ID: 384486
Sample Name:
J62DQ7fO0b.exe
Cookbook: default.jbs
Time: 10:06:11
Date: 09/04/2021
Version: 31.0.0 Emerald

Table of Contents

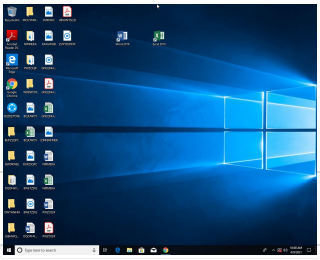
Analysis Report J62DQ7fO0b.exe

Overview

General Information

Sample Name:	J62DQ7fO0b.exe
Analysis ID:	384486
MD5:	a74ece32bc1b6d..
SHA1:	25ea63e67b8426..
SHA256:	20e490afba639ea.
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

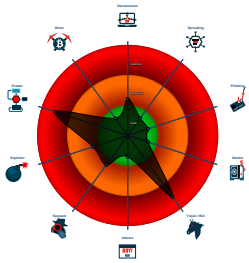
Nanocore

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…
- Snort IDS alert for network traffic (e….
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- 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…

Classification



Startup

- **System is w10x64**
- J62DQ7fO0b.exe (PID: 6516 cmdline: 'C:\Users\user\Desktop\J62DQ7fO0b.exe' MD5: A74ECE32BC1B6DB38A2D379C7FC78D2C)
  - schtasks.exe (PID: 6628 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\tHyARuOEdFlN' /XML 'C:\Users\user\AppData\Local\Temp\tmpC6A9.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6636 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 6672 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
- dhcpmon.exe (PID: 7068 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 7092 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"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.671018247.0000000002ECB000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.674143460.0000000003E7C000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1177b5:$x1: NanoCore.ClientPluginHost • 0x149fd5:$x1: NanoCore.ClientPluginHost • 0x1177f2:$x2: IClientNetworkHost • 0x14a012:$x2: IClientNetworkHost • 0x11b325:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x14db45:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.674143460.0000000003E7C000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.674143460.0000000003E7C000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x11751d:$a: NanoCore • 0x11752d:$a: NanoCore • 0x117761:$a: NanoCore • 0x117775:$a: NanoCore • 0x1177b5:$a: NanoCore • 0x149d3d:$a: NanoCore • 0x149d4d:$a: NanoCore • 0x149f81:$a: NanoCore • 0x149f95:$a: NanoCore • 0x149fd5:$a: NanoCore • 0x11757c:$b: ClientPlugin • 0x11777e:$b: ClientPlugin • 0x1177be:$b: ClientPlugin • 0x149d9c:$b: ClientPlugin • 0x149f9e:$b: ClientPlugin • 0x149fde:$b: ClientPlugin • 0x1176a3:$c: ProjectData • 0x149ec3:$c: ProjectData • 0x1180aa:$d: DESCrypto • 0x14a8ca:$d: DESCrypto • 0x11fa76:$e: KeepAlive
Process Memory Space: J62DQ7fO0b.exe PID: 6516	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
0.2.J62DQ7fO0b.exe.3f83628.1.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.J62DQ7fO0b.exe.3f83628.1.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.J62DQ7fO0b.exe.3f83628.1.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:$e: KeepAlive
0.2.J62DQ7fO0b.exe.3f83628.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.J62DQ7fO0b.exe.3f83628.1.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
Click to see the 2 entries				

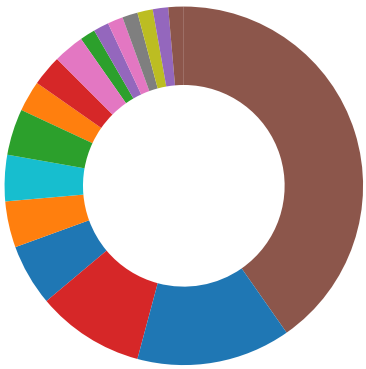
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- 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:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)

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:

- Injects a PE file into a foreign processes
- Writes to foreign memory regions

Stealing of Sensitive Information:

