ID: 357125
Sample Name:
YoWPu2BQzA9FeDd.exe
Cookbook: default.jbs
Time: 08:21:11
Date: 24/02/2021
Version: 31.0.0 Emerald

Table of Contents

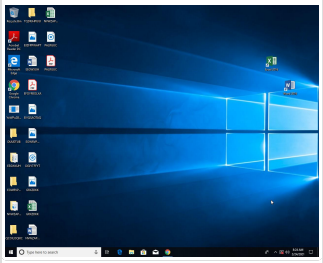
Analysis Report YoWPu2BQzA9FeDd.exe

Overview

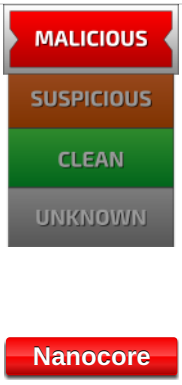
General Information

Sample Name:	YoWPu2BQzA9FeDd.exe
Analysis ID:	357125
MD5:	d89532eebd77f5b.
SHA1:	2905b1b7c97572..
SHA256:	619c9abd416553..
Infos:	

Most interesting Screenshot:



Detection



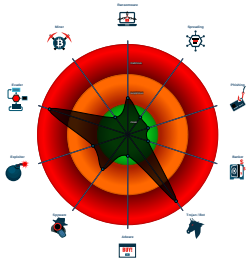
Nanocore

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 doma…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Connects to many ports of the same…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…

Classification



Startup

- **System is w10x64**
- YoWPu2BQzA9FeDd.exe (PID: 4828 cmdline: 'C:\Users\user\Desktop\YoWPu2BQzA9FeDd.exe' MD5: D89532EEBD77F5BCF86552E5178EB695)
  - schtasks.exe (PID: 780 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\jVzJHCyF' /XML 'C:\Users\user\AppData\Local\Temp\tmpA75F.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3728 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 4544 cmdline: {path} MD5: 71369277D09DA0830C8C59F9E22BB23A)
    - schtasks.exe (PID: 372 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp525A.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6172 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6284 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp5614.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6316 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegSvcs.exe (PID: 6508 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe 0 MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 6520 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 6532 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 6548 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 6684 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 71369277D09DA0830C8C59F9E22BB23A)
  - conhost.exe (PID: 6692 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "572eb7a9-aedf-4b39-8669-f7563dab8a38",
  "Group": "GREAT",
  "Domain1": "strongodss.ddns.net",
  "Domain2": "79.134.225.43",
  "Port": 58103,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Enable",
  "SetCriticalProcess": "Enable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Enable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8009,
  "BufferSize": "02000100",
  "MaxPacketSize": "",
  "GCThreshold": "",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.506475973.00000000056F0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000008.00000002.506475973.00000000056F0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
00000000.00000002.283047547.000000000381000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x21957d:$x1: NanoCore.ClientPluginHost • 0x24db8d:$x1: NanoCore.ClientPluginHost • 0x2195ba:$x2: IClientNetworkHost • 0x24dbca:$x2: IClientNetworkHost • 0x21d0ed:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x2516fd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.283047547.000000000381000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.283047547.000000000381000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x2192e5:$a: NanoCore • 0x2192f5:$a: NanoCore • 0x219529:$a: NanoCore • 0x21953d:$a: NanoCore • 0x21957d:$a: NanoCore • 0x24d8f5:$a: NanoCore • 0x24d905:$a: NanoCore • 0x24db39:$a: NanoCore • 0x24db4d:$a: NanoCore • 0x24db8d:$a: NanoCore • 0x219344:$b: ClientPlugin • 0x219546:$b: ClientPlugin • 0x219586:$b: ClientPlugin • 0x24d954:$b: ClientPlugin • 0x24db56:$b: ClientPlugin • 0x24db96:$b: ClientPlugin • 0x160265:$c: ProjectData • 0x21946b:$c: ProjectData • 0x24da7b:$c: ProjectData • 0x219e72:$d: DESCrypto • 0x24e482:$d: DESCrypto

