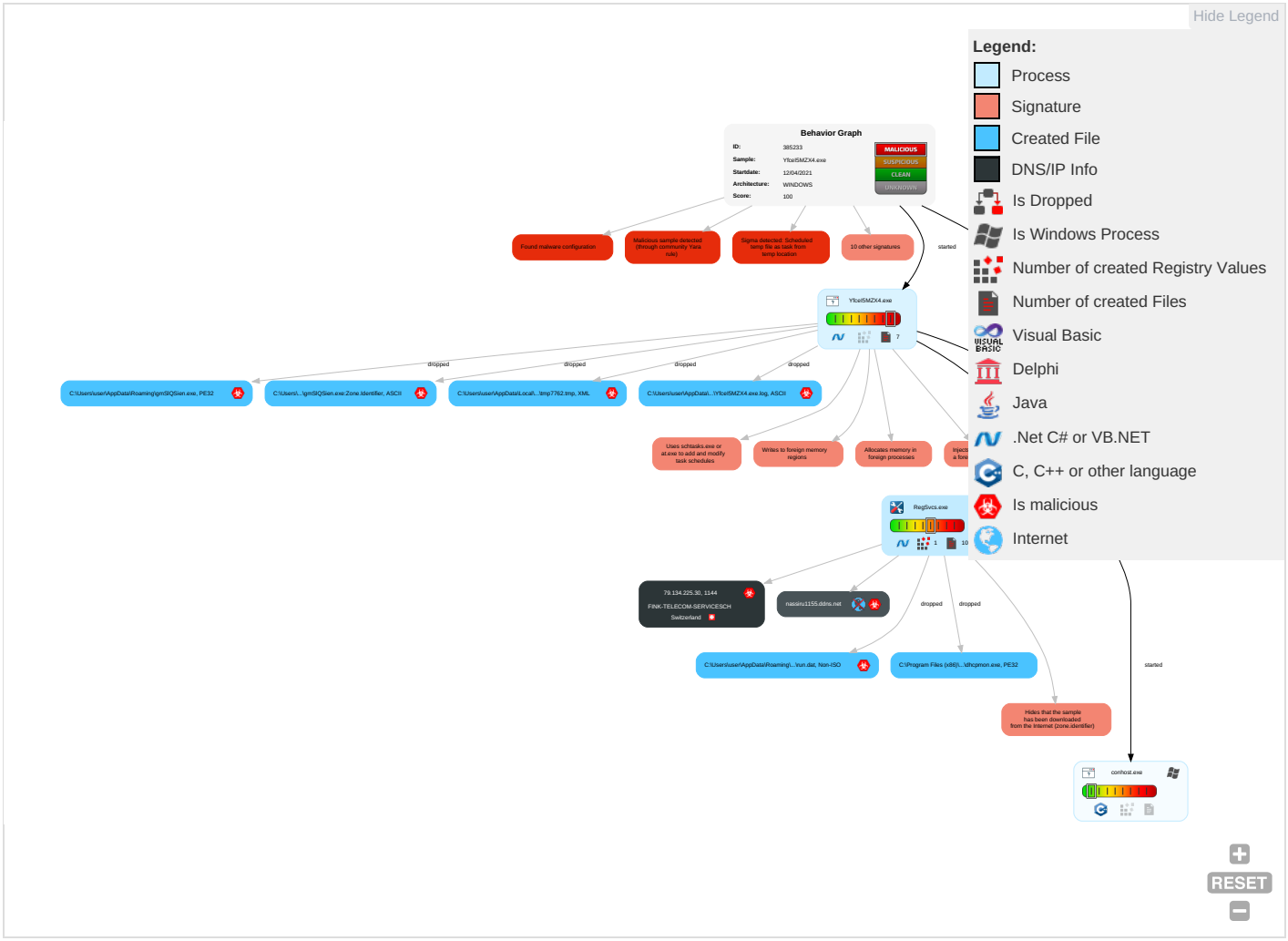
Detected Nanocore Rat

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	Masquerading 2	Input Capture 1 1	Security Software Discovery 1 1 1	Remote Services	Input Capture 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	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Application Window Discovery 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	Process Injection 3 1 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	System Information Discovery 1 3	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	Obfuscated Files or Information 3	Proc Filesystem	Network Service Scanning	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)	Software Packing 1 3	/etc/passwd and /etc/shadow	System Network Connections Discovery	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
Yfcel5MZX4.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\gmSlQSien.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.RegSvcs.exe.58d0000.9.unpack	100%	Avira	TR/NanoCore.fadte		Download File
5.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
nassiru1155.ddns.net	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krN.TTFp	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.sandoll.co.krAh	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/&t	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/=t	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://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.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.jiyu-kobo.co.jp/ut	0%	Avira URL Cloud	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	
http://www.tiro.comtn	0%	Avira URL Cloud	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.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	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.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.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.jiyu-kobo.co.jp/Lt	0%	Avira URL Cloud	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.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.jiyu-kobo.co.jp/x	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/x	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/x	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/gt	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.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.fonts.comtem7W	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.founder.com.cn/cnmf	0%	Avira URL Cloud	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	
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.founder.com.cn/cne	0%	Avira URL Cloud	safe	
http://www.fontbureau.comiona=	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnsof	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