- Yara detected Nanocore RAT

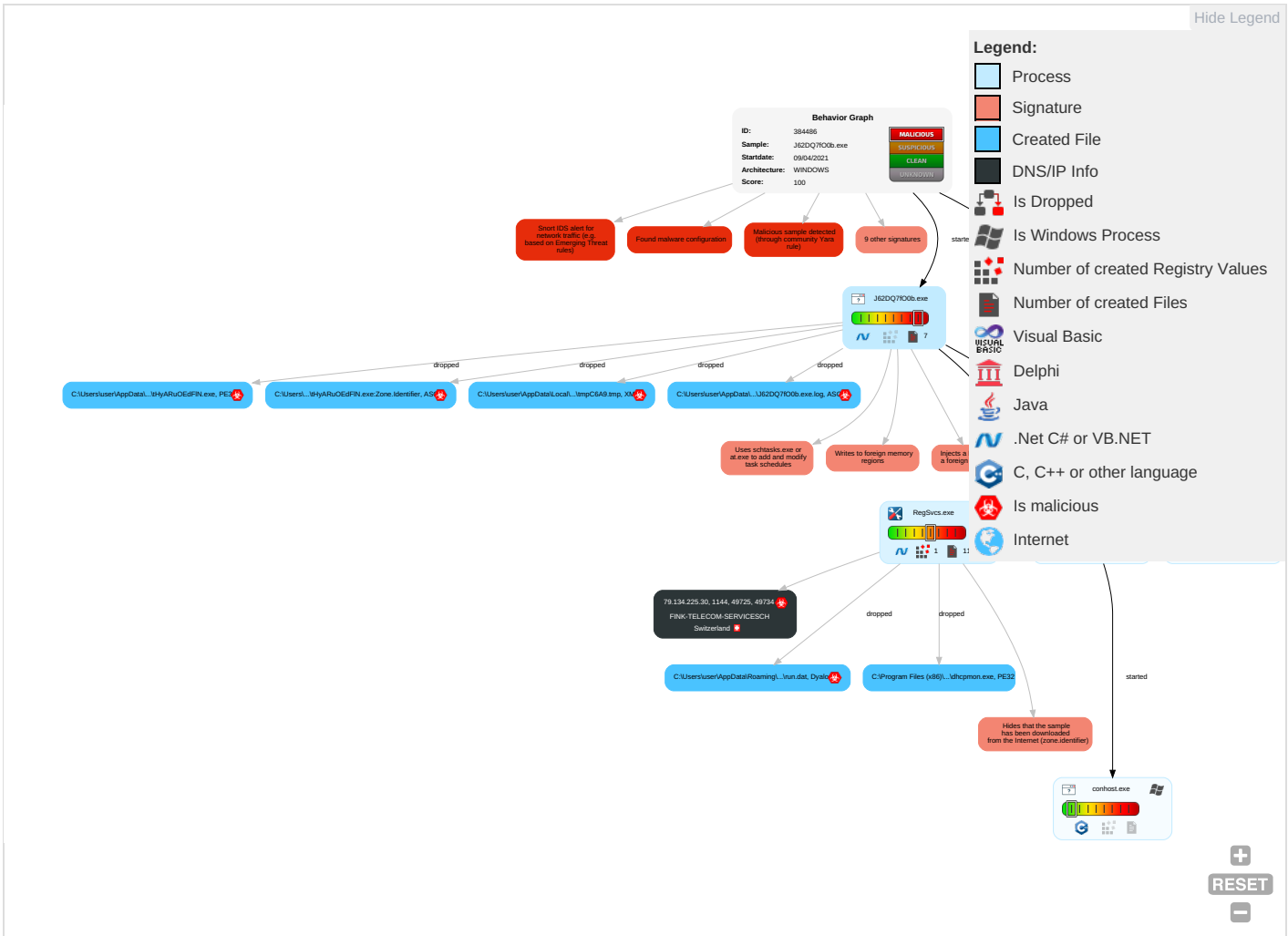
Remote Access Functionality:

- 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	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 2 1 1	Masquerading 2	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesc Insecu Netwo Comm
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit Track I Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2 1 1	NTDS	Virtualization/Sandbox Evasion 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1	DCSync	System Information Discovery 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

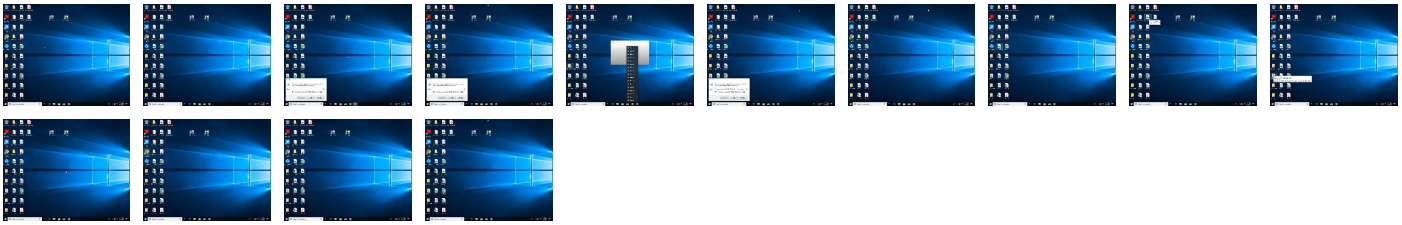
Behavior Graph



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
J62DQ7fO0b.exe	100%	Joe Sandbox ML		

Dropped Files

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

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
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/cnporF	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnbli	0%	Avira URL Cloud	safe	
http://www.carterandcone.comams	0%	Avira URL Cloud	safe	
http://www.carterandcone.comen	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.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnF	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.founder.com.cn/cn/-e	0%	Avira URL Cloud	safe	
http://www.carterandcone.comily	0%	Avira URL Cloud	safe	
http://www.carterandcone.comsofz	0%	Avira URL Cloud	safe	
http://www.carterandcone.comMic&	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/a	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.carterandcone.comext	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.sandoll.co.krF	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.sandoll.co.krpl	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	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.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/cnivZ	0%	Avira URL Cloud	safe	
http://www.carterandcone.comtk	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.sandoll.co.kro.kr-d	0%	Avira URL Cloud	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comCQ	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr_4F	0%	Avira URL Cloud	safe	
79.134.225.30	0%	Avira URL Cloud	safe	
http://www.carterandcone.comhe	0%	Avira URL Cloud	safe	
http://www.goodfont.co.krkrF	0%	Avira URL Cloud	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.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.fontbureau.comt	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.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.founder.com.cn/cnbliQ	0%	Avira URL Cloud	safe	
http://www.monotype.B	0%	Avira URL Cloud	safe	
http://www.monotype.=	0%	Avira URL Cloud	safe	
http://www.carterandcone.comand	0%	Avira URL Cloud	safe	
http://www.carterandcone.comol	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

