ID: 384479
Sample Name:
oE6O5K1emC.exe
Cookbook: default.jbs
Time: 09:46:16
Date: 09/04/2021
Version: 31.0.0 Emerald

Table of Contents

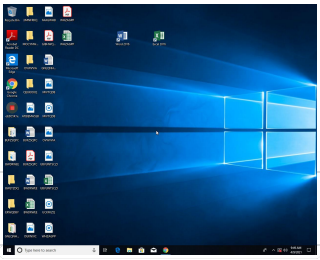
Analysis Report oE6O5K1emC.exe

Overview

General Information

Sample Name:	oE6O5K1emC.exe
Analysis ID:	384479
MD5:	0cf0cd25346ee69..
SHA1:	ca13e5bbc69f2d8..
SHA256:	f542bc0175168da.
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

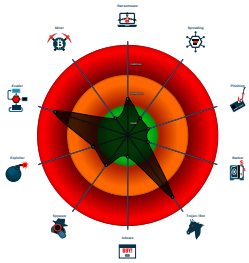
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- 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…

Classification



Startup

- **System is w10x64**
- oE6O5K1emC.exe (PID: 6360 cmdline: 'C:\Users\user\Desktop\oE6O5K1emC.exe' MD5: 0CF0CD25346EE69B7E5AA8E366C886E9)
  - schtasks.exe (PID: 6456 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\DKCbURUccsVSl' /XML 'C:\Users\user\AppData\Local\Temp\tmp8EBC.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6464 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 6500 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe MD5: 71369277D09DA0830C8C59F9E22BB23A)
- dhcpmon.exe (PID: 7024 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 7032 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
00000000.00000002.676048550.000000000363F000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.676767398.00000000046CA000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xa85fd:$x1: NanoCore.ClientPluginHost • 0xdae1d:$x1: NanoCore.ClientPluginHost • 0xa863a:$x2: IClientNetworkHost • 0xdae5a:$x2: IClientNetworkHost • 0xac16d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0xde98d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.676767398.00000000046CA000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.676767398.00000000046CA000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xa8365:$a: NanoCore • 0xa8375:$a: NanoCore • 0xa85a9:$a: NanoCore • 0xa85bd:$a: NanoCore • 0xa85fd:$a: NanoCore • 0xdab85:$a: NanoCore • 0xdab95:$a: NanoCore • 0xdadc9:$a: NanoCore • 0xdaddd:$a: NanoCore • 0xdae1d:$a: NanoCore • 0xa83c4:$b: ClientPlugin • 0xa85c6:$b: ClientPlugin • 0xa8606:$b: ClientPlugin • 0xdabe4:$b: ClientPlugin • 0xdade6:$b: ClientPlugin • 0xdae26:$b: ClientPlugin • 0xa84eb:$c: ProjectData • 0xdad0b:$c: ProjectData • 0xa8ef2:$d: DESCrypto • 0xdb712:$d: DESCrypto • 0xb08be:$e: KeepAlive
Process Memory Space: oE6O5K1emC.exe PID: 6360	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
3.3.RegSvcs.exe.3d02987.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x41ee:$x1: NanoCore.ClientPluginHost • 0x422b:$x2: IClientNetworkHost

Source	Rule	Description	Author	Strings
3.3.RegSvcs.exe.3d02987.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x41ee:$x2: NanoCore.ClientPluginHost • 0x7641:$s4: PipeCreated • 0x4218:$s5: IClientLoggingHost
0.2.oE6O5K1emC.exe.4762470.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.oE6O5K1emC.exe.4762470.1.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
0.2.oE6O5K1emC.exe.4762470.1.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 6 entries				