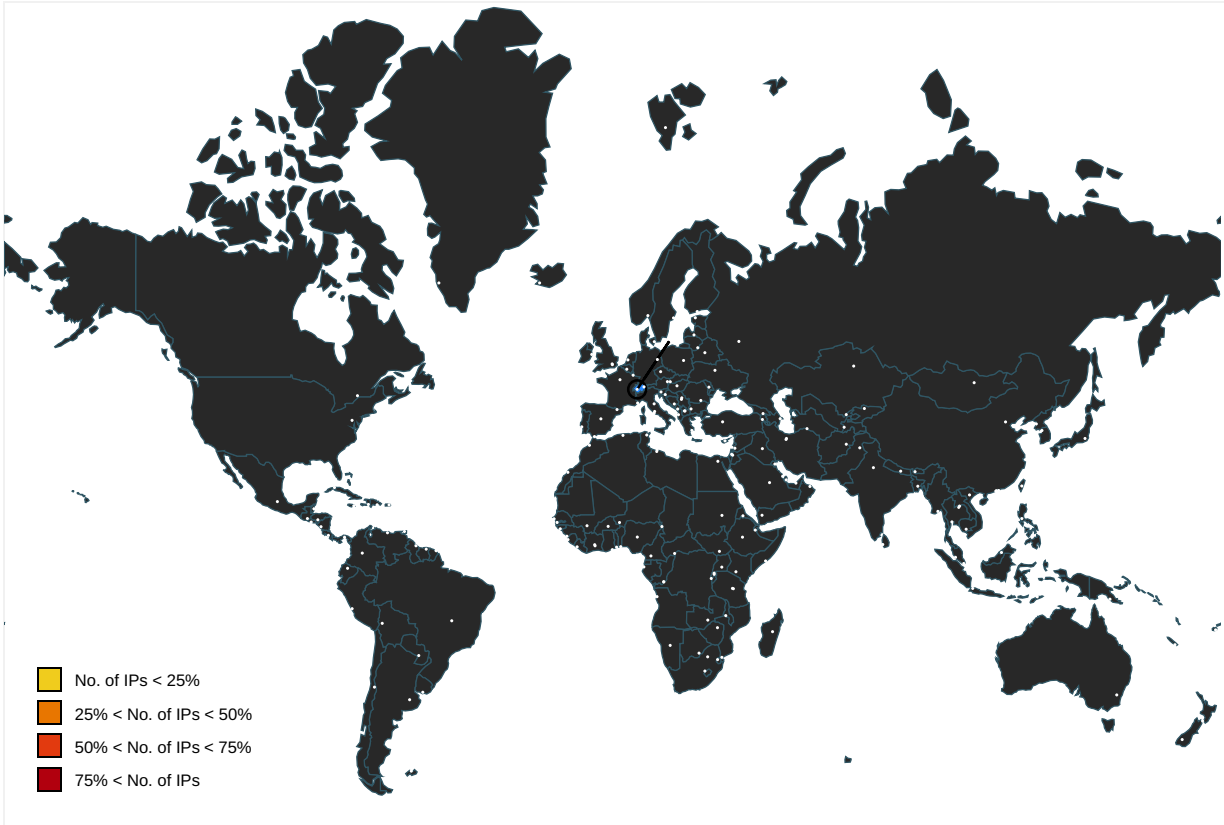
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	YfceI5MZX4.exe, 00000000.00000002.252311067.0000000006042000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	YfceI5MZX4.exe, 00000000.00000002.252311067.0000000006042000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	YfceI5MZX4.exe, 00000000.00000002.252311067.0000000006042000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.krN.TTFp	YfceI5MZX4.exe, 00000000.00000003.228260396.0000000004D09000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	YfceI5MZX4.exe, 00000000.00000002.252311067.0000000006042000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	YfceI5MZX4.exe, 00000000.00000002.252311067.0000000006042000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	YfceI5MZX4.exe, 00000000.00000002.252311067.0000000006042000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.krAh	YfceI5MZX4.exe, 00000000.00000003.228260396.0000000004D09000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/&t	YfceI5MZX4.exe, 00000000.00000003.230882117.0000000004D04000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/=t	YfceI5MZX4.exe, 00000000.00000003.230882117.0000000004D04000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	YfceI5MZX4.exe, 00000000.00000002.252311067.0000000006042000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	YfceI5MZX4.exe, 00000000.00000003.233084984.0000000004D0D000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.goodfont.co.kr	YfceI5MZX4.exe, 00000000.00000002.252311067.0000000006042000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	YfceI5MZX4.exe, 00000000.00000003.230882117.0000000004D04000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/ut	YfceI5MZX4.exe, 00000000.00000003.230882117.0000000004D04000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.coma	YfceI5MZX4.exe, 00000000.00000003.245702831.0000000004D00000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.comtn	YfceI5MZX4.exe, 00000000.00000003.227413461.0000000004D1B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comX	YfceI5MZX4.exe, 00000000.00000003.227190711.0000000004D1B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	YfceI5MZX4.exe, 00000000.00000002.247117060.0000000002945000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	YfceI5MZX4.exe, 00000000.00000002.252311067.0000000006042000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	YfceI5MZX4.exe, 00000000.00000003.227000738.0000000004D1B000.00000004.00000001.sdmp, YfceI5MZX4.exe, 00000000.00000002.252311067.0000000006042000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	YfceI5MZX4.exe, 00000000.00000003.229242210.0000000004D04000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	