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

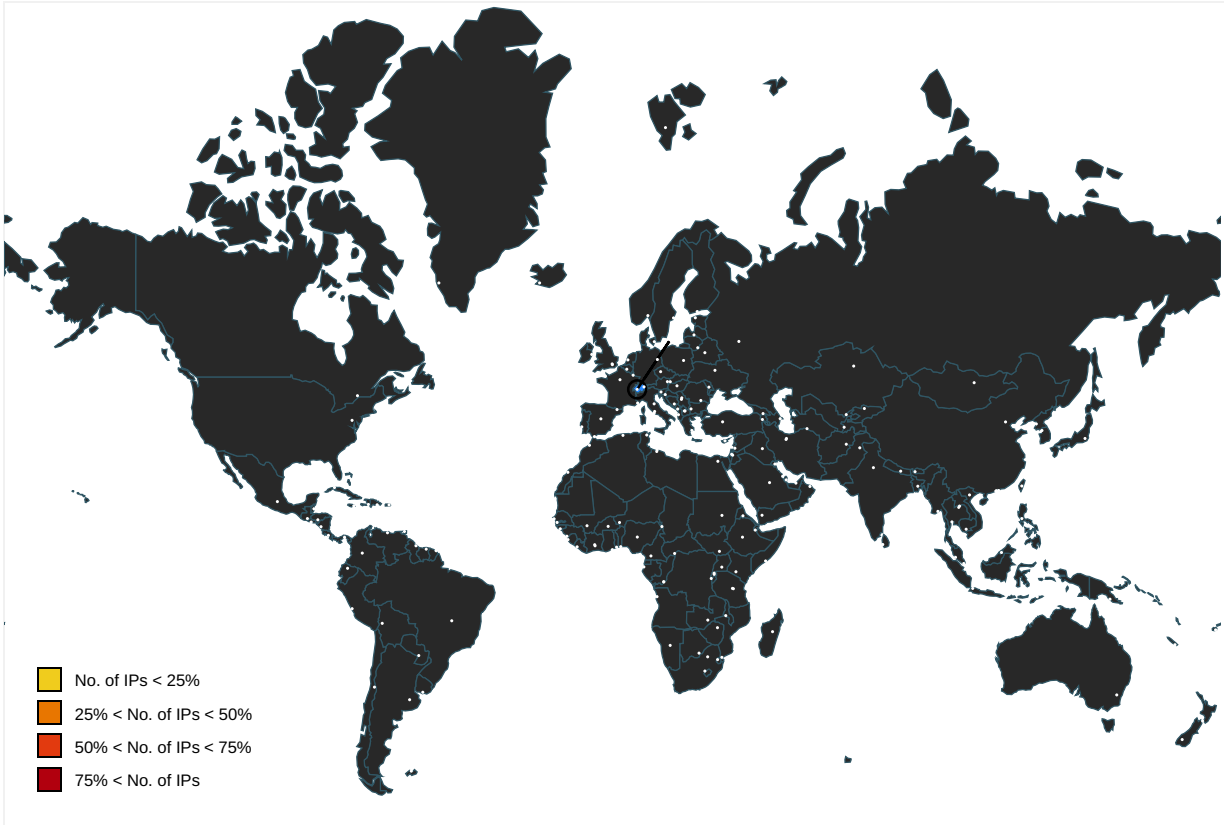
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	J62DQ7fO0b.exe, 00000000.00000002.677595020.0000000005F90000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/?	J62DQ7fO0b.exe, 00000000.00000002.677595020.0000000005F90000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	J62DQ7fO0b.exe, 00000000.00000002.677595020.0000000005F90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnporF	J62DQ7fO0b.exe, 00000000.00000003.641710944.000000000146B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	J62DQ7fO0b.exe, 00000000.00000002.677595020.0000000005F90000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cnbli	J62DQ7fO0b.exe, 00000000.00000003.641650393.0000000005EA9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comams	J62DQ7fO0b.exe, 00000000.00000003.642738927.0000000005EAF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comen	J62DQ7fO0b.exe, 00000000.00000003.642529232.0000000005EA2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name4	J62DQ7fO0b.exe, 00000000.00000002.671216367.0000000002F1A000.00000004.00000001.sdmp	false		high
http://www.tiro.com	J62DQ7fO0b.exe, 00000000.00000002.677595020.0000000005F90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	J62DQ7fO0b.exe, 00000000.00000002.677595020.0000000005F90000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	J62DQ7fO0b.exe, 00000000.00000002.677595020.0000000005F90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	J62DQ7fO0b.exe, 00000000.00000003.642738927.0000000005EAF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnF	J62DQ7fO0b.exe, 00000000.00000003.641650393.0000000005EA9000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http:// https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	J62DQ7fO0b.exe, 00000000.00000002.671018247.0000000002ECB000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.com	J62DQ7fO0b.exe, 00000000.00000002.677595020.0000000005F90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	J62DQ7fO0b.exe, 00000000.00000002.677595020.0000000005F90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	J62DQ7fO0b.exe, 00000000.00000002.677595020.0000000005F90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	J62DQ7fO0b.exe, 00000000.00000002.677595020.0000000005F90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	J62DQ7fO0b.exe, 00000000.00000002.677595020.0000000005F90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/-e	J62DQ7fO0b.exe, 00000000.00000003.641873996.000000000146B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comily	J62DQ7fO0b.exe, 00000000.00000003.642529232.0000000005EA2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comsofz	J62DQ7fO0b.exe, 00000000.00000003.642529232.0000000005EA2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comMic&	J62DQ7fO0b.exe, 00000000.00000003.642738927.0000000005EAF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cn/a	J62DQ7fO0b.exe, 00000000.00000003.641496129.0000000005EA6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	J62DQ7fO0b.exe, 00000000.00000002.677595020.0000000005F90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comext	J62DQ7fO0b.exe, 00000000.00000003.642529232.0000000005EA2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	J62DQ7fO0b.exe, 00000000.00000002.677595020.0000000005F90000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	J62DQ7fO0b.exe, 00000000.00000002.677595020.0000000005F90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krF	J62DQ7fO0b.exe, 00000000.00000003.641496129.0000000005EA6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	J62DQ7fO0b.exe, 00000000.00000002.677595020.0000000005F90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.krpl	J62DQ7fO0b.exe, 00000000.00000003.641496129.0000000005EA6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn	J62DQ7fO0b.exe, 00000000.00000003.642529232.0000000005EA2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	J62DQ7fO0b.exe, 00000000.00000002.670741597.0000000002E71000.00000004.00000001.sdmp, J62DQ7fO0b.exe, 00000000.00000002.671216367.0000000002F1A000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	J62DQ7fO0b.exe, 00000000.00000002.677595020.0000000005F90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnivZ	J62DQ7fO0b.exe, 00000000.00000003.641710944.000000000146B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comtk	J62DQ7fO0b.exe, 00000000.00000003.642529232.0000000005EA2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	J62DQ7fO0b.exe, 00000000.00000003.642142169.000000000146B000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	J62DQ7fO0b.exe, 00000000.00000002.677595020.0000000005F90000.00000002.00000001.sdmp	false		high
http://www.galapagosdesign.com/	J62DQ7fO0b.exe, 00000000.00000003.646392618.0000000005EE5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sandoll.co.kro.kr-d	J62DQ7fO0b.exe, 00000000.00000003.641496129.0000000005EA6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comTC	J62DQ7fO0b.exe, 00000000.00000003.642529232.0000000005EA2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comCQ	J62DQ7fO0b.exe, 00000000.00000003.642529232.0000000005EA2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr_4F	J62DQ7fO0b.exe, 00000000.00000003.641496129.0000000005EA6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.comhe	J62DQ7fO0b.exe, 00000000.00000003.642529232.0000000005EA2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.krkrF	J62DQ7fO0b.exe, 00000000.00000003.641496129.0000000005EA6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	J62DQ7fO0b.exe, 00000000.00000002.677595020.0000000005F90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	J62DQ7fO0b.exe, 00000000.00000003.641998608.0000000005EAC000.00000004.00000001.sdmp, J62DQ7fO0b.exe, 00000000.00000003.641490648.0000000005EDD000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	J62DQ7fO0b.exe, 00000000.00000002.677595020.0000000005F90000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	J62DQ7fO0b.exe, 00000000.00000003.641650393.0000000005EA9000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	J62DQ7fO0b.exe, 00000000.00000002.677595020.0000000005F90000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.monotype.	J62DQ7fO0b.exe, 00000000.00000003.646317309.0000000005EE5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comt	J62DQ7fO0b.exe, 00000000.00000002.669671162.0000000001460000.00000004.00000040.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	J62DQ7fO0b.exe, 00000000.00000002.677595020.0000000005F90000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	J62DQ7fO0b.exe, 00000000.00000002.677595020.0000000005F90000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cnbliQ	J62DQ7fO0b.exe, 00000000.00000003.641627718.0000000005EA6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.monotype.B	J62DQ7fO0b.exe, 00000000.00000003.646942158.0000000005EE5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.monotype.=	J62DQ7fO0b.exe, 00000000.00000003.646271163.0000000005EE5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.comand	J62DQ7fO0b.exe, 00000000.00000003.642529232.0000000005EA2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comol	J62DQ7fO0b.exe, 00000000.00000003.642529232.0000000005EA2000.00000004.00000001.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:	384486
Start date:	09.04.2021
Start time:	10:06:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	J62DQ7fO0b.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:	20
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@8/11@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 89% • 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. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe • 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/384486/sample/J62DQ7fO0b.exe