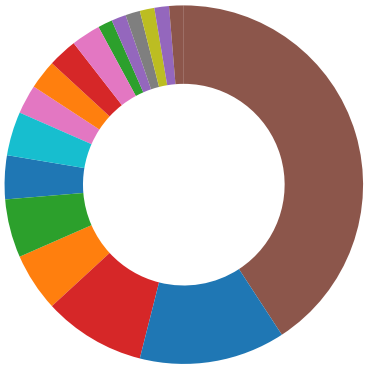
Sigma Overview

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

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

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

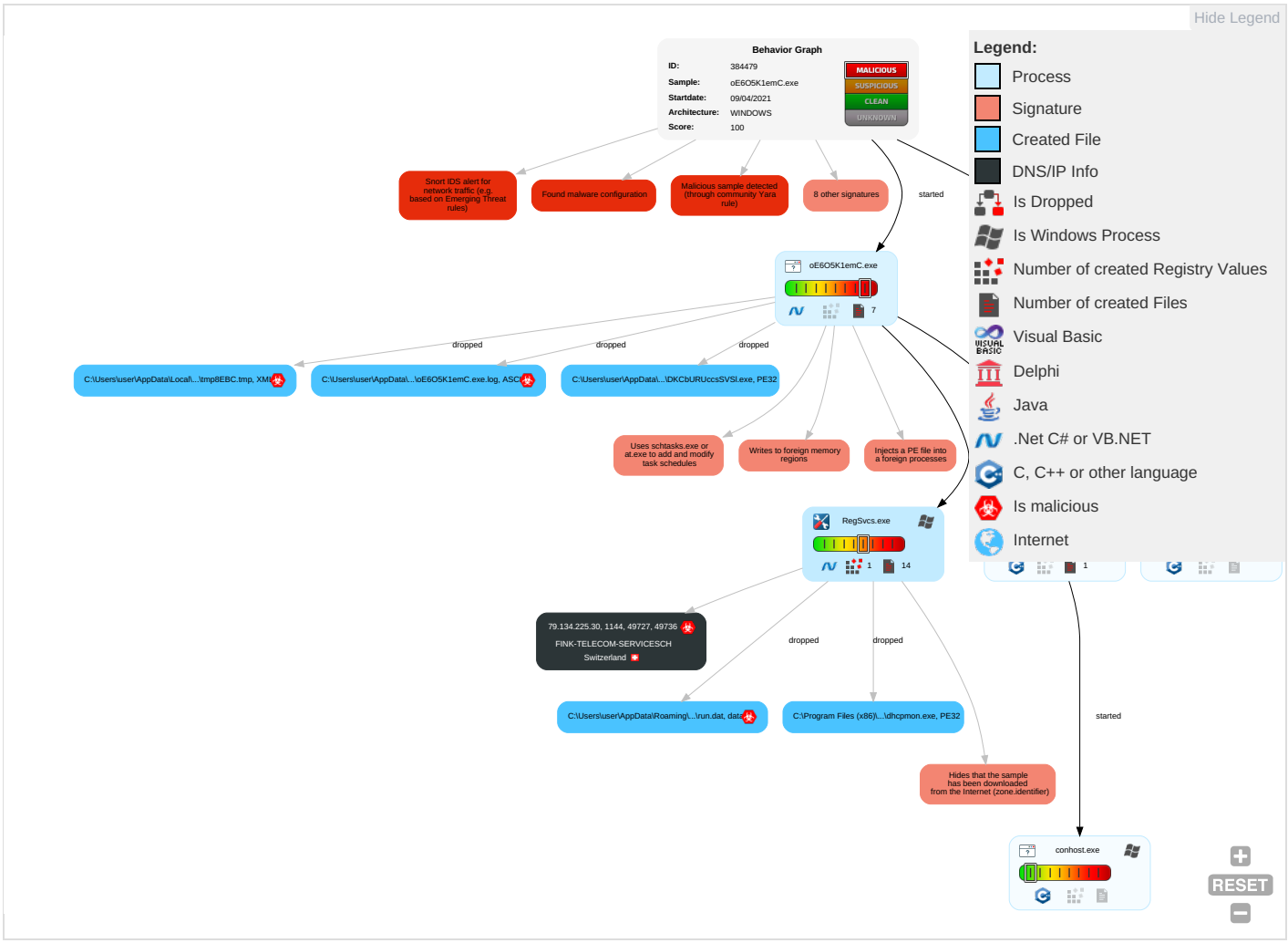
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Access Token Manipulation 1	Masquerading 2	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Comr
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Process Injection 2 1 2	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	Explo Redir Calls/
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Explo Track Locat
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Virtualization/Sandbox Evasion 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1	SIM (Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 2 1 2	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamn Denia Servi

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	System Information Discovery 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dowr Insec Proto

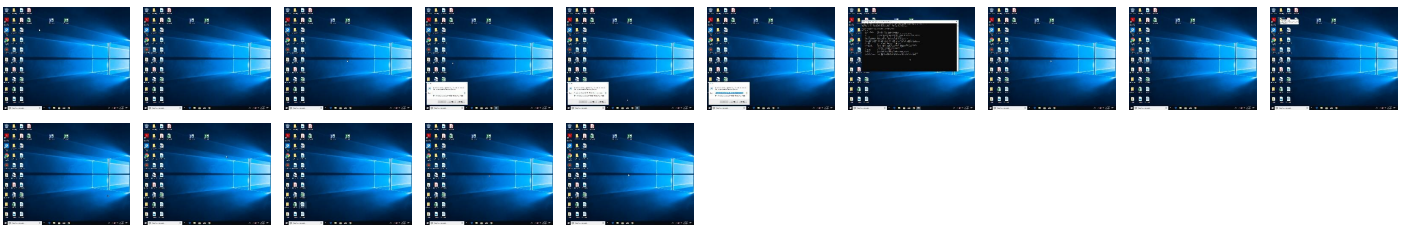
Behavior Graph



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
oE6O5K1emC.exe	13%	Virustotal		Browse

Dropped Files

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

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.carterandcone.comTCe	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
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/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.comypoD	0%	Avira URL Cloud	safe	
http://www.fonts.com)	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.carterandcone.comTCH	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.carterandcone.comTCD	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comM.TTFK	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/g	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.tiro.comtna	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.fonts.comx	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cni	0%	Avira URL Cloud	safe	
http://www.fontbureau.comasa	0%	Avira URL Cloud	safe	
http://www.carterandcone.comexcR	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.carterandcone.comd	0%	URL Reputation	safe	
http://www.carterandcone.comd	0%	URL Reputation	safe	
http://www.carterandcone.comd	0%	URL Reputation	safe	
http://www.carterandcone.comgy	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	

Source	Detection	Scanner	Label	Link
http://www.carterandcone.comX	0%	Avira URL Cloud	safe	
http://www.founder.com.c	0%	URL Reputation	safe	
http://www.founder.com.c	0%	URL Reputation	safe	
http://www.founder.com.c	0%	URL Reputation	safe	
http://www.galapagosdesign.com/C	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kre	0%	Avira URL Cloud	safe	
79.134.225.30	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.urwpp.dew	0%	Avira URL Cloud	safe	
http://www.fontbureau.comionm	0%	Avira URL Cloud	safe	
http://www.carterandcone.comnew=	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cne-d	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.fontbureau.comFg	0%	Avira URL Cloud	safe	
http://en.w7	0%	Avira URL Cloud	safe	
http://www.fontbureau.comsiefeq	0%	Avira URL Cloud	safe	
http://www.carterandcone.comTCoo	0%	Avira URL Cloud	safe	
http://www.fonts.com-u	0%	Avira URL Cloud	safe	
http://www.fontbureau.com~	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