YfceI5MZX4.exe, 00000000.00000002.252311067.0000000006042000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	YfceI5MZX4.exe, 00000000.00000002.252311067.0000000006042000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	YfceI5MZX4.exe, 00000000.00000002.252311067.0000000006042000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Lt	YfceI5MZX4.exe, 00000000.00000003.230882117.0000000004D04000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	YfceI5MZX4.exe, 00000000.00000002.252311067.0000000006042000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	YfceI5MZX4.exe, 00000000.00000002.252311067.0000000006042000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	YfceI5MZX4.exe, 00000000.00000002.252311067.0000000006042000.00000004.00000001.sdmp, YfceI5MZX4.exe, 00000000.00000003.228908914.0000000004D3D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/x	YfceI5MZX4.exe, 00000000.00000003.230882117.0000000004D04000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	YfceI5MZX4.exe, 00000000.00000002.252311067.0000000006042000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/gt	YfceI5MZX4.exe, 00000000.00000003.230882117.0000000004D04000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	YfceI5MZX4.exe, 00000000.00000002.252311067.0000000006042000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	YfceI5MZX4.exe, 00000000.00000002.252311067.0000000006042000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	YfceI5MZX4.exe, 00000000.00000002.252311067.0000000006042000.00000004.00000001.sdmp	false		high
http://www.fonts.comtem7W	YfceI5MZX4.exe, 00000000.00000003.227156723.0000000004D1B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	YfceI5MZX4.exe, 00000000.00000002.252311067.0000000006042000.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	YfceI5MZX4.exe, 00000000.00000002.252311067.0000000006042000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnmf	YfceI5MZX4.exe, 00000000.00000003.229331040.0000000004D0B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	YfceI5MZX4.exe, 00000000.00000002.252311067.0000000006042000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	YfceI5MZX4.exe, 00000000.00000002.252311067.0000000006042000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	YfceI5MZX4.exe, 00000000.00000002.252311067.0000000006042000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cne	YfceI5MZX4.exe, 00000000.00000003.228931312.0000000004D04000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comiona=	YfceI5MZX4.exe, 00000000.00000003.245702831.0000000004D00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cnsof	YfceI5MZX4.exe, 00000000.00000003.229242210.0000000004D04000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