Source	Rule	Description	Author	Strings
Click to see the 14 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.YoWPu2BQzA9FeDd.exe.3934140.1.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x10643d:$x1: NanoCore.ClientPluginHost • 0x13aa4d:$x1: NanoCore.ClientPluginHost • 0x10647a:$x2: IClientNetworkHost • 0x13aa8a:$x2: IClientNetworkHost • 0x109fad:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x13e5bd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.YoWPu2BQzA9FeDd.exe.3934140.1.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.YoWPu2BQzA9FeDd.exe.3934140.1.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x1061a5:$a: NanoCore • 0x1061b5:$a: NanoCore • 0x1063e9:$a: NanoCore • 0x1063fd:$a: NanoCore • 0x10643d:$a: NanoCore • 0x13a7b5:$a: NanoCore • 0x13a7c5:$a: NanoCore • 0x13a9f9:$a: NanoCore • 0x13aa0d:$a: NanoCore • 0x13aa4d:$a: NanoCore • 0x106204:$b: ClientPlugin • 0x106406:$b: ClientPlugin • 0x106446:$b: ClientPlugin • 0x13a814:$b: ClientPlugin • 0x13aa16:$b: ClientPlugin • 0x13aa56:$b: ClientPlugin • 0x4d125:$c: ProjectData • 0x10632b:$c: ProjectData • 0x13a93b:$c: ProjectData • 0x106d32:$d: DESCrypto • 0x13b342:$d: DESCrypto
0.2.YoWPu2BQzA9FeDd.exe.398cb50.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xada2d:$x1: NanoCore.ClientPluginHost • 0xe203d:$x1: NanoCore.ClientPluginHost • 0xada6a:$x2: IClientNetworkHost • 0xe207a:$x2: IClientNetworkHost • 0xb159d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0xe5bad:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.YoWPu2BQzA9FeDd.exe.398cb50.2.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 48 entries				

Sigma Overview

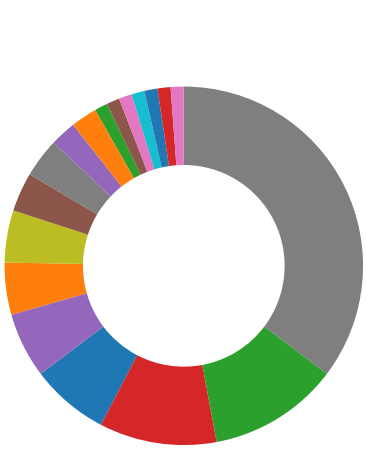
System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview

- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- Operating System Destruction
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging



Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for domain / URL
- Yara detected Nanocore RAT
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Compliance:

- Uses 32bit PE files
- Uses new MSVCR Dlls
- Contains modern PE file flags such as dynamic base (ASLR) or NX
- Binary contains paths to debug symbols

Networking:

- C2 URLs / IPs found in malware configuration
- Connects to many ports of the same IP (likely port scanning)
- Uses dynamic DNS services

E-Banking Fraud:

- Yara detected Nanocore RAT

Operating System Destruction:

- Protects its processes via BreakOnTermination flag

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- .NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Yara detected AntiVM_3

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

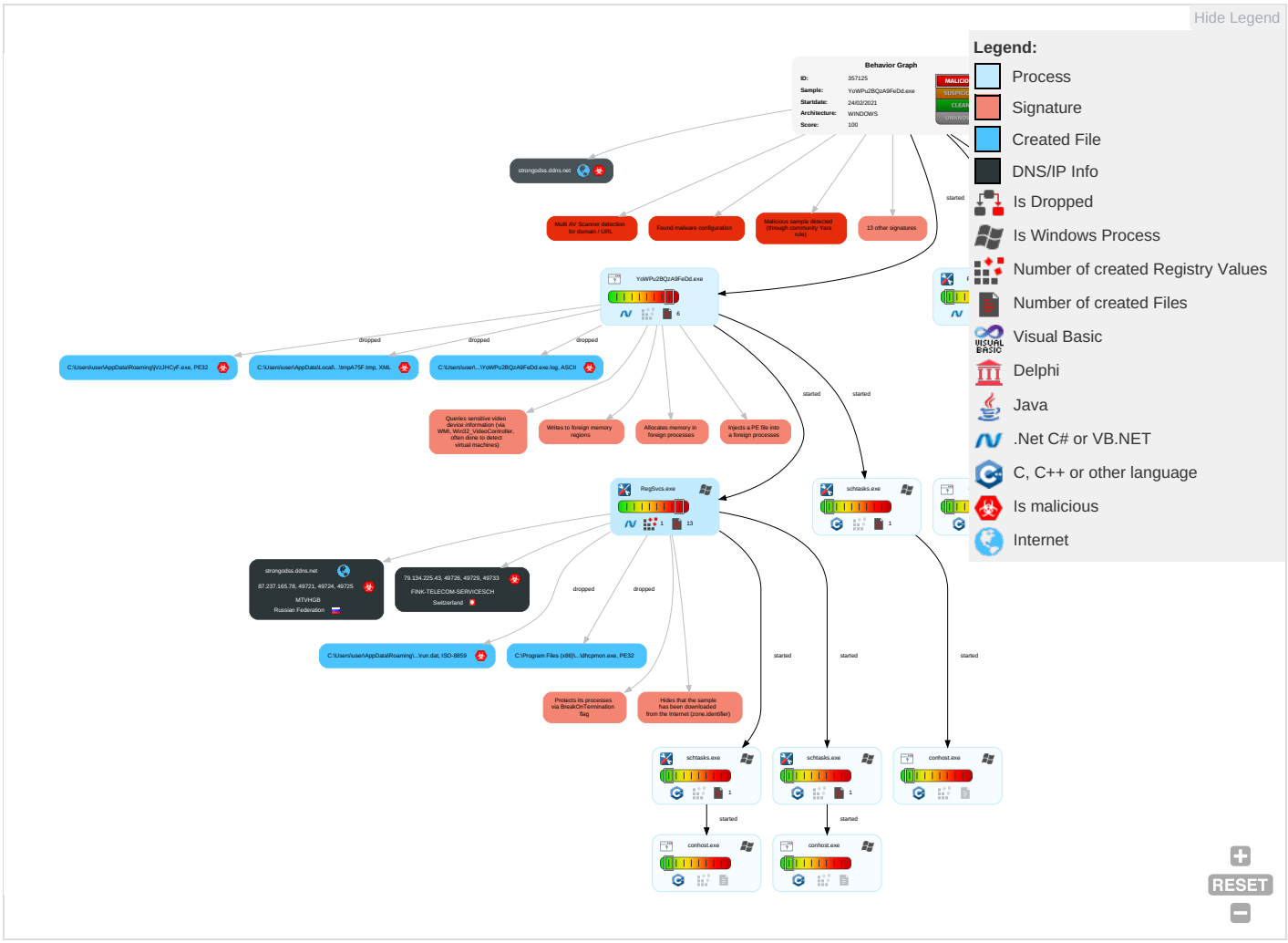
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1	Input Capture 2 1	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Process Injection 3 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 3	Security Account Manager	System Information Discovery 1 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Security Software Discovery 2 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 2	LSA Secrets	Virtualization/Sandbox Evasion 1 3	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3	Cached Domain Credentials	Process Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 3 1 2	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