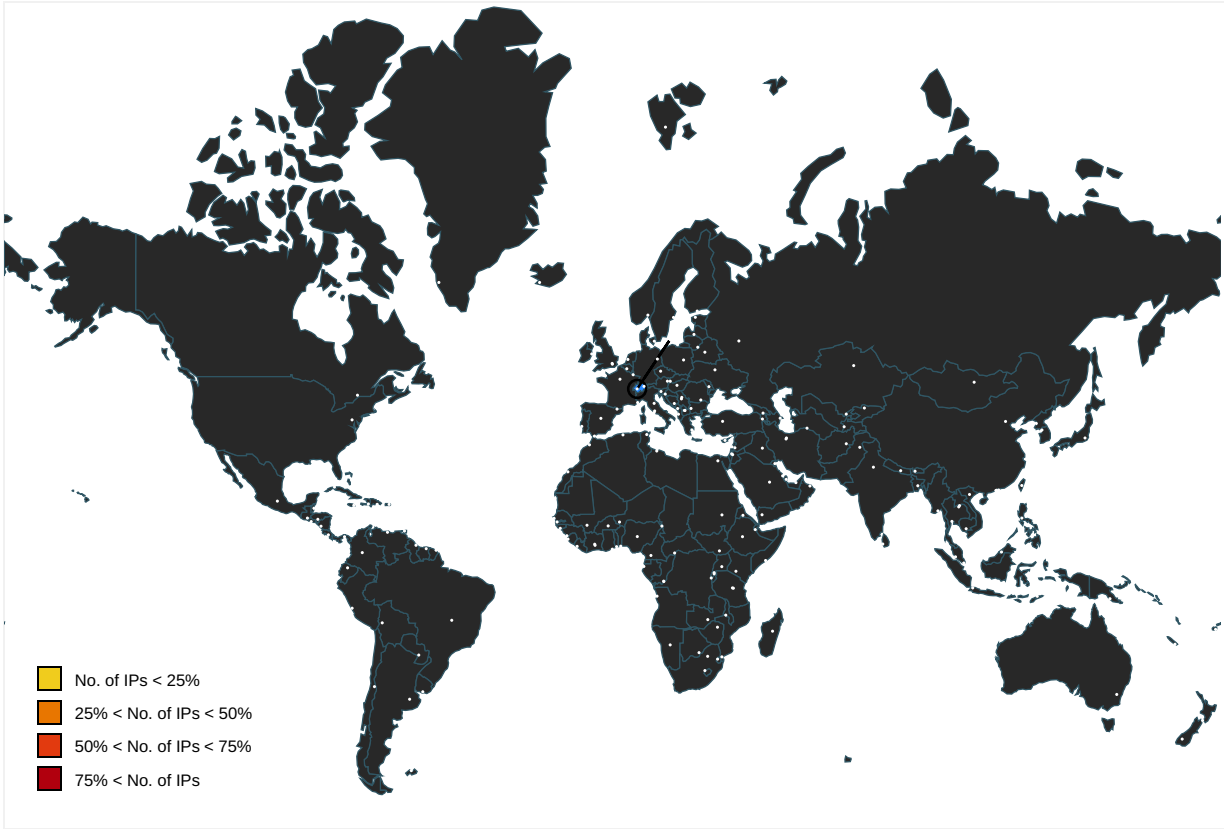
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	oE6O5K1emC.exe, 00000000.00000002.680503330.0000000006BD2000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comTCe	oE6O5K1emC.exe, 00000000.00000003.651855574.00000000059FE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	oE6O5K1emC.exe, 00000000.00000002.680503330.0000000006BD2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	oE6O5K1emC.exe, 00000000.00000002.680503330.0000000006BD2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comypoD	oE6O5K1emC.exe, 00000000.00000003.651652317.00000000059FE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersJ	oE6O5K1emC.exe, 00000000.00000003.654970747.00000000059F5000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	oE6O5K1emC.exe, 00000000.00000002.680503330.0000000006BD2000.00000004.00000001.sdmp, oE6O5K1emC.exe, 00000000.00000003.655396524.00000000059F5000.00000004.00000001.sdmp	false		high
http://www.fonts.com)	oE6O5K1emC.exe, 00000000.00000003.649295268.00000000059DB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designers/frere-user.html/	oE6O5K1emC.exe, 00000000.00000003.654947203.00000000059F5000.00000004.00000001.sdmp	false		high
http://www.tiro.com	oE6O5K1emC.exe, 00000000.00000002.680503330.0000000006BD2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	oE6O5K1emC.exe, 00000000.00000003.659379671.00000000059F5000.00000004.00000001.sdmp, oE6O5K1emC.exe, 00000000.00000003.654702563.00000000059F5000.00000004.00000001.sdmp, oE6O5K1emC.exe, 00000000.00000003.654666209.00000000059F5000.00000004.00000001.sdmp, oE6O5K1emC.exe, 00000000.00000003.655363826.00000000059F5000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	oE6O5K1emC.exe, 00000000.00000002.680503330.0000000006BD2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	oE6O5K1emC.exe, 00000000.00000003.651544478.00000000059FE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comTCH	oE6O5K1emC.exe, 00000000.00000003.652006523.00000000059FE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	oE6O5K1emC.exe, 00000000.00000002.676048550.000000000363F000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.com	oE6O5K1emC.exe, 00000000.00000003.649181303.00000000059DB000.00000004.00000001.sdmp, oE6O5K1emC.exe, 00000000.00000002.680503330.0000000006BD2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	oE6O5K1emC.exe, 00000000.00000002.680503330.0000000006BD2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	oE6O5K1emC.exe, 00000000.00000002.680503330.0000000006BD2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	oE6O5K1emC.exe, 00000000.00000002.680503330.0000000006BD2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	oE6O5K1emC.exe, 00000000.00000002.680503330.0000000006BD2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comTCD	oE6O5K1emC.exe, 00000000.00000003.651855574.00000000059FE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	oE6O5K1emC.exe, 00000000.00000002.680503330.0000000006BD2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comM.TTFK	oE6O5K1emC.exe, 00000000.00000003.655776932.00000000059C4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	oE6O5K1emC.exe, 00000000.00000002.680503330.0000000006BD2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/g	oE6O5K1emC.exe, 00000000.00000003.651132859.00000000059C4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kr	oE6O5K1emC.exe, 00000000.00000002.680503330.0000000006BD2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.comtna	oE6O5K1emC.exe, 00000000.00000003.649513321.00000000059DB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	oE6O5K1emC.exe, 00000000.00000002.680503330.0000000006BD2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	oE6O5K1emC.exe, 00000000.00000002.680503330.0000000006BD2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	oE6O5K1emC.exe, 00000000.00000002.680503330.0000000006BD2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comx	oE6O5K1emC.exe, 00000000.00000003.649273531.00000000059DB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cni	oE6O5K1emC.exe, 