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:	385233
Start date:	12.04.2021
Start time:	08:41:27
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	YfceI5MZX4.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:	29
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@9/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.8% (good quality ratio 0.5%) • Quality average: 37.4% • Quality standard deviation: 34.8%
HCA Information:	• Successful, ratio: 98% • 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): 204.79.197.200, 13.107.21.200, 93.184.220.29, 20.82.210.154, 40.88.32.150, 92.122.145.220, 104.43.193.48, 184.30.24.56, 104.43.139.144, 168.61.161.212, 92.122.213.194, 92.122.213.247, 104.42.151.234, 67.26.73.254, 67.26.137.254, 8.241.78.254, 8.241.90.126, 8.241.79.126, 20.50.102.62, 20.54.26.129, 20.49.157.6 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/385233/sample/YfceI5MZX4.exe

Simulations

Behavior and APIs

Time	Type	Description
08:42:23	API Interceptor	1x Sleep call for process: YfceI5MZX4.exe modified
08:42:27	API Interceptor	981x Sleep call for process: RegSvcs.exe modified
08:42:27	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	SOL2021-03-14-NETC-NI-21-049-CEVA INV.xlsx	Get hash	malicious	Browse	
	TSskTqG9V9.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
	Inquiries_scan_011023783591374376585.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	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
	wDIaJji4Vv.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	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	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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	
	Ixli7b5j6A.exe	Get hash	malicious	Browse	
	nq0aCrCXyE.exe	Get hash	malicious	Browse	
	73SriHObnQ.exe	Get hash	malicious	Browse	
	0672IMP000158021.pdf.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:	2F470383E3C796C4CF212EC280854DBB9E7E8C8010CE6857E58F8E7066D7516B7CD7039BC5C0F547E1F5C7F9F2287869ADFFB2869800B08B2982A88BE96E9FB7
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• 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: Ixli7b5j6A.exe, Detection: malicious, Browse • Filename: nq0aCrCXyE.exe, Detection: malicious, Browse • Filename: 73SriHObnQ.exe, Detection: malicious, Browse • Filename: 0672IMP000158021.pdf.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
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\YfceI5MZX4.exe.log

Process:	C:\Users\user\Desktop\YfceI5MZX4.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

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\YfceI5MZX4.exe.log	
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.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\35774dc3cd31b4550ab06c3354cf4ba5\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\tmp7762.tmp	
Process:	C:\Users\user\Desktop\YfceI5MZX4.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1646
Entropy (8bit):	5.163880473843948
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBatn:cbhC7ZlNQF/rydbz9I3YODOLNdq3W
MD5:	50FDC626522E1DF1A07E1D398F973780
SHA1:	0ABC2C77CCC61B37DE9D46F29D4C5502E557A025
SHA-256:	1C91BC758FA2DDAAAA0436A3AA7D56AA59D381A358658FBB8632CCACE623E026
SHA-512:	A4AF7DCABE63A86D665C64C8F0C80D240D11EDEA89E4F33FDBF0E4F82EE892C61E713F6D5044CA601271DE26956B6E0A8F7A680DA8F8669EEF7DFFF4F285ED22
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>t

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:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:hRn:Ln
MD5:	A127AD6897FA6E51DF688E6D956222AC
SHA1:	0D7279C1E6363F5B40B8BE2D0B8153E84C88469F
SHA-256:	2A2A333F41D3469127ACFF3D213E66B1E987AE2DF1B47C928774B2F1757BC33B
SHA-512:	116C9B6576214AB66D5D19B2B2B7C47F3573FCB7385FB1C28E3D585B4891B2259C63A906C5951832264CFBA4F016B1ED27C5C7B1E5894333D207B5F3B7E5BC3
Malicious:	**true**
Reputation:	low
Preview:	7.D....H

C:\Users\user\AppData\Roaming\gmSlQSien.exe	
Process:	C:\Users\user\Desktop\YfceI5MZX4.exe