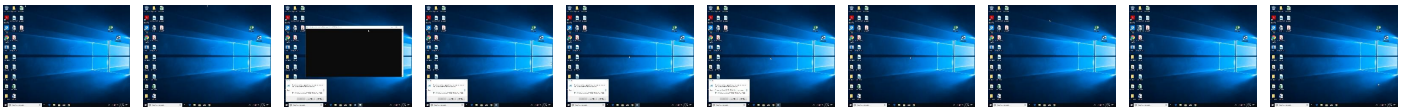
Behavior Graph



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
YoWPu2BQzA9FeDd.exe	100%	Joe Sandbox ML		

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
8.2.RegSvcs.exe.5990000.11.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

Source	Detection	Scanner	Label	Link
strongodss.ddns.net	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/CursF	0%	Avira URL Cloud	safe	
79.134.225.43	1%	Virustotal		Browse
79.134.225.43	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/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/a-e	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Treb	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Negr4	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.fontbureau.como?	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnj	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnw	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comkjz:	0%	Avira URL Cloud	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.tiro.com(	0%	Avira URL Cloud	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.tiro.com#	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0ta?	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kre	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/gH	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.fonts.comX	0%	Avira URL Cloud	safe	
strongodss.ddns.net	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/cn1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/u	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/u	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/u	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.jiyu-kobo.co.jp/ita	0%	Avira URL Cloud	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/-	0%	Avira URL Cloud	safe	
http://www.fonts.comcr	0%	Avira URL Cloud	safe	
http://www.tiro.comcom#	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/c	0%	Avira URL Cloud	safe	
http://www.tiro.comh	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
strongodss.ddns.net	87.237.165.78	true	true	• 8%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
79.134.225.43	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
strongodss.ddns.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