00000000.00000003.651132859.00000000059C4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersn	oE6O5K1emC.exe, 00000000.00000003.655634998.00000000059F5000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comasa	oE6O5K1emC.exe, 00000000.00000003.655776932.00000000059C4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designerss	oE6O5K1emC.exe, 00000000.00000003.655634998.00000000059F5000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	oE6O5K1emC.exe, 00000000.00000002.680503330.0000000006BD2000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comexcR	oE6O5K1emC.exe, 00000000.00000003.651855574.00000000059FE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com	oE6O5K1emC.exe, 00000000.00000002.680503330.0000000006BD2000.00000004.00000001.sdmp, oE6O5K1emC.exe, 00000000.00000003.655776932.00000000059C4000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/	oE6O5K1emC.exe, 00000000.00000003.656920941.00000000059CD000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comd	oE6O5K1emC.exe, 00000000.00000003.651855574.00000000059FE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comgy	oE6O5K1emC.exe, 00000000.00000003.651544478.00000000059FE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comTC	oE6O5K1emC.exe, 00000000.00000003.651855574.00000000059FE000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comX	oE6O5K1emC.exe, 00000000.00000003.651855574.00000000059FE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.c	oE6O5K1emC.exe, 00000000.00000003.650828055.00000000059C4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/C	oE6O5K1emC.exe, 00000000.00000003.656920941.00000000059CD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kre	oE6O5K1emC.exe, 00000000.00000003.650167999.00000000059C6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comX	oE6O5K1emC.exe, 00000000.00000003.649256448.00000000059DB000.00000004.00000001.sdmp	false		unknown
http://www.carterandcone.coml	oE6O5K1emC.exe, 00000000.00000002.680503330.0000000006BD2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	oE6O5K1emC.exe, 00000000.00000003.651132859.00000000059C4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	oE6O5K1emC.exe, 00000000.00000002.680503330.0000000006BD2000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn	oE6O5K1emC.exe, 00000000.00000002.680503330.0000000006BD2000.00000004.00000001.sdmp, oE6O5K1emC.exe, 00000000.00000003.650806583.00000000059FD000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.dew	oE6O5K1emC.exe, 00000000.00000003.655776932.00000000059C4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	oE6O5K1emC.exe, 00000000.00000002.680503330.0000000006BD2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comionm	oE6O5K1emC.exe, 00000000.00000003.673968990.00000000059C0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comnew=	oE6O5K1emC.exe, 00000000.00000003.651855574.00000000059FE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cne-d	oE6O5K1emC.exe, 00000000.00000003.650806583.00000000059FD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	oE6O5K1emC.exe, 00000000.00000002.680503330.0000000006BD2000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comFg	oE6O5K1emC.exe, 00000000.00000003.655776932.00000000059C4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://en.w7	oE6O5K1emC.exe, 00000000.00000003.649181303.00000000059DB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	oE6O5K1emC.exe, 00000000.00000002.680503330.0000000006BD2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comsiefeq	oE6O5K1emC.exe, 00000000.00000003.655776932.00000000059C4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comTCoo	oE6O5K1emC.exe, 00000000.00000003.652274217.00000000059FE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/	oE6O5K1emC.exe, 00000000.00000003.654419205.00000000059F5000.00000004.00000001.sdmp	false		high
http://www.fonts.com-u	oE6O5K1emC.exe, 00000000.00000003.649256448.00000000059DB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com~	oE6O5K1emC.exe, 00000000.00000003.655776932.00000000059C4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