C:\Users\user\AppData\Roaming\gmSlQSien.exe	
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	802304
Entropy (8bit):	7.807064216316379
Encrypted:	false
SSDEEP:	12288:fqPhNb1Cpc0vs3YpRTYmuCBWhfCfyxmbKzYwafnJMKrXe3tw2luRVZzQKaq:iPhxcpHUIpRTY0c1uyUeU3nJMKoCaq
MD5:	A3CBEB3E732B11954572B3EE6755242C
SHA1:	EBB41B49DE8F1B09EA20DABFFCFD85B93B68D7F3
SHA-256:	E006460AD1E34DDBBC28430C2D529A7EE491893C7AE8B6902B2D8D8C56620510
SHA-512:	455C3CAE5F85B8F3334004E09C5EF42BB6E8410F7501AEF0D520E1023EB376E31D6FA892DAB8DC8AAEA94914F31EC7915E8424362F1046F25F9B55C58EF94BD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....s`.....P..2.....P... ..`....@.. ....@.....@P..O...`..... ..... ..H.....text....0... ...2..... ..`.rsrc.....`.....4.....@..@.rel oc.....<.....@..B.....tP.....H.....}..du.....].....0.....(....(.....(.....o ....*.....(!.....("....(#.....($.....(%....*N..(....o....(&....*&..('....*.s(.....s).....s*.....s+.....s,.....*....0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0..<.....~.....(2.....,!r...p.....(3...o4...s5.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\gmSlQSien.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\YfceI5MZX4.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
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:	E713E6F304A469FB71235C598BC7E2C6F8458ABC61DAF3D1F364F66579CAFA4A7F3023E585BDA552FB400009E7805A8CA0311A50D5EDC9C2AD2D067772A071B E
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 [optio ns] AssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target app lication, 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... /rec onfig Reconfigure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /no logo 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):	7.807064216316379

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	YfceI5MZX4.exe
File size:	802304
MD5:	a3cbeb3e732b11954572b3ee6755242c
SHA1:	ebb41b49de8f1b09ea20dabffcfd85b93b68d7f3
SHA256:	e006460ad1e34ddbbc28430c2d529a7ee491893c7ae8b6 902b2d8d8c56620510
SHA512:	455c3cae5f85b8f3334004e09c5ef42bb6e8410f7501aef0 d520e1023eb376e31d6fa892dab8dc8aaea94914f31ec79 15e8424362f1046f25f9b55c58ef94bd6
SSDEEP:	12288:fqPhNb1Cpc0vs3YpRTYmuCBWhfCfyxmbKzYw afnJMKrXe3tw2luRVZzQKaq:iPhxcpHUIpRTY0c1uyUe U3nJMKoCaq
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....s`.....P..2.....P... ...`....@.. ....@.....

File Icon

	
Icon Hash:	5dd0e0ccc4ecb3f0

Static PE Info

General

Entrypoint:	0x4b5092
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:	0x6073DD85 [Mon Apr 12 05:41:25 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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb5040	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb6000	0x107ec	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc8000	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	0xb3098	0xb3200	False	0.954216732816	data	7.9540154939	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb6000	0x107ec	0x10800	False	0.389012192235	data	4.61893381614	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc8000	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_ICON	0xb6370	0x2e8	data		
RT_ICON	0xb6658	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0xb6780	0xea8	data		
RT_ICON	0xb7628	0x8a8	data		
RT_ICON	0xb7ed0	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0xb8438	0x35e2	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		

Name	RVA	Size	Type	Language	Country
RT_ICON	0xbba1c	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 240, next used block 117440512		
RT_ICON	0xbfc44	0x25a8	data		
RT_ICON	0xc21ec	0x1a68	data		
RT_ICON	0xc3c54	0x10a8	data		
RT_ICON	0xc4cfc	0x988	data		
RT_ICON	0xc5684	0x6b8	data		
RT_ICON	0xc5d3c	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xc61a4	0xbc	data		
RT_VERSION	0xc6260	0x39e	data		
RT_MANIFEST	0xc6600	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

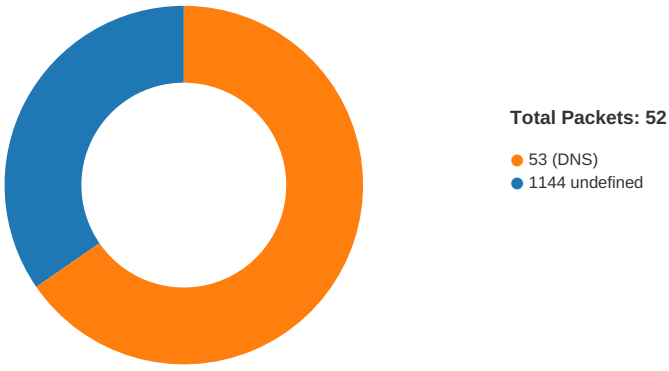
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2012
Assembly Version	8.1.1.15
InternalName	HostProtectionAttribute.exe
FileVersion	8.1.1.14
CompanyName	Landskip Yard Care
LegalTrademarks	A++
Comments	
ProductName	LevelActivator
ProductVersion	8.1.1.14
FileDescription	LevelActivator
OriginalFilename	HostProtectionAttribute.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 08:42:29.363123894 CEST	49699	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 08:42:32.425513029 CEST	49699	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 08:42:38.511714935 CEST	49699	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 08:42:49.366292953 CEST	49706	1144	192.168.2.5	79.134.225.30