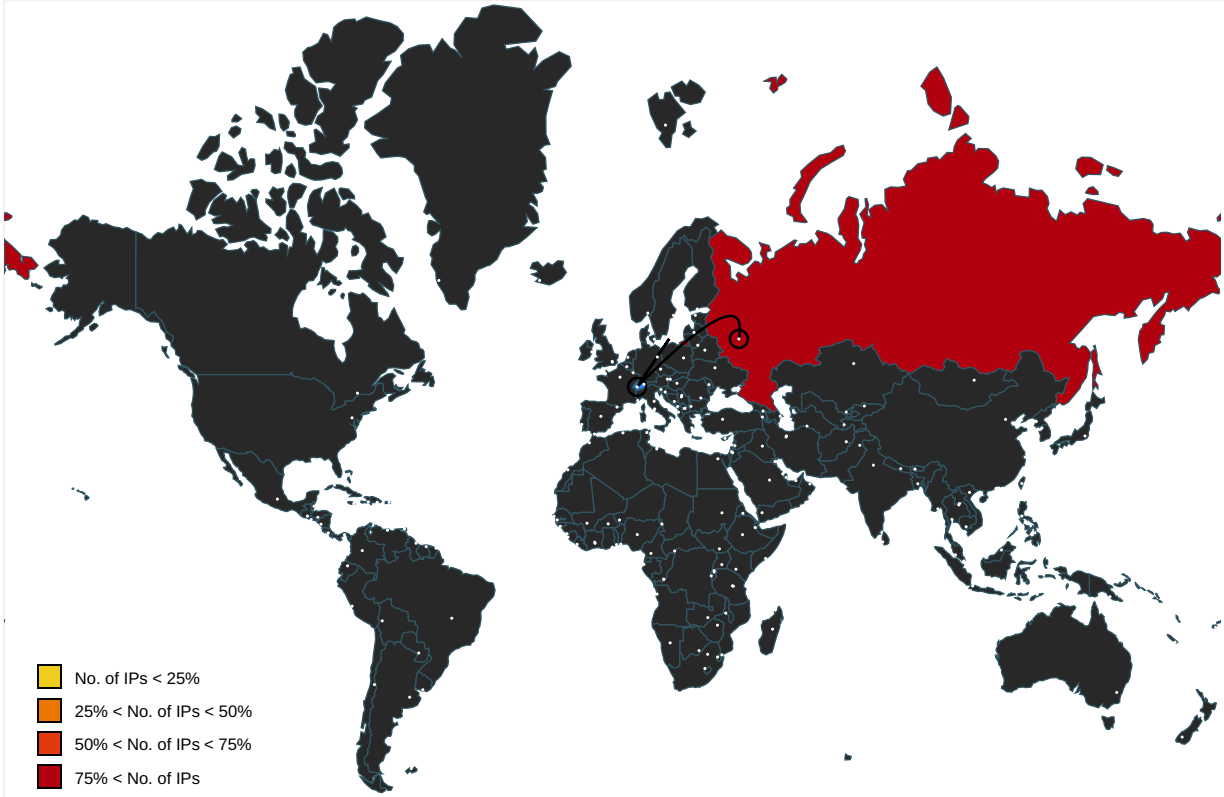
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/CursF	YoWPu2BQzA9FeDd.exe, 00000000.00000003.231570437.0000000004C04000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	YoWPu2BQzA9FeDd.exe, 00000000.00000002.284590175.0000000004D70000.00000002.00000001.sdmp, YoWPu2BQzA9FeDd.exe, 00000000.00000003.233677879.0000000004C0D000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	YoWPu2BQzA9FeDd.exe, 00000000.00000002.284590175.0000000004D70000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	YoWPu2BQzA9FeDd.exe, 00000000.00000002.284590175.0000000004D70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/a-e	YoWPu2BQzA9FeDd.exe, 00000000.00000003.231570437.0000000004C04000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers?	YoWPu2BQzA9FeDd.exe, 00000000.00000002.284590175.0000000004D70000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/Treb	YoWPu2BQzA9FeDd.exe, 00000000.00000003.231570437.0000000004C04000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	YoWPu2BQzA9FeDd.exe, 00000000.00000002.284590175.0000000004D70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	YoWPu2BQzA9FeDd.exe, 00000000.00000002.284590175.0000000004D70000.00000002.00000001.sdmp, YoWPu2BQzA9FeDd.exe, 00000000.00000003.233377138.0000000004C09000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	YoWPu2BQzA9FeDd.exe, 00000000.00000002.284590175.0000000004D70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Negr4	YoWPu2BQzA9FeDd.exe, 00000000.00000003.231570437.0000000004C04000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	YoWPu2BQzA9FeDd.exe, 00000000.00000002.284590175.0000000004D70000.00000002.00000001.sdmp, YoWPu2BQzA9FeDd.exe, 00000000.00000003.228812281.0000000004C1B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	YoWPu2BQzA9FeDd.exe, 00000000.00000002.284590175.0000000004D70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	YoWPu2BQzA9FeDd.exe, 00000000.00000002.284590175.0000000004D70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	YoWPu2BQzA9FeDd.exe, 00000000.00000002.284590175.0000000004D70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	YoWPu2BQzA9FeDd.exe, 00000000.00000002.284590175.0000000004D70000.00000002.00000001.sdmp, YoWPu2BQzA9FeDd.exe, 00000000.00000003.228983734.0000000004C1B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.como?	YoWPu2BQzA9FeDd.exe, 00000000.00000003.278818842.0000000004C00000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnj	YoWPu2BQzA9FeDd.exe, 00000000.00000003.230415696.0000000004C04000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnw	YoWPu2BQzA9FeDd.exe, 00000000.00000003.230415696.0000000004C04000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.comkjz:	YoWPu2BQzA9FeDd.exe, 00000000.00000003.228715164.0000000004C1B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.comn	YoWPu2BQzA9FeDd.exe, 00000000.00000003.228812281.0000000004C1B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	YoWPu2BQzA9FeDd.exe, 00000000.00000002.284590175.0000000004D70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	YoWPu2BQzA9FeDd.exe, 00000000.00000002.284590175.0000000004D70000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	YoWPu2BQzA9FeDd.exe, 00000000.00000002.284590175.0000000004D70000.00000002.00000001.sdmp, YoWPu2BQzA9FeDd.exe, 00000000.00000003.229801364.0000000004C06000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	YoWPu2BQzA9FeDd.exe, 00000000.00000002.284590175.0000000004D70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.com(	YoWPu2BQzA9FeDd.exe, 00000000.00000003.229033812.0000000004C1B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.zhongyicts.com.cn	YoWPu2BQzA9FeDd.exe, 00000000.00000002.284590175.0000000004D70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.tiro.com#	YoWPu2BQzA9FeDd.exe, 00000000.00000003.229005082.0000000004C1B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	YoWPu2BQzA9FeDd.exe, 00000000.00000002.284590175.0000000004D70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y	YoWPu2BQzA9FeDd.exe, 00000000.00000003.231570437.0000000004C04000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	YoWPu2BQzA9FeDd.exe, 00000000.00000002.284590175.0000000004D70000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	YoWPu2BQzA9FeDd.exe, 00000000.00000002.284590175.0000000004D70000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/Y0ta?	