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:	384479
Start date:	09.04.2021
Start time:	09:46:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	oE6O5K1emC.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:	23
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@8/12@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.3% (good quality ratio 1.8%) • Quality average: 51.1% • Quality standard deviation: 33.7%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	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.

Simulations

Behavior and APIs

Time	Type	Description
09:47:11	API Interceptor	1x Sleep call for process: oE6O5K1emC.exe modified
09:47:18	API Interceptor	936x Sleep call for process: RegSvcs.exe modified
09:47:20	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	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	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
	yBio5dWAOI.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
	cJtVGjtNGZ.exe	Get hash	malicious	Browse	• 79.134.225.40

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	GS_ PO NO.1862021.exe	Get hash	malicious	Browse	
	wDIaJji4Vv.exe	Get hash	malicious	Browse	
	cJtVGjtNGZ.exe	Get hash	malicious	Browse	
	Bilansno placanje.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Inject4.9647.20479.exe	Get hash	malicious	Browse	
	wnIPBdB5OF.exe	Get hash	malicious	Browse	
	Delivery Form C.exe	Get hash	malicious	Browse	
	h6uc8EaDQX.exe	Get hash	malicious	Browse	
	3aDHivUqWtumbXb.exe	Get hash	malicious	Browse	
	fMy120EQiT6NaRd.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Bulz.394792.29952.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.578.18498.exe	Get hash	malicious	Browse	
	sfTZCyMKuC.exe	Get hash	malicious	Browse	
	y9Rtu1cnBk.exe	Get hash	malicious	Browse	
	lxli7b5j6A.exe	Get hash	malicious	Browse	
	nq0aCrCXyE.exe	Get hash	malicious	Browse	
	73SriHObnQ.exe	Get hash	malicious	Browse	
	0672IMP000158021.pdf.exe	Get hash	malicious	Browse	
	rb86llCYzA.exe	Get hash	malicious	Browse	
	C3GWn5tduT.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	3.7515815714465193
Encrypted:	false
SSDEEP:	384:BOj9Y8/gS7SDriLGKq1MHR5U4Ag6ihJSxUCR1rgCPKabK2t0X5P7DZ+JgWSW72uw:B+gSAdN1MH3HAFRJngW2u
MD5:	71369277D09DA0830C8C59F9E22BB23A
SHA1:	37F9781314F0F6B7E9CB529A573F2B1C8DE9E93F
SHA-256:	D4527B7AD2FC4778CC5BE8709C95AEA44EAC0568B367EE14F7357D72898C3698
SHA-512:	2F470383E3C796C4CF212EC280854DBB9E7E8C8010CE6857E58F8E7066D7516B7CD7039BC5C0F547E1F5C7F9F2287869ADFFB2869800B08B2982A88BE96E9FB
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: GS_ PO NO.1862021.exe, Detection: malicious, Browse • Filename: wDIaJji4Vv.exe, Detection: malicious, Browse • Filename: cJtVGjtNGZ.exe, Detection: malicious, Browse • Filename: Bilansno placanje.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.Inject4.9647.20479.exe, Detection: malicious, Browse • Filename: wnIPBdB5OF.exe, Detection: malicious, Browse • Filename: Delivery Form C.exe, Detection: malicious, Browse • Filename: h6uc8EaDQX.exe, Detection: malicious, Browse • Filename: 3aDHivUqWtumbXb.exe, Detection: malicious, Browse • Filename: fMy120EQiT6NaRd.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Variant.Bulz.394792.29952.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.PackedNET.578.18498.exe, Detection: malicious, Browse • Filename: sfTZCyMKuC.exe, Detection: malicious, Browse • Filename: y9Rtu1cnBk.exe, Detection: malicious, Browse • Filename: lxli7b5j6A.exe, Detection: malicious, Browse • Filename: nq0aCrCXyE.exe, Detection: malicious, Browse • Filename: 73SriHObnQ.exe, Detection: malicious, Browse • Filename: 0672IMP000158021.pdf.exe, Detection: malicious, Browse • Filename: rb86llCYzA.exe, Detection: malicious, Browse • Filename: C3GWn5tduT.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\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\Microsoft\CLR_v2.0_32\UsageLogs\oE6O5K1emC.exe.log	
Process:	C:\Users\user\Desktop\oE6O5K1emC.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	664
Entropy (8bit):	5.288448637977022
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk70U2xANlW3ANv:MLF20NaL3z2p29hJ5g522rW2xAi3A9
MD5:	B1DB55991C3DA14E35249AEA1BC357CA
SHA1:	0DD2D91198FDEF296441B12F1A906669B279700C
SHA-256:	34D3E48321D5010AD2BD1F3F0B728077E4F5A7F70D66FA36B57E5209580B6BDC
SHA-512:	BE38A31888C9C2F8047FA9C99672CB985179D325107514B7500DDA9523AE3E1D20B45EACC4E6C8A5D096360D0FBB98A120E63F38FFE324DF8A0559F6890CC80
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.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\Temp\tmp8EBC.tmp	
Process:	C:\Users\user\Desktop\oE6O5K1emC.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1647
Entropy (8bit):	5.185753707490085
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBG6kbBtn:cbhK79lNQR/rydbz9I3YODOLNdq3Vkn
MD5:	8691364F6187303B5A987AB904210902
SHA1:	23A74D45BD4BD827501964713B23CBF891EFD72E
SHA-256:	43D8999891D99A3D4406474CC11A627A59E769993069DE5E4240CCD5C9862841
SHA-512:	9EA6FA83631DC1618B820EF9762C65128F5E148B2969165F1C39A0A590B0195EEB5F13D399BA09CDD9DCA1F8F0E30D361839F78350EF50555BA02F16D5142E3B
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\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	7.012278113302776
Encrypted:	false
SSDEEP:	24:IQnybgCyHJ5lQnybgCyHJ5lQnybgCyHJ5lQnybgCyHJ5lQnybgCy6:IkR5lkR5lkR5lkR5lkR5lkR5i

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
MD5:	383833878D639AB9D3EE3ADF842AC47F
SHA1:	E873365BC70A3B3F0E4B2156478B5FC45FAA8098
SHA-256:	DA0C5534BB335E6BDFFA15200AC4ED932500D425999D1200C855A48FF4483FB0
SHA-512:	22117398C7BD9D74CBF8EF5B3CB3D259806A5B363DB85C3990B31EE51B647C7BD0E4F95FFBC5AAD060520E910FCB43817E56DEADA96781A8DF15B1EEA573DA 9F
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\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Q9tn:Q9t
MD5:	8BACB37884A4AF96860567FB19A77E4C
SHA1:	BBBE9A196EDA91481E15FC68C5AE337DED70E0A9
SHA-256:	4391234F02BA7E0982E043C27997CD7046186ECC7329E798C3582657E5EF55AF
SHA-512:	C51F23901A481F26B8AB5B85366E7899F76A15EFD1DB98B04CD68E2E1F38C9FAF325D2B91BB38C67B9C65F4853BAF91AC7AFED231FEED71AA5072EC7F87225(C
Malicious:	**true**
Preview:	*/..+..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	4.501629167387823
Encrypted:	false
SSDEEP:	3:9bzY6oRDIvYk:RzWDI3
MD5:	ACD3FB4310417DC77FE06F15B0E353E6
SHA1:	80E7002E655EB5765FDEB21114295CB96AD9D5EB
SHA-256:	DC3AE604991C9BB8FF8BC4502AE3D0DB8A3317512C0F432490B103B89C1A4368
SHA-512:	DA46A917DB6276CD4528CFE4AD113292D873CA2EBE53414730F442B83502E5FAF3D1AE87BFA295ADF01E3B44FDBCE239E21A318BFB2CCD1F4753846CB21F6F 97
Malicious:	false
Preview:	9iH...}Z.4..f..J".C;"a