Simulations

Behavior and APIs

Time	Type	Description
10:07:02	API Interceptor	1x Sleep call for process: J62DQ7fO0b.exe modified
10:07:11	API Interceptor	947x Sleep call for process: RegSvcs.exe modified
10:07:15	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	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	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
	DkZY1k3y9F.exe	Get hash	malicious	Browse	• 79.134.225.23
	hbvo9thTAX.exe	Get hash	malicious	Browse	• 79.134.225.7
	SCAN ORDER DOC 040202021.exe	Get hash	malicious	Browse	• 79.134.225.71
	Waybill Doc_pdf.exe	Get hash	malicious	Browse	• 79.134.225.92
	gfcYixSdyD.exe	Get hash	malicious	Browse	• 79.134.225.71

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	HSBc20210216B1.exe	Get hash	malicious	Browse	
	zunUbtZ2Y3.exe	Get hash	malicious	Browse	
	bank transfer.exe	Get hash	malicious	Browse	
	nunu.exe	Get hash	malicious	Browse	
	quotation.exe	Get hash	malicious	Browse	
	GS_ PO NO.1862021.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	UPDATED SOA.exe	Get hash	malicious	Browse	
	comprobante de pago bancario.exe	Get hash	malicious	Browse	
	ANS_309487487_#049844874.exe	Get hash	malicious	Browse	
	Dekont_12VK2102526 VAKIF KATILIM.exe	Get hash	malicious	Browse	
	taiwan.exe	Get hash	malicious	Browse	
	SWIFT COPY.exe	Get hash	malicious	Browse	
	GS_ PO NO.1862021.exe	Get hash	malicious	Browse	
	purchase order.exe	Get hash	malicious	Browse	
	Payment Advice.exe	Get hash	malicious	Browse	
	Quotation.pdf...exe	Get hash	malicious	Browse	
	PURCHASE ORDER.exe	Get hash	malicious	Browse	
	money.exe	Get hash	malicious	Browse	
	TT COPY.exe	Get hash	malicious	Browse	
	$$$.exe	Get hash	malicious	Browse	