YoWPu2BQzA9FeDd.exe, 00000000.00000003.231570437.0000000004C04000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kre	YoWPu2BQzA9FeDd.exe, 00000000.00000003.229801364.0000000004C06000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/gH	YoWPu2BQzA9FeDd.exe, 00000000.00000003.230415696.0000000004C04000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	YoWPu2BQzA9FeDd.exe, 00000000.00000003.231570437.0000000004C04000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.come.com	YoWPu2BQzA9FeDd.exe, 00000000.00000003.278818842.0000000004C00000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.comX	YoWPu2BQzA9FeDd.exe, 00000000.00000003.228746620.0000000004C1B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	YoWPu2BQzA9FeDd.exe, 00000000.00000002.284590175.0000000004D70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	YoWPu2BQzA9FeDd.exe, 00000000.00000003.230415696.0000000004C04000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	YoWPu2BQzA9FeDd.exe, 00000000.00000002.284590175.0000000004D70000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn1	YoWPu2BQzA9FeDd.exe, 00000000.00000003.230415696.0000000004C04000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	YoWPu2BQzA9FeDd.exe, 00000000.00000002.284590175.0000000004D70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	YoWPu2BQzA9FeDd.exe, 00000000.00000002.284590175.0000000004D70000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/u	YoWPu2BQzA9FeDd.exe, 00000000.00000003.231570437.0000000004C04000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	YoWPu2BQzA9FeDd.exe, 00000000.00000002.284590175.0000000004D70000.00000002.00000001.sdmp, YoWPu2BQzA9FeDd.exe, 00000000.00000003.231570437.0000000004C04000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/ita	YoWPu2BQzA9FeDd.exe, 00000000.00000003.231570437.0000000004C04000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.como	YoWPu2BQzA9FeDd.exe, 00000000.00000003.278818842.0000000004C00000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/-	YoWPu2BQzA9FeDd.exe, 00000000.00000003.231570437.0000000004C04000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	YoWPu2BQzA9FeDd.exe, 00000000.00000002.284590175.0000000004D70000.00000002.00000001.sdmp	false		high
http://www.fonts.comcr	YoWPu2BQzA9FeDd.exe, 00000000.00000003.228766582.0000000004C1B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.comcom#	YoWPu2BQzA9FeDd.exe, 00000000.00000003.229033812.0000000004C1B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/c	YoWPu2BQzA9FeDd.exe, 00000000.00000003.231570437.0000000004C04000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers:	YoWPu2BQzA9FeDd.exe, 00000000.00000003.233377138.0000000004C09000.00000004.00000001.sdmp	false		high
http://www.tiro.comh	YoWPu2BQzA9FeDd.exe, 00000000.00000003.229033812.0000000004C1B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersURWf	YoWPu2BQzA9FeDd.exe, 00000000.00000003.233677879.0000000004C0D000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
87.237.165.78	unknown	Russian Federation		49967	MTVHGB	true
79.134.225.43	unknown	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	357125
Start date:	24.02.2021
Start time:	08:21:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	YoWPu2BQzA9FeDd.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:	35
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@18/13@11/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 16.5% (good quality ratio 11.6%) • Quality average: 43.6% • Quality standard deviation: 35.8%
HCA Information:	• Successful, ratio: 94% • 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): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, HxTsr.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 51.103.5.159, 131.253.33.200, 13.107.22.200, 204.79.197.200, 13.107.21.200, 51.11.168.160, 93.184.220.29, 104.43.193.48, 40.88.32.150, 92.122.145.220, 184.30.20.56, 51.104.144.132, 93.184.221.240, 51.104.139.180, 92.122.213.247, 92.122.213.194, 20.54.26.129 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, cs9.wac.phicdn.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, vip1-par02p.wns.notify.trafficmanager.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, www.bing.com, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, wu.ec.azureedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many 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
08:22:06	API Interceptor	1x Sleep call for process: YoWPu2BQzA9FeDd.exe modified
08:22:28	API Interceptor	822x Sleep call for process: RegSvcs.exe modified
08:22:29	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe" s>$(Arg0)
08:22:29	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
08:22:30	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
87.237.165.78	M5QDAaK9yM.exe	Get hash	malicious	Browse	
	TdX45jQWjj.exe	Get hash	malicious	Browse	
79.134.225.43	TdX45jQWjj.exe	Get hash	malicious	Browse	
	JfRbEbUkpV39K4L.exe	Get hash	malicious	Browse	
	Dachser Consulta de cliente saliente no. 000150849 - SKBMT03082020-0012-IMG0149.exe	Get hash	malicious	Browse	
	290453721.xls	Get hash	malicious	Browse	
	nUo0FukkVO.xls	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
strongodss.ddns.net	M5QDAaK9yM.exe	Get hash	malicious	Browse	• 87.237.165.78
	TdX45jQWjj.exe	Get hash	malicious	Browse	• 87.237.165.78