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	5.320159765557392
Encrypted:	false
SSDEEP:	3:9bzY6oRDIvYVsRLY6oRDT6P2bfVn1:RzWDIfRWDT621
MD5:	BB0F9B9992809E733EFFF8B0E562CFD6
SHA1:	F0BAB3CF73A04F5A689E6AFC764FEE9276992742
SHA-256:	C48F04FE7525AA3A3F9540889883F649726233DE021724823720A59B4F37CEAC
SHA-512:	AE4280AA460DC1C0301D458A3A443F6884A0BE37481737B2ADAFD72C33C55F09BED88ED239C91FE6F19CA137AC3CD7C9B8454C21D3F8E759687F701C8B3C7A 6
Malicious:	false
Preview:	9iH...}Z.4..f..J".C;"a9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	data

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Category:	dropped
Size (bytes):	426840
Entropy (8bit):	**7.999608491116724**
Encrypted:	**true**
SSDEEP:	12288:zKf137EiDsTjevgA4p0V7njXuWSvdVU7V4OC0Rr:+134i2lp67i5d8+OCg
MD5:	963D5E2C9C0008DFF05518B47C367A7F
SHA1:	C183D601FABBC9AC8FBFA0A0937DECC677535E74
SHA-256:	5EACF2974C9BB2C2E24CDC651C4840DD6F4B76A98F0E85E90279F1DBB2E6F3C0
SHA-512:	0C04E1C1A13070D48728D9F7F300D9B26DEC6EC8875D8D3017EAD52B9EE5BDF9B651A7F0FCC537761212831107646ED72B8ED017E7477E600BC0137EF857AE2
Malicious:	false
Preview:	..g&jo...IPg...GM....R>i...o...I.>.&.r{....8...}...E....v.!7.u3e.. .....db...}.....".t(.xC9.cp.B....7...'.....%.....w.^.._.....B.W%.<..i.0.{9.xS...5...)..w..$..C..?`F..u.5.T.X.w'Si..z.n{...Y!m. ..RA...xg....[7...z..9@.K.-...T..+.ACe....R....enO.....AoNMT.\^....}H&..4I...B.:..@..J...v..rI5..kP.....2j....B..B.~.T..>.c..emW;Rn<9..[.r.o....R[....@=...:...L.g<.....I..%4[.G^.~.I'.....v .p&.....+..S...9d/.{..H.`@.1.....f.\s...X.a.].<.h*...J4*...k.x....%3.....3.c..?%....>.!.}..)(.{...H...3..`].Q.[sN..JX(.%pH....+.....(...v.....H...3..8.a_..J..?4...y.N(..D.*h..g.jD..I...44 Q?..N.....oX.A.....I...n?./.....$.!.;.^9"H.....*...OkF....v.m_.e.v..f...".bq{.....O.-....%R+...-..P.i..t5....2Z# ...#...,L..{..j..heT -=Z.P;...g.m)<owJ].J..../.p..8.u8.&..#.m9...j%..g&... .g.x.I,....u.[....>./W.....*X...b*Z...ex.0..x.}.....Tb...[..H_M._.^N.d&...g._."@4N.pDs].GbT.....&p.....Nw...%$=....{..J.1....2....<E{..<!G..

C:\Users\user\AppData\Roaming\DKCbURUccsSVSl.exe	
Process:	C:\Users\user\Desktop\oE6O5K1emC.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1554944
Entropy (8bit):	7.385331204380147
Encrypted:	false
SSDEEP:	24576:8ZHdBedlcA8hbbgPFbg3TwSxivyHOcq5pCkQha6g53oG4l2GfONmPr:uBedlv8hbbgPFbhGYDHJ6g545lpfi8
MD5:	0CF0CD25346EE69B7E5AA8E366C886E9
SHA1:	CA13E5BBC69F2D808139EE18EA5AD56579F8B003
SHA-256:	F542BC0175168DAA808CE1448A019F88B058DF6D0702C6DAA4A0F83A481F2A5E
SHA-512:	03DFE9E8D76C37AB36CFF64E569F22861C10BAADAFEDA98C6CD9400A17ECBD93B38DF885BAC7C9D4237C912796F9C2C2A163D360D4FF7D58A101F59E021D5 19
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...P.o`.....6.... ... ....@.. ..... ..... ..@.....W....@..... ..... ..... ..H.....text...<.... ..... ..`.reloc..... .....@..B.rsr c.....@.....@..@.....H.....o.....,.....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\DKCbURUccsSVSl.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\oE6O5K1emC.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

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

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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.385331204380147
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:	oE6O5K1emC.exe
File size:	1554944
MD5:	0cf0cd25346ee69b7e5aa8e366c886e9
SHA1:	ca13e5bbc69f2d808139ee18ea5ad56579f8b003
SHA256:	f542bc0175168daa808ce1448a019f88b058df6d0702c6daa4a0f83a481f2a5e
SHA512:	03dfe9e8d76c37ab36cff64e569f22861c10baadafeda98c6cd9400a17ecbd93b38df885bac7c9d4237c912796f9c2c2a163d360d4ff7d58a101f59e021d5219
SSDEEP:	24576:8ZHdBedlcA8hbbgPFbg3TwSxivyHOcq5pCkQha6g53oG4l2GfONmPr:uBedlv8hbbgPFbhGYDHJ6g545lpfi8
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...P.o`.....6.... ... .@.. ....@.....