Created / dropped Files

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	768:bBbSoy+SdIBf0k2dsYyV6Iq87PiU9FViaLmf:EoOIBf0ddsYy8LUjVBC
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D(B42
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: HSBc20210216B1.exe, Detection: malicious, Browse • Filename: zunUbtZ2Y3.exe, Detection: malicious, Browse • Filename: bank transfer.exe, Detection: malicious, Browse • Filename: nunu.exe, Detection: malicious, Browse • Filename: quotation.exe, Detection: malicious, Browse • Filename: GS_ PO NO.1862021.exe, Detection: malicious, Browse • Filename: UPDATED SOA.exe, Detection: malicious, Browse • Filename: comprobante de pago bancario.exe, Detection: malicious, Browse • Filename: ANS_309487487_#049844874.exe, Detection: malicious, Browse • Filename: Dekont_12VK2102526 VAKIF KATILIM.exe, Detection: malicious, Browse • Filename: taiwan.exe, Detection: malicious, Browse • Filename: SWIFT COPY.exe, Detection: malicious, Browse • Filename: GS_ PO NO.1862021.exe, Detection: malicious, Browse • Filename: purchase order.exe, Detection: malicious, Browse • Filename: Payment Advice.exe, Detection: malicious, Browse • Filename: Quotation.pdf...exe, Detection: malicious, Browse • Filename: PURCHASE ORDER.exe, Detection: malicious, Browse • Filename: money.exe, Detection: malicious, Browse • Filename: TT COPY.exe, Detection: malicious, Browse • Filename: $$$.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zX.Z.....0..d.....V.... .....@.. .....".. ..`.....O.....8.....r..`>..... ....H.....text...\c... ...d..... ..`.rsrc...8.....f.....@..@.reloc..... .....p.....@..B.....8.....H.....+...S.....\|...P.....r...p(....*2.(....(....*z..r...p(....(....(.....}....*..{....*.s.....*.0..{.....Q.-.s.....+i~....o....(..... s.....o.....r!..p..(....Q.P,:.P.....(....o....o .....(....o!...o".....,..o#...t.....*..0..(..... ....s$.....o%....X..(....-..*.o&...*.0.....('.....&.....*.*.....0.....(.....&.....*..... .....0.....(.....(....~....,(....~....o....9]...

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\J62DQ7fO0b.exe.log

Process:	C:\Users\user\Desktop\J62DQ7fO0b.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\J62DQ7fO0b.exe.log	
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WglAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczlAFXMWTyAGCDLIP12MUAvvw
MD5:	8C0458BB9EA02D50565175E38D577E35
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\tmpC6A9.tmp	
Process:	C:\Users\user\Desktop\J62DQ7fO0b.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.18058135981098
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGRKatn:cbhK79lNQR/rydbz9I3YODOLNdq3EV
MD5:	F97E80A87AE958D4BC07AD23DE478B2A
SHA1:	47F349B089D0861714DF39749A40E92DAE653DA9
SHA-256:	3A01767F80C0386EBB0F5918844F2D1C781C02E3CED00A1B089CF443349AAE72
SHA-512:	A3096C0D7947F1313139EEE2F5CFE82383A6F9C695B90BD2573C84D568FCA2C9D3DBFA032C2CE3FE0995A0AB7B42F3775299846AA97D2809EA390C003FD4891
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\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	1512
Entropy (8bit):	7.012278113302776
Encrypted:	false
SSDEEP:	24:IQnybgCyHJ5lQnybgCyHJ5lQnybgCyHJ5lQnybgCyHJ5lQnybgCyz:IkR5lkR5lkR5lkR5lkR5lkR5i
MD5:	99595ABE9D87E2528BEEAAB442B21B36
SHA1:	340D15872EEA4FB38B0BE5EC0BFF3F251A2BA69E
SHA-256:	4EC04D88C855C45BED9EDF5CF9684B402ACAE3DFB1A0161D9D6371E966B9EE6D

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

SHA-512:	E58CD537D72C7E00376D7595BA8F91A15452E1D3A08E97C74F99D0E5A8201C7039E8C3BDC8ADE74FD9DB7B55C129327C3A160576AA0D2012FCDFF7C938D8C 5
Malicious:	false
Reputation:	low
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h.P.vY.........S.5.6.C4..E.Y.|........).zs...w.gl..\.G..J.M.vES.0....P.:..6...T....+5.1............r.P.V..+..(.*2d.f... ..q.. 7iO.+..c.....!.'.*..mL |XGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h.P.vY.........S.5.6.C4..E.Y.|........).zs...w.gl..\.G..J.M.vES.0....P.:..6...T....+5.1............r.P.V..+..(.*2d.f... ..q.. 7iO.+..c.....!.'.*.. mL|XGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h.P.vY.........S.5.6.C4..E.Y.|........).zs...w.gl..\.G..J.M.vES.0....P.:..6...T....+5.1............r.P.V..+..(.*2d.f... ..q.. 7iO.+..c.....!.'.* ..mL|XGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h.P.vY.........S.5.6.C4..E.Y.|........).zs...w.gl..\.G..J.M.vES.0....P.:..6...T....+5.1............r.P.V..+..(.*2d.f... ..q.. 7iO.+..c.....!.' .*..mL|XGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h.P.vY.........S.5.6.C4..E.Y.|........).zs...w.gl..\.G..J.M.vES.0....P.:..6..

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	Dyalog APL external variable shared version 6.122
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:Hy:S
MD5:	E301BD4595E07EF6742AD3F194ACB0DB
SHA1:	C92A55F687D43CD1BDD5A632F037D1A58D00223B
SHA-256:	2AC8CF690E88B0C0A42129AB9925DBFFA3ABF501A119FE80A6CCFAFEEFED4410
SHA-512:	27DB5F621B7783CA0A043796A03ED91B0AD902EE013BFC5E7C744CFE34D5AD816720376CC87BE10AA70515C6087FEDEF561C7C5770516EEC8817B7DCB37A15 B
Malicious:	**true**
Reputation:	low
Preview:	...z...H

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671 CB
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	9iH...}Z.4..f.~a........~.~.......3.U.