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MTVHGB	M5QDAaK9yM.exe	Get hash	malicious	Browse	• 87.237.165.78
	TdX45jQWjj.exe	Get hash	malicious	Browse	• 87.237.165.78
	QUOTATION 19 01 2021.exe	Get hash	malicious	Browse	• 87.237.165.162
FINK-TELECOM-SERVICESCH	xF7GogN7tM.exe	Get hash	malicious	Browse	• 79.134.225.120
	TZgGVyMJYF.exe	Get hash	malicious	Browse	• 79.134.225.74
	ilpbALnKbE.exe	Get hash	malicious	Browse	• 79.134.225.103
	Documents.exe	Get hash	malicious	Browse	• 79.134.225.87
	SWcNyi2YBj.exe	Get hash	malicious	Browse	• 79.134.225.103
	Confirmation Transfer Note Ref Number0002636.exe	Get hash	malicious	Browse	• 79.134.225.8
	TdX45jQWjj.exe	Get hash	malicious	Browse	• 79.134.225.43
	e92b274943f4a3a557881ee0dd57772d.exe	Get hash	malicious	Browse	• 79.134.225.105
	WxTm2cWLHF.exe	Get hash	malicious	Browse	• 79.134.225.71
	Payment Confirmation.exe	Get hash	malicious	Browse	• 79.134.225.30
	rjHlt1zz28.exe	Get hash	malicious	Browse	• 79.134.225.49
	Deadly Variants of Covid 19.doc	Get hash	malicious	Browse	• 79.134.225.49
	document.exe	Get hash	malicious	Browse	• 79.134.225.122
	5293ea9467ea45e928620a5ed74440f5.exe	Get hash	malicious	Browse	• 79.134.225.105
	f1a14e6352036833f1c109e1bb2934f2.exe	Get hash	malicious	Browse	• 79.134.225.105
	256ec8f8f67b59c5e085b0bb63afcd13.exe	Get hash	malicious	Browse	• 79.134.225.105
	JOIN.exe	Get hash	malicious	Browse	• 79.134.225.30
	Delivery pdf.exe	Get hash	malicious	Browse	• 79.134.225.25
	d88e07467ddcf9e3b19fa972b9f000d1.exe	Get hash	malicious	Browse	• 79.134.225.105