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 08:42:52.418766022 CEST	49706	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 08:42:58.427855968 CEST	49706	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 08:43:08.273983955 CEST	49713	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 08:43:11.288147926 CEST	49713	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 08:43:17.304327965 CEST	49713	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 08:43:38.994872093 CEST	49722	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 08:43:42.011059999 CEST	49722	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 08:43:48.009885073 CEST	49722	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 08:43:56.278103113 CEST	49724	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 08:43:59.276504993 CEST	49724	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 08:44:05.277298927 CEST	49724	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 08:44:14.357616901 CEST	49727	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 08:44:17.356199980 CEST	49727	1144	192.168.2.5	79.134.225.30
Apr 12, 2021 08:44:23.356575012 CEST	49727	1144	192.168.2.5	79.134.225.30

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 08:42:10.067460060 CEST	52704	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:42:10.116363049 CEST	53	52704	8.8.8.8	192.168.2.5
Apr 12, 2021 08:42:10.292814970 CEST	52212	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:42:10.342643023 CEST	53	52212	8.8.8.8	192.168.2.5
Apr 12, 2021 08:42:10.418169022 CEST	54302	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:42:10.457545042 CEST	53784	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:42:10.478559971 CEST	53	54302	8.8.8.8	192.168.2.5
Apr 12, 2021 08:42:10.506891966 CEST	53	53784	8.8.8.8	192.168.2.5
Apr 12, 2021 08:42:14.032279015 CEST	65307	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:42:14.089629889 CEST	53	65307	8.8.8.8	192.168.2.5
Apr 12, 2021 08:42:14.621452093 CEST	64344	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:42:14.682523966 CEST	53	64344	8.8.8.8	192.168.2.5
Apr 12, 2021 08:42:30.647139072 CEST	62060	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:42:30.696383953 CEST	53	62060	8.8.8.8	192.168.2.5
Apr 12, 2021 08:42:37.969374895 CEST	61805	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:42:38.033551931 CEST	53	61805	8.8.8.8	192.168.2.5
Apr 12, 2021 08:42:47.482378006 CEST	54795	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:42:47.554399967 CEST	53	54795	8.8.8.8	192.168.2.5
Apr 12, 2021 08:42:55.569442034 CEST	49557	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:42:55.618032932 CEST	53	49557	8.8.8.8	192.168.2.5
Apr 12, 2021 08:42:56.509201050 CEST	61733	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:42:56.560765982 CEST	53	61733	8.8.8.8	192.168.2.5
Apr 12, 2021 08:42:57.330655098 CEST	65447	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:42:57.392369032 CEST	53	65447	8.8.8.8	192.168.2.5
Apr 12, 2021 08:42:57.416785955 CEST	52441	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:42:57.468317986 CEST	53	52441	8.8.8.8	192.168.2.5
Apr 12, 2021 08:42:58.331079006 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:42:58.382704973 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 12, 2021 08:43:05.623831987 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:43:05.681453943 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 12, 2021 08:43:14.520704985 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:43:14.572243929 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 12, 2021 08:43:15.428941965 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:43:15.477699041 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 12, 2021 08:43:16.488647938 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:43:16.545650959 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 12, 2021 08:43:17.499808073 CEST	56969	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:43:17.551426888 CEST	53	56969	8.8.8.8	192.168.2.5
Apr 12, 2021 08:43:18.761195898 CEST	55161	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:43:18.820871115 CEST	53	55161	8.8.8.8	192.168.2.5
Apr 12, 2021 08:43:25.496901989 CEST	54757	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:43:25.556852102 CEST	53	54757	8.8.8.8	192.168.2.5
Apr 12, 2021 08:43:25.590512991 CEST	49992	53	192.168.2.5	8.8.4.4
Apr 12, 2021 08:43:25.642020941 CEST	53	49992	8.8.4.4	192.168.2.5
Apr 12, 2021 08:43:25.719460964 CEST	60075	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:43:25.781299114 CEST	53	60075	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 12, 2021 08:43:29.804601908 CEST	55016	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:43:29.853324890 CEST	53	55016	8.8.8.8	192.168.2.5
Apr 12, 2021 08:43:30.054189920 CEST	64345	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:43:30.113343954 CEST	53	64345	8.8.8.8	192.168.2.5
Apr 12, 2021 08:43:30.342442989 CEST	57128	53	192.168.2.5	8.8.4.4
Apr 12, 2021 08:43:30.399633884 CEST	53	57128	8.8.4.4	192.168.2.5
Apr 12, 2021 08:43:30.409482956 CEST	54791	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:43:30.458221912 CEST	53	54791	8.8.8.8	192.168.2.5
Apr 12, 2021 08:43:33.248797894 CEST	50463	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:43:33.309731007 CEST	53	50463	8.8.8.8	192.168.2.5
Apr 12, 2021 08:43:34.618954897 CEST	50394	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:43:34.677774906 CEST	53	50394	8.8.8.8	192.168.2.5
Apr 12, 2021 08:43:34.846693993 CEST	58530	53	192.168.2.5	8.8.4.4
Apr 12, 2021 08:43:34.903510094 CEST	53	58530	8.8.4.4	192.168.2.5
Apr 12, 2021 08:43:34.932809114 CEST	53813	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:43:34.981901884 CEST	53	53813	8.8.8.8	192.168.2.5
Apr 12, 2021 08:43:49.493936062 CEST	63732	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:43:49.559073925 CEST	53	63732	8.8.8.8	192.168.2.5
Apr 12, 2021 08:44:12.017734051 CEST	57344	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:44:12.069437027 CEST	53	57344	8.8.8.8	192.168.2.5
Apr 12, 2021 08:44:13.993952036 CEST	54450	53	192.168.2.5	8.8.8.8
Apr 12, 2021 08:44:14.042953014 CEST	53	54450	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 12, 2021 08:43:25.496901989 CEST	192.168.2.5	8.8.8.8	0x2d32	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 08:43:25.590512991 CEST	192.168.2.5	8.8.4.4	0x5856	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 08:43:25.719460964 CEST	192.168.2.5	8.8.8.8	0x3e34	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 08:43:30.054189920 CEST	192.168.2.5	8.8.8.8	0x287e	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 08:43:30.342442989 CEST	192.168.2.5	8.8.4.4	0xa69	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 08:43:30.409482956 CEST	192.168.2.5	8.8.8.8	0xdd53	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 08:43:34.618954897 CEST	192.168.2.5	8.8.8.8	0xaa7	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 08:43:34.846693993 CEST	192.168.2.5	8.8.4.4	0xea51	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)
Apr 12, 2021 08:43:34.932809114 CEST	192.168.2.5	8.8.8.8	0x471	Standard query (0)	nassiru1155.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