File Icon

Icon Hash:	f0cef27270b2ce70

Static PE Info

General

Entrypoint:	0x560836
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:	0x606FFB50 [Fri Apr 9 06:59:28 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1607dc	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x164000	0x1cacc	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x162000	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	0x15e83c	0x15ea00	False	0.646118120544	Applesoft BASIC program data, first line number 22	7.5082657765	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x162000	0xc	0x200	False	0.044921875	data	0.0776331623432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x164000	0x1cacc	0x1cc00	False	0.35202955163	data	4.73788431456	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x164220	0x4228	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x168448	0x10a8	data		
RT_ICON	0x1694f0	0x25a8	data		
RT_ICON	0x16ba98	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	0x16fcc0	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 16777216, next used block 16777216		
RT_GROUP_ICON	0x1804e8	0x14	data		
RT_GROUP_ICON	0x1804fc	0x4c	data		
RT_VERSION	0x180548	0x338	data		
RT_MANIFEST	0x180880	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	SafeBuffer.exe
FileVersion	2.1.0.8
CompanyName	Northern Star
LegalTrademarks	
Comments	
ProductName	MDM
ProductVersion	2.1.0.8
FileDescription	MDM
OriginalFilename	SafeBuffer.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/09/21-09:47:19.737316	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49727	1144	192.168.2.4	79.134.225.30
04/09/21-09:47:27.294035	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49736	1144	192.168.2.4	79.134.225.30
04/09/21-09:47:33.578124	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49743	1144	192.168.2.4	79.134.225.30
04/09/21-09:47:39.889240	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	1144	192.168.2.4	79.134.225.30
04/09/21-09:47:46.602499	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49747	1144	192.168.2.4	79.134.225.30
04/09/21-09:47:52.785449	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49748	1144	192.168.2.4	79.134.225.30
04/09/21-09:47:59.259086	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49750	1144	192.168.2.4	79.134.225.30

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/09/21-09:48:05.484805	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49758	1144	192.168.2.4	79.134.225.30
04/09/21-09:48:11.811392	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49760	1144	192.168.2.4	79.134.225.30
04/09/21-09:48:17.958802	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49761	1144	192.168.2.4	79.134.225.30
04/09/21-09:48:24.238559	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49762	1144	192.168.2.4	79.134.225.30
04/09/21-09:48:30.288193	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49763	1144	192.168.2.4	79.134.225.30
04/09/21-09:48:36.397083	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49766	1144	192.168.2.4	79.134.225.30
04/09/21-09:48:42.401372	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49768	1144	192.168.2.4	79.134.225.30
04/09/21-09:48:48.419509	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49774	1144	192.168.2.4	79.134.225.30
04/09/21-09:48:54.493298	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49775	1144	192.168.2.4	79.134.225.30
04/09/21-09:49:00.548310	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49776	1144	192.168.2.4	79.134.225.30
04/09/21-09:49:06.594824	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49777	1144	192.168.2.4	79.134.225.30
04/09/21-09:49:12.597526	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49778	1144	192.168.2.4	79.134.225.30

TCP Packets

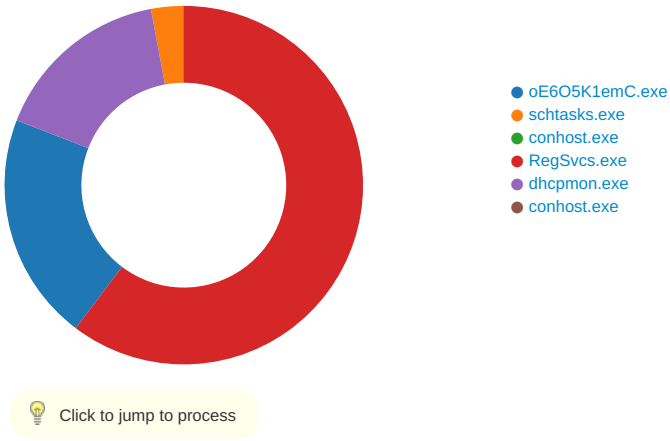
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 09:47:19.387187004 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:19.569410086 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:19.570259094 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:19.737315893 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:19.953636885 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:19.988003016 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:20.082568884 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:20.082724094 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:20.206301928 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:20.206500053 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:20.307507992 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:20.389694929 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:20.389797926 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:20.605148077 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:20.605645895 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:20.828927040 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:20.829598904 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:20.881007910 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:20.881432056 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:20.882491112 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:20.882616997 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:20.882684946 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:20.883604050 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:20.885317087 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:20.885413885 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:20.885556936 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:20.885907888 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:20.885955095 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:20.887207985 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:20.887270927 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:20.887959003 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:20.888298988 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:20.888351917 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:21.051882029 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.075663090 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.089603901 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.090198994 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:21.090348959 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.090464115 CEST	1144	49727	79.134.225.30	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 9, 2021 09:47:21.091731071 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.091831923 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:21.093956947 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.094014883 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.094084978 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.094121933 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:21.094146013 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:21.095455885 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.100219011 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.100867987 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.100920916 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.100979090 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:21.101022959 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:21.101886988 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.103204966 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.103307962 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:21.104449034 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.104614973 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.104712009 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:21.105263948 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.105859995 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.109786987 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:21.115653038 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.115708113 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.115840912 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:21.151675940 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:21.278796911 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.280217886 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.280369043 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:21.288764954 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.288822889 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.289503098 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:21.297285080 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.297326088 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.297487020 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:21.297586918 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.298300028 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:21.298979044 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.299038887 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.300040007 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.300153971 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:21.303910017 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.304107904 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.304913998 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:21.305011988 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.305495977 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:21.305567026 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.305697918 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:21.305702925 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.305758953 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:21.307041883 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.307765961 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.307977915 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.308029890 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:21.308058977 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:21.317260027 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.317495108 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.317498922 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:21.317555904 CEST	49727	1144	192.168.2.4	79.134.225.30
Apr 9, 2021 09:47:21.317639112 CEST	1144	49727	79.134.225.30	192.168.2.4
Apr 9, 2021 09:47:21.317718029 CEST	1144	49727	79.134.225.30	192.168.2.4