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	fnfqzfwC44.exe	Get hash	malicious	Browse	• 79.134.225.25

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	M5QDAaK9yM.exe	Get hash	malicious	Browse	
	oMWv1Zof2y.exe	Get hash	malicious	Browse	
	TdX45jQWjj.exe	Get hash	malicious	Browse	
	QTxFuxF5NQ.exe	Get hash	malicious	Browse	
	a34b93ef-dea2-45f8-a5bf-4f6b0b5291c7.exe	Get hash	malicious	Browse	
	3fcd8c19-af88-4cd9-87e7-0bfea1de01a1.exe	Get hash	malicious	Browse	
	Vietnam Order.exe	Get hash	malicious	Browse	
	Dhl Shipping Document.exe	Get hash	malicious	Browse	
	PO-WJO-001, pdf.exe	Get hash	malicious	Browse	
	byWuWAR5FD.exe	Get hash	malicious	Browse	
	parcel_images.exe	Get hash	malicious	Browse	
	0712020.exe	Get hash	malicious	Browse	
	JfRbEbUkpV39K4L.exe	Get hash	malicious	Browse	
	DECEMBER QUOTATION REQUEST FOR FR12007PO H0008_PO0000143_ETQ.exe	Get hash	malicious	Browse	
	DECEMBER QUOTATION REQUEST FOR FR12007PO H0008_PO0000143_ETQ.exe	Get hash	malicious	Browse	
	zC3edqmNNt.exe	Get hash	malicious	Browse	
	Shipping Document.pdf..exe	Get hash	malicious	Browse	
	PPR & CPR_HEA_DECEMBER 4 2020.exe	Get hash	malicious	Browse	
	AdministratorDownloadsBL,.rar.exe	Get hash	malicious	Browse	
	signed_19272.zip(#U007e18 KB) (2).exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	3.7515815714465193
Encrypted:	false
SSDEEP:	384:BOj9Y8/gS7SDriLGKq1MHR5U4Ag6ihJSxUCR1rgCPKabK2t0X5P7DZ+JgWSW72uw:B+gSAdN1MH3HAFRJngW2u
MD5:	71369277D09DA0830C8C59F9E22BB23A
SHA1:	37F9781314F0F6B7E9CB529A573F2B1C8DE9E93F
SHA-256:	D4527B7AD2FC4778CC5BE8709C95AEA44EAC0568B367EE14F7357D72898C3698
SHA-512:	2F470383E3C796C4CF212EC280854DBB9E7E8C8010CE6857E58F8E7066D7516B7CD7039BC5C0F547E1F5C7F9F2287869ADFFB2869800B08B2982A88BE96E9FB7
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Joe Sandbox View:	• Filename: M5QDAaK9yM.exe, Detection: malicious, Browse • Filename: oMWv1Zof2y.exe, Detection: malicious, Browse • Filename: TdX45jQWjj.exe, Detection: malicious, Browse • Filename: QTxFuxF5NQ.exe, Detection: malicious, Browse • Filename: a34b93ef-dea2-45f8-a5bf-4f6b0b5291c7.exe, Detection: malicious, Browse • Filename: 3fcd8c19-af88-4cd9-87e7-0bfea1de01a1.exe, Detection: malicious, Browse • Filename: Vietnam Order.exe, Detection: malicious, Browse • Filename: Dhl Shipping Document.exe, Detection: malicious, Browse • Filename: PO-WJO-001, pdf.exe, Detection: malicious, Browse • Filename: byWuWAR5FD.exe, Detection: malicious, Browse • Filename: parcel_images.exe, Detection: malicious, Browse • Filename: 0712020.exe, Detection: malicious, Browse • Filename: JfRbEbUkpV39K4L.exe, Detection: malicious, Browse • Filename: DECEMBER QUOTATION REQUEST FOR FR12007POH0008_PO0000143_ETQ.exe, Detection: malicious, Browse • Filename: DECEMBER QUOTATION REQUEST FOR FR12007POH0008_PO0000143_ETQ.exe, Detection: malicious, Browse • Filename: zC3edqmNNt.exe, Detection: malicious, Browse • Filename: Shipping Document.pdf..exe, Detection: malicious, Browse • Filename: PPR & CPR_HEA_DECEMBER 4 2020.exe, Detection: malicious, Browse • Filename: AdministratorDownloadsBL,.rar.exe, Detection: malicious, Browse • Filename: signed_19272.zip(#U007e18 KB) (2).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\RegSvcs.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.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
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\YoWPu2BQzA9FeDd.exe.log	
Process:	C:\Users\user\Desktop\YoWPu2BQzA9FeDd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	655
Entropy (8bit):	5.273171405160065
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9t0U2WUXBQav:MLF20NaL329hJ5g522rWz2p29XBT
MD5:	2703120C370FBB4A8BA08C6D1754039E
SHA1:	EC0DB47BF00A4A828F796147619386C0BBEA66A1
SHA-256:	F95566974BC44F3A757CAFB1456D185D8F333AC84775089DE18310B90C18B1BC
SHA-512:	BC05A2A1BE5B122FC6D3DEA66EF4258522F13351B9754378395AAD019631E312CFD3BC990F3E3D5C7BB0BDBA1EAD54A2B34A96DEE2FCCD703721E98F6192EE 48
Malicious:	**true**
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\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_3 2\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.Vi sualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Management\4de9980 4c29261edb63c93616550f034\System.Management.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	120
Entropy (8bit):	5.016405576253028
Encrypted:	false
SSDEEP:	3:QHXMKaoWglAFXMWA2yTMGfsbNXLVd49Am12MFuAvOAsDeieVyn:Q3LawlAFXMWTyAGCFLIP12MUAvvrs