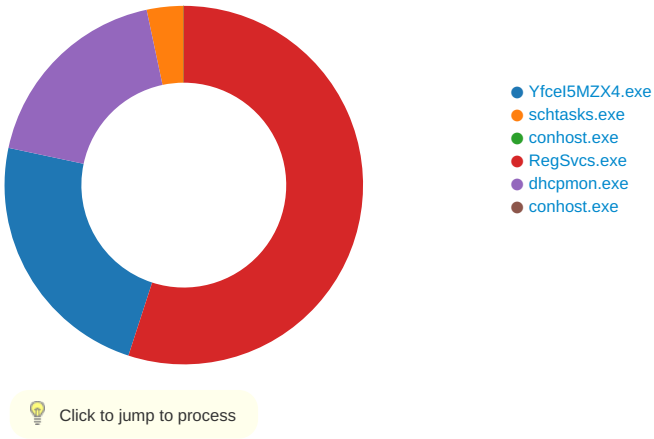
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 12, 2021 08:43:25.556852102 CEST	8.8.8.8	192.168.2.5	0x2d32	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 08:43:25.642020941 CEST	8.8.4.4	192.168.2.5	0x5856	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 08:43:25.781299114 CEST	8.8.8.8	192.168.2.5	0x3e34	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 08:43:30.113343954 CEST	8.8.8.8	192.168.2.5	0x287e	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 08:43:30.399633884 CEST	8.8.4.4	192.168.2.5	0xa69	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 08:43:30.458221912 CEST	8.8.8.8	192.168.2.5	0xdd53	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 08:43:34.677774906 CEST	8.8.8.8	192.168.2.5	0xaa7	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 08:43:34.903510094 CEST	8.8.4.4	192.168.2.5	0xea51	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)
Apr 12, 2021 08:43:34.981901884 CEST	8.8.8.8	192.168.2.5	0x471	Name error (3)	nassiru1155.ddns.net	none	none	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: YfceI5MZX4.exe PID: 6136 Parent PID: 5552