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i......~...|..fX_...Xf.p^......>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i...........J.5b7}..fK..HV..,...0.... ....n.w6PMl.......v."".v.......#..X.a....../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz......(...o......b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O..........Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?............b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.......H...6$. ..d...|m...N..1.R..B.i..........$....$........CY}..$....r.....H...8...li.....7 P......?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. I..&<}....`|.B....3.....l..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\tHyARuOEdFIN.exe	
Process:	C:\Users\user\Desktop\J62DQ7fO0b.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1865728
Entropy (8bit):	7.042310357804828
Encrypted:	false
SSDEEP:	49152:9Ni8vaKvPuXtaD5LNaw/RRMbBRtlxaJvxdrLBF+F36q:Bzv4w/RRMbBRZaJvz3XO35
MD5:	A74ECE32BC1B6DB38A2D379C7FC78D2C
SHA1:	25EA63E67B842641E57BC5B405EA51EC9C6BEB5B
SHA-256:	20E490AFBA639EA251A2F095A8B9B85E1B9922FF6D8B6F47CEB567BA62521A28
SHA-512:	63A026DEDC6B2478A0CA7625534045E98334185BFEA76B7DAA74C1FE8CB32757AB26F97ACE14B8400EA70DF8FDDD0F10DBA51041F2444534A11BF49F4174667
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....o`..... .....@.. ..... ..@.....W.... ..t..... ..... ..H.....text..... ..... ..`.reloc.....@..B.rsrc...t.... .....@..@.....H.....p.....D.....z.{.....}.....(...o!...}....*..*...0.....{.....E.....8...Z...u.....*..}.....].4S}.....}.....*..}... .. ..Q.}.....}.....*..}.....{.... Km.a}.....}.....*..}..... ,...}.....}.....*..}.....{.... ..=.a}.....}.....*..}..... ....}.....}.....*..}..... "G.R}.....}.....*..}.....*...{....*.s"...z.2.{.....f...*....0..<.....{.....3..{....(...o!...3...}.....+..s.....{....}..

C:\Users\user\AppData\Roaming\tHyARuOEdFIN.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\J62DQ7fO0b.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):	1141
Entropy (8bit):	4.44831826838854
Encrypted:	false
SSDEEP:	24:zKLXkb4DObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0b4DQntKKH1MqJC
MD5:	1AEB3A784552CFD2AEDEDC1D43A97A4F
SHA1:	804286AB9F8B3DE053222826A69A7CDA3492411A
SHA-256:	0BC438F4B1208E1390C12D375B6CBB08BF47599D1F24BD07799BB1DF384AA293
SHA-512:	5305059BA86D5C2185E590EC036044B2A17ED9FD9863C2E3C7E7D8035EF0C79E53357AF5AE735F7D432BC70156D4BD3ACB42D100CFB05C2FB669EA22368F141
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..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 Re configure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo S uppress logo output... /quiet Suppress logo output and success output... /c

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.042310357804828

General

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:	J62DQ7fO0b.exe
File size:	1865728
MD5:	a74ece32bc1b6db38a2d379c7fc78d2c
SHA1:	25ea63e67b842641e57bc5b405ea51ec9c6beb5b
SHA256:	20e490afba639ea251a2f095a8b9b85e1b9922ff6d8b6f47ceb567ba62521a28
SHA512:	63a026dedc6b2478a0ca7625534045e98334185bfea76b7daa74c1fe8cb32757ab26f97ace14b8400ea70df8fddd0f10dba51041f2444534a11bf49f41746672
SSDEEP:	49152:9Ni8vaKvPuXtaD5LNaw/RRMbBRtlxaJvxdrLBF+F36q:Bzv4w/RRMbBRZaJvz3XO35
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....o`..... ....@.. ..... @.....

File Icon

Icon Hash:	71f0d4d4ccccf070

Static PE Info

General

Entrypoint:	0x55f0de
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x606FFEAC [Fri Apr 9 07:13:48 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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	0x15f084	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x162000	0x6a074	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x160000	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	0x15d0e4	0x15d200	False	0.644486495256	data	7.5077416615	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0x160000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x162000	0x6a074	0x6a200	False	0.217089038575	data	4.26679146424	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x162220	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x172a48	0x42028	data		
RT_ICON	0x1b4a70	0x25a8	data		
RT_ICON	0x1b7018	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x1bb240	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 16777216, next used block 16777216		

Name	RVA	Size	Type	Language	Country
RT_GROUP_ICON	0x1cba68	0x22	data		
RT_GROUP_ICON	0x1cba8c	0x4c	data		
RT_VERSION	0x1cbad8	0x350	data		
RT_MANIFEST	0x1cbe28	0x249	XML 1.0 document, UTF-8 Unicode (with BOM) text, with very long lines, with no line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Northern Star
Assembly Version	2.1.0.8
InternalName	IBindableIterable.exe
FileVersion	2.1.0.8
CompanyName	Northern Star
LegalTrademarks	
Comments	
ProductName	MDM
ProductVersion	2.1.0.8
FileDescription	MDM
OriginalFilename	IBindableIterable.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/09/21-10:07:12.671031	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49725	1144	192.168.2.4	79.134.225.30
04/09/21-10:07:19.452199	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49734	1144	192.168.2.4	79.134.225.30
04/09/21-10:07:26.421327	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49736	1144	192.168.2.4	79.134.225.30
04/09/21-10:07:33.554381	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49739	1144	192.168.2.4	79.134.225.30
04/09/21-10:07:39.696069	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49740	1144	192.168.2.4	79.134.225.30
04/09/21-10:07:46.643686	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49742	1144	192.168.2.4	79.134.225.30
04/09/21-10:07:52.853588	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	1144	192.168.2.4	79.134.225.30
04/09/21-10:07:59.880822	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49752	1144	192.168.2.4	79.134.225.30
04/09/21-10:08:06.886756	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49756	1144	192.168.2.4	79.134.225.30
04/09/21-10:08:13.696819	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49757	1144	192.168.2.4	79.134.225.30
04/09/21-10:08:19.884335	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49758	1144	192.168.2.4	79.134.225.30
04/09/21-10:08:26.972195	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49761	1144	192.168.2.4	79.134.225.30
04/09/21-10:08:33.851582	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49763	1144	192.168.2.4	79.134.225.30
04/09/21-10:08:39.897169	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49769	1144	192.168.2.4	79.134.225.30
04/09/21-10:08:46.177906	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49770	1144	192.168.2.4	79.134.225.30
04/09/21-10:08:52.997147	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49771	1144	192.168.2.4	79.134.225.30
04/09/21-10:08:59.086454	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49772	1144	192.168.2.4	79.134.225.30