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: oE6O5K1emC.exe PID: 6360 Parent PID: 5940

General

Start time:	09:47:04
Start date:	09/04/2021
Path:	C:\Users\user\Desktop\oE6O5K1emC.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\oE6O5K1emC.exe'
Imagebase:	0xde0000
File size:	1554944 bytes
MD5 hash:	0CF0CD25346EE69B7E5AA8E366C886E9
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: 00000000.00000002.676048550.000000000363F000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.676767398.00000000046CA000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.676767398.00000000046CA000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.676767398.00000000046CA000.00000004.00000001.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	722760AC	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	722760AC	unknown
C:\Users\user\AppData\Roaming\DKCbURUccsSVSl.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	585140C	CopyFileW
C:\Users\user\AppData\Roaming\DKCbURUccsSVSl.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	585140C	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp8EBC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	71809869	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\oE6O5K1emC.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	722634A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8EBC.tmp	success or wait	1	585217A	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\DKCbURUccsSVSl.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 50 fb 6f 60 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 ea 15 00 00 ce 01 00 00 00 00 00 36 08 16 00 00 20 00 00 00 20 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 20 18 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...P.o`.......... ....6.... ... .@.. ....@.................	success or wait	6	585140C	CopyFileW
C:\Users\user\AppData\Roaming\DKCbURUccsSVSl.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	585140C	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8EBC.tmp	unknown	1647	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	5851E37	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\oE6O5K1emC.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 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	7254A33A	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	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown

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	722A8738	ReadFile

Analysis Process: schtasks.exe PID: 6456 Parent PID: 6360

General

Start time:	09:47:15
Start date:	09/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\DKCbURUccsSVSl' /XML 'C:\Users\user\AppData\Local\Temp\tmp8EBC.tmp'
Imagebase:	0xf70000
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\tmp8EBC.tmp	unknown	2	success or wait	1	F7AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp8EBC.tmp	unknown	1648	success or wait	1	F7ABD9	ReadFile

Analysis Process: conhost.exe PID: 6464 Parent PID: 6456

General

Start time:	09:47:16
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: 6500 Parent PID: 6360

General

Start time:	09:47:16
Start date:	09/04/2021
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:	0x30000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	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	722760AC	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	23507A1	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	235089B	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	23507A1	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	2350B20	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	23507A1	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	23507A1	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	722760AC	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	722760AC	unknown
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	1	235089B	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	235089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	2	235089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	2350B20	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	success or wait	1	76BF0E	DeleteFileW

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	2a 2f 11 b3 2b fb d8 48	*/..+..H	success or wait	1	2350A53	WriteFile
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 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	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......PE..L..... {Z.................P... ....k... ....@.. ....[....@.................	success or wait	1	2350B20	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	216	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	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	success or wait	1	2350A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	426840	c1 e9 67 26 6a 6f 1f 01 d5 49 50 67 08 81 cd a2 47 4d d1 a4 d4 0d a7 52 3e 69 e1 fc 09 6f 8c b1 04 49 e1 3e e3 bb b0 26 9f 72 7b d6 fa a5 93 38 a9 d3 a5 93 7d ff da 89 8a 45 03 7f ea e6 96 76 cf 21 37 95 75 33 65 bc fc 20 fb c0 05 b7 f7 64 62 bd 90 15 7d b2 c7 1d 02 02 ab e8 22 c2 74 28 06 78 43 39 b8 63 70 15 42 e6 e0 91 e1 37 82 0f 1b 27 bd 93 ad a1 d3 7f c2 25 bd 09 b2 06 eb c7 77 86 5e ac c1 5f 13 c4 d2 02 d8 9d d4 b4 f1 42 b7 57 25 fd 3c ce a6 d9 a4 69 e1 30 d1 7b 39 bb 78 53 fc ab fb 35 c5 d8 c7 29 05 ef 77 ca 0f 24 14 92 43 87 80 3f 60 46 d7 8f da 75 a8 35 db 92 54 b6 58 ab 77 27 53 69 f4 f0 7a b2 6e 7b 8f ef b9 ea 9f 84 59 21 6d d8 d3 1c 52 41 f8 b9 e3 78 67 d3 d0 ba 03 e9 5b 37 8a 18 89 7a b7 9f 39 40 02 4b ca 2d 9a fe 88 54 95 8d 2b d8 41 43 65	..g&jo...IPg....GM.....R>i...o ...I.>...&.r{....8....}....E.. ...v.!7.u3e.. .....db...}..... ..".t(.xC9.cp.B....7...'..... .%.....w.^.._.........B.W%.<. ...i.0.{9.xS...5...)..w..$..C..? `F...u.5..T.X.w'Si..z.n{.... ..Y!m...RA...xg..... [7...z..9@.K.-...T..+.ACe	success or wait	1	2350A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	216	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	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	success or wait	5	2350A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	24	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d f0 4a 22 83 43 3b 22 61	9iH....}Z..4..f..J".C;"a	success or wait	2	2350A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	0	24	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d f0 4a 22 83 43 3b 22 61	9iH....}Z..4..f..J".C;"a	success or wait	1	2350B20	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	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7234BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7234BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	4096	success or wait	1	7234BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	512	success or wait	1	7234BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	2350A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	success or wait	1	2350A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	end of file	1	2350A53	ReadFile

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	2350C12	RegSetValueExW

Analysis Process: dhcpmon.exe PID: 7024 Parent PID: 3424

General

Start time:	09:47:29
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:	0xdc0000
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	722760AC	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	722760AC	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	722634A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	2E6A53F	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	2E6A53F	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 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 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	2E6A53F	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 2e 2e 2e 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	2E6A53F	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	7254A33A	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	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile

Analysis Process: conhost.exe PID: 7032 Parent PID: 7024

General

Start time:	09:47:29
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