General

Start time:	08:42:17
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\YfceI5MZX4.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\YfceI5MZX4.exe'
Imagebase:	0x160000
File size:	802304 bytes
MD5 hash:	A3CBEB3E732B11954572B3EE6755242C
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: 00000000.00000002.247117060.0000000002945000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.248677483.0000000003AB9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.248677483.0000000003AB9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.248677483.0000000003AB9000.00000004.00000001.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	72B660AC	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	72B660AC	unknown
C:\Users\user\AppData\Roaming\gmSlQSien.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	6A91158	CopyFileW
C:\Users\user\AppData\Roaming\gmSlQSien.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6A91158	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp7762.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	A0B2F8	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\YfceI5MZX4.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72B534A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7762.tmp	success or wait	1	6A91EC6	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\gmSlQSien.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 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 85 dd 73 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 32 0b 00 00 0a 01 00 00 00 00 00 92 50 0b 00 00 20 00 00 00 60 0b 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 a0 0c 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.....s`.......... ....P..2...........P... ...`....@.. ....@................	success or wait	4	6A91158	CopyFileW
C:\Users\user\AppData\Roaming\gmSlQSien.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	6A91158	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp7762.tmp	unknown	1646	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 61 6c 66 6f 6e 73 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	<?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>.. </RegistrationI	success or wait	1	6A91B83	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\YfceI5MZX4.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	72E3A33A	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	72B95544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72B95544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72B98738	ReadFile

Analysis Process: schtasks.exe PID: 5564 Parent PID: 6136

General

Start time:	08:42:25
Start date:	12/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\gmSlQSien' /XML 'C:\Users\user\AppData\Local\Temp\tmp7762.tmp'
Imagebase:	0x12d0000
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\tmp7762.tmp	unknown	2	success or wait	1	12DAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7762.tmp	unknown	1647	success or wait	1	12DABD9	ReadFile

Analysis Process: conhost.exe PID: 2908 Parent PID: 5564

General

Start time:	08:42:25
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 5996 Parent PID: 6136

General

Start time:	08:42:26
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:	0x9b0000
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: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.500274474.0000000003FBB000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.500274474.0000000003FBB000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.492901504.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.492901504.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.492901504.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.501754781.0000000005470000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.501754781.0000000005470000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.502139157.00000000058D0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.502139157.00000000058D0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.502139157.00000000058D0000.00000004.00000001.sdmp, Author: Joe Security
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	72B660AC	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	72B660AC	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	52A07A1	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	52A089B	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	52A07A1	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	52A0B20	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	52A07A1	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	52A07A1	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	72B660AC	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	72B660AC	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	37 a0 44 93 c9 fd d8 48	7.D....H	success or wait	1	52A0A53	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 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 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......PE..L..... {Z.................P... ....k... ....@.. ....[....@.................	success or wait	1	52A0B20	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	72B95544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72B95544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72B95544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72B95544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72B98738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72B98738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72B98738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	72C3BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	72C3BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	4096	success or wait	1	72C3BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	512	success or wait	1	72C3BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72B95544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72B95544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72B95544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72B95544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	52A0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	success or wait	1	52A0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	end of file	1	52A0A53	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	72C3BF06	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	72C3BF06	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	52A0C12	RegSetValueExW

Analysis Process: dhcpmon.exe PID: 6464 Parent PID: 3472

General

Start time:	08:42:35
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:	0x3f0000
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	72B660AC	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	72B660AC	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	72B534A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	CEA53F	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	CEA53F	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	CEA53F	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 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	CEA53F	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	72E3A33A	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	72B95544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72B95544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72B98738	ReadFile

Analysis Process: conhost.exe PID: 6472 Parent PID: 6464

General

Start time:	08:42:36
Start date:	12/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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