TCP Packets

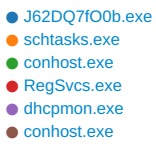
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 10:07:12.412424088 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:12.633583069 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:12.633719921 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:12.671030998 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:12.927891970 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:12.996145010 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:13.081242085 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.134944916 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:13.212373018 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.212693930 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:13.393297911 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.447668076 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:13.453150034 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:13.692616940 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.725742102 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.726242065 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.726407051 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:13.727564096 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.728598118 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.728713036 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:13.729443073 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.736000061 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.736355066 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.736476898 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:13.737448931 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.737550020 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:13.737701893 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.738715887 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.740179062 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:13.929099083 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.929168940 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.929254055 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:13.929281950 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.930774927 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.930814981 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.930840015 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:13.939450026 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.939610004 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:13.940675020 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.941261053 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.941380024 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:13.946429014 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.949985027 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.950076103 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:13.971633911 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.971663952 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.971793890 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:13.972151995 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.972893953 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.972995043 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:13.980684996 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.981470108 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.981534958 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.981574059 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:13.981698036 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.981760979 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:13.981897116 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.990417004 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:13.990533113 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:13.995167971 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:14.123945951 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:14.124001026 CEST	1144	49725	79.134.225.30	192.168.2.4

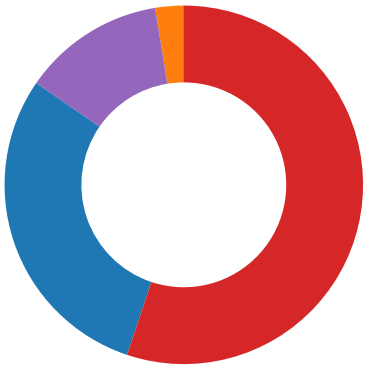
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 10:07:14.124145031 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:14.124556065 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:14.125138998 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:14.134424925 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:14.134581089 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:14.142329931 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:14.142369986 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:14.142514944 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:14.142600060 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:14.142676115 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:14.143532038 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:14.143637896 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:14.143879890 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:14.143968105 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:14.144741058 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:14.144814968 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:14.145612955 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:14.145750999 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:14.145838976 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:14.146193981 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:14.146723986 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:14.146874905 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:14.147619009 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:14.147720098 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:14.148710012 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:14.148770094 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:14.148778915 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:14.148844957 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:14.157772064 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:14.157849073 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:14.158587933 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:14.158675909 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:14.158726931 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:14.158791065 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:14.158813000 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:14.158845901 CEST	1144	49725	79.134.225.30	192.168.2.4
Apr 9, 2021 10:07:14.158888102 CEST	49725	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 10:07:14.180831909 CEST	1144	49725	79.134.225.30	192.168.2.4

Code Manipulations

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: J62DQ7fO0b.exe PID: 6516 Parent PID: 6084

General

Start time:	10:06:54
Start date:	09/04/2021
Path:	C:\Users\user\Desktop\J62DQ7fO0b.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\J62DQ7fO0b.exe'
Imagebase:	0x990000
File size:	1865728 bytes
MD5 hash:	A74ECE32BC1B6DB38A2D379C7FC78D2C
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: 00000000.00000002.671018247.0000000002ECB000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.674143460.0000000003E7C000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.674143460.0000000003E7C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.674143460.0000000003E7C000.00000004.00000001.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	6D38CF06	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	6D38CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\tHyARuOEdFlN.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	6C1DDD66	CopyFileW
C:\Users\user\AppData\Roaming\tHyARuOEdFlN.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C1DDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpC6A9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C1D7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\J62DQ7fO0b.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC6A9.tmp	success or wait	1	6C1D6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\tHyARuOEdFlN.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 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 ac fe 6f 60 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 d2 15 00 00 a4 06 00 00 00 00 00 de f0 15 00 00 20 00 00 00 00 16 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 e0 1c 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.....o`.......... ....@.. ....@................	success or wait	8	6C1DDD66	CopyFileW
C:\Users\user\AppData\Roaming\tHyARuOEdFlN.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	6C1DDD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC6A9.tmp	unknown	1645	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 6a 6f 6e 65 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 6e	<?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>.. </RegistrationIn	success or wait	1	6C1D1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\J62DQ7fO0b.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 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 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D69C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile

Analysis Process: schtasks.exe PID: 6628 Parent PID: 6516

General

Start time:	10:07:07
Start date:	09/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\tHyARuOEdFlN' /XML 'C:\Users\user\AppData\Local\Temp\tmpC6A9.tmp'
Imagebase:	0x8d0000
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\tmpC6A9.tmp	unknown	2	success or wait	1	8DAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpC6A9.tmp	unknown	1646	success or wait	1	8DABD9	ReadFile

Analysis Process: conhost.exe PID: 6636 Parent PID: 6628

General

Start time:	10:07:07
Start date:	09/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6672 Parent PID: 6516

General

Start time:	10:07:08
Start date:	09/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0xa50000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

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	6D38CF06	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	6D38CF06	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	6C1DBEFF	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	6C1D1E60	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	6C1DBEFF	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	6C1DDD66	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	6C1DBEFF	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	6C1DBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	10	6C1D1E60	CreateFileW

<table>
<tr><th>File Path</th><th>Access</th><th>Attributes</th><th>Options</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat</td><td>read attributes | synchronize | generic write</td><td>device</td><td>synchronous io non alert | non directory file | open no recall</td><td>success or wait</td><td>1</td><td>6C1D1E60</td><td>CreateFileW</td></tr>
<tr><td>C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin</td><td>read attributes | synchronize | generic write</td><td>device</td><td>synchronous io non alert | non directory file | open no recall</td><td>success or wait</td><td>1</td><td>6C1D1E60</td><td>CreateFileW</td></tr>
</table>

File Written

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat</td><td>unknown</td><td>8</td><td>aa 06 06 7a 2e fb d8 48</td><td>...z...H</td><td>success or wait</td><td>1</td><td>6C1D1B4F</td><td>WriteFile</td></tr>
<tr><td>C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe</td><td>0</td><td>45152</td><td>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 7a 58 8e 5a 00
00 00 00 00 00 00 00
e0 00 02 01 0b 01 30
00 00 64 00 00 00 0c
00 00 00 00 00 00 56
83 00 00 00 20 00 00
00 a0 00 00 00 00 40
00 00 20 00 00 00 02
00 00 04 00 00 00 00
00 00 00 06 00 00 00
00 00 00 00 00 e0 00
00 00 02 00 00 a9 22
01 00 03 00 60 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</td><td>MZ......................@.....
....
............!..L.!This program
cannot be run in DOS
mode....
$.......PE..L...zX.Z..........
....0..d..........V.... ....@..
....
......."....`................
..............</td><td>success or wait</td><td>1</td><td>6C1DDD66</td><td>CopyFileW</td></tr>
<tr><td>C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat</td><td>unknown</td><td>216</td><td>47 6a 93 68 5c a3 33
c7 ba 41 97 d8 c4 35
b2 78 95 96 26 15 ab
98 69 2b 98 cd 89 63
28 31 a3 50 c6 e5 50
83 63 4c 54 a1 9f c5
82 41 c5 62 c9 e2 1b
95 b8 f0 f0 e7 34 68
a6 50 f4 76 59 a1 02
b3 8b 02 19 e1 11 b5
53 f0 35 8a 36 12 43
34 2e dd 45 b1 59 db
7c f7 f1 8d 15 ba ff 7f
82 16 29 8e 7a 73 0c
a9 ef 77 e2 b4 67 6c
ef e7 5c ec 47 c3 1a
4a 18 4d f2 76 45 53
8c 30 e0 df 9b ff d2
9b 50 f7 3a 82 b9 36
fc f0 01 54 a7 89 a5
c8 2b 35 80 31 a7 c4
19 c1 b3 0c ea a6 a9
b1 9d e7 e0 c5 72 06
50 1d 56 9b 95 2b 91
e6 28 cc 2a 32 64 09
66 87 b6 cf 20 ed ed
ba 9e 71 c3 85 cb 20
37 69 4f ca 2b 81 bb
63 da e6 8b b2 fa cf
09 21 c9 27 ed 2a c7
14 6d 4c 7c 58</td><td>Gj.h\.3..A...5.x..&...i+...c(1
.P..P.cLT....A.b........4h.P.v
Y.........S.5.6.C4..E.Y.|.....
....).zs...w..gl..\.G..J.M.vES
.0......P.:..6...T....+5.1....
..........r.P.V..+..(.*2d.f...
....q... 7iO.+..c.......!.'.*
..mL|X</td><td>success or wait</td><td>7</td><td>6C1D1B4F</td><td>WriteFile</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	327432	70 54 c7 ab ad 21 b0 08 57 f6 fa 47 14 4a ba aa 61 dd a0 29 17 40 c6 8b 69 8b df 77 70 4b 98 73 6f 40 e2 06 e5 35 e7 b7 3d e9 b8 90 5e ab 1d 51 82 6f 79 f9 3d 65 40 39 c3 42 8d f7 95 46 bc cb 30 39 75 22 33 8b f5 20 30 74 c0 19 52 44 6e 5f 34 64 fb b8 17 02 df 45 c0 90 06 69 f4 08 9f ae bb 8a 7e 0c 89 85 7c 87 eb 66 58 5f 0e c2 ed 58 66 88 70 5e e2 f5 ff 94 03 e5 3e 61 db 8b 91 24 8d 8a 8f 65 05 36 3a 37 64 b6 28 61 05 41 e4 fe e0 3d be 29 2a 0d 96 a8 90 8e 7b 42 1c 5b ab 87 cb 79 25 b3 2a e4 b8 b1 9f 69 a7 51 84 3c f3 94 a2 90 78 74 c4 a9 58 13 11 48 09 d7 20 ad cc a4 48 46 37 67 0f e0 c5 49 96 2a 33 03 7b 0c 6e 92 bf 90 be 4c d1 9b 79 3b 69 87 bc 73 2d 1e b6 f9 b8 28 35 69 c2 8b 92 d6 10 ac a7 02 93 ee 89 08 17 4a 09 35 62 37 7d fe 86 66 4b af ab 48 56	pT...!..W..G.J..a..).@..i..wpK .so@...5..=...^..Q.oy.=e@9 .B...F..09u"3.. 0t..RDn_4d.....E.. .i.....~...|..fX_...Xf.p^.... ..>a...$...e.6:7d.(a.A...=.)*. ....{B.[...y%.*....i.Q.<....xt ..X..H.. ...HF7g...l.*3.{.n... .L..y;i..s-....(5i..... .J.5b7}..fK..HV	success or wait	1	6C1D1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 7e 61 d3 f8 a3 01 06 96 0c a9 7e ba 7e 86 90 d9 e5 05 8d ca 33 e7 55 0b	9iH....}Z..4..f.~a.....~.~. .....3.U.	success or wait	1	6C1D1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D36CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6C1D1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D34D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D34D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe	unknown	4096	success or wait	1	6D34D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe	unknown	512	success or wait	1	6D34D72F	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6D365705	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	6C1D646A	RegSetValueExW

Analysis Process: dhcpmon.exe PID: 7068 Parent PID: 3424

General

Start time:	10:07:23
Start date:	09/04/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x8c0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D69C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	6C1D1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	141	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 34 2e 37 2e 33 30 35 36 2e 30 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 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 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....	success or wait	1	6C1D1B4F	WriteFile
\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	6C1D1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\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 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 interfaces... /appdir:<path> Set application root directory to specified path.....	success or wait	1	6C1D1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	unknown	142	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 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 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..	success or wait	1	6D69C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D365705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D365705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D36CA54	ReadFile

Analysis Process: conhost.exe PID: 7092 Parent PID: 7068

General

Start time:	10:07:24
Start date:	09/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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