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
MD5:	50DEC1858E13F033E6DCA3CBFAD5E8DE
SHA1:	79AE1E9131B0FAF215B499D2F7B4C595AA120925
SHA-256:	14A557E226E3BA8620BB3A70035E1E316F1E9FB5C9E8F74C07110EE90B8D8AE4
SHA-512:	1BD73338DF685A5B57B0546E102ECFDEE65800410D6F77845E50456AC70DE72929088AF19B59647F01CBA7A5ACFB399C52D9EF2402A9451366586862EF88E7BF
Malicious:	false
Preview:	1,"fusion","GAC",0..2,"System.EnterpriseServices, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\tmp525A.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	5.135021273392143
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mn4xtn:cbk4oL600QydbQxIYODOLedq3Z4j
MD5:	40B11EF601FB28F9B2E69D36857BF2EC
SHA1:	B6454020AD2CEED193F4792B77001D0BD741B370
SHA-256:	C51E12D18CC664425F6711D8AE2507068884C7057092CFA11884100E1E9D49E1
SHA-512:	E3C5BCC714CBFCA4B8058DDCDDF231DCEFA69C15881CE3F8123E59ED45CFB5DA052B56E1945DCF8DC7F800D62F9A4EECB82BCA69A66A1530787AEFFEB15E 2BD5
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp5614.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpA75F.tmp	
Process:	C:\Users\user\Desktop\YoWPu2BQzA9FeDd.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.184387907108357
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB1ltn:cbhC7ZlNQF/rydbz9l3YODOLNdq3XP
MD5:	00610593D653206BB931FCF95B1203BB
SHA1:	1C7C0CCA00A060BDBEC31112A2BEB698B80FE70E
SHA-256:	1B3CD0A440D8A8EBBB0BCC7DC5D3ED7A442899384700F925EFD5A9BEB388BBC2
SHA-512:	F2195BA16493ED0300E13DF91BC36537DB820F03E6D1B5EA18F8BE24C4713D61FB0BF599A14480BD2D35E9E50DB2A6625DCE0C10024B38EF0B40E6737801A6E
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\tmpA75F.tmp

Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

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

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	ISO-8859 text
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:B6H9tn:UPn
MD5:	D1B6084630019902FEB9DE04281559F5
SHA1:	E70B066BA32E2D81E593EB4D5B4C3B9D0B8CBF73
SHA-256:	EA08804D6AB9E9F7708C2D0DC62474D681028F726BC403EFAF5BE1EAC40213F4
SHA-512:	C5F428D1EBD3BD998647045A8132A9EDF5EFB918D633C461DCF312F96EF453D8C7F58261B8EAED9C76D1B185E44B81BA98ED8A081B4D66845F5F1F153FA1ACA
Malicious:	**true**
Preview:	.O._...H

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

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.795707286467131
Encrypted:	false
SSDEEP:	3:oMty8WbSX/MNn:oMLWus
MD5:	D685103573539B7E9FDBF5F1D7DD96CE
SHA1:	4B2FE6B5C0B37954B314FCAEE1F12237A9B02D07
SHA-256:	D78BC23B0CA3EDDF52D56AB85CDC30A71B3756569CB32AA2F6C28DBC23C76E8E
SHA-512:	17769A5944E8929323A34269ABEEF0861D5C6799B0A27F5545FBFADC80E5AB684A471AD6F6A7FC623002385154EA89DE94013051E09120AB94362E542AB0F1DD
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe

C:\Users\user\AppData\Roaming\jVzJHCyF.exe

Process:	C:\Users\user\Desktop\YoWPu2BQzA9FeDd.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	393216
Entropy (8bit):	7.913835302870024
Encrypted:	false
SSDEEP:	6144:vd1ZByWI+5c6hL1DNxNGmSMRTOenrUb89mBKAIB1bG3gmA6caIndoQ2NTWqDivu:zrEe7p1DVnrUIGKAIB1PR9dl2NTjD
MD5:	D89532EEBD77F5BCF86552E5178EB695
SHA1:	2905B1B7C9757266077D4C79A81CF410188AA9EE
SHA-256:	619C9ABD4165537A7E53C57F2C0A2AB9597C35F53A4BB0B9CDFF82814DDD73CD
SHA-512:	076391F8D60D3A4901469E0F16B4D3DD988848B587ACB217BBB6C8A83FB4EFA2956219AA3ACDF267E835EC1F6704EFE5AC4E1834E1B8729F9CFD35458D020AF8
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...9.5`................................. ........@.. .......................`.......... ..@....................................K.... ....@.. ....H............text........ ....`.rsrc........ .......................@..@.rel oc.......@......................@..B........................H....... ...`[...........g..HQ..r.(8......r...p(7.....o;....*....0............{.....+..*.0..*.........#.............,...}....+..#........}... .*...0............{.....+..*.0..*.........#............,...}....+..#........}....*...0............{.....+..*.0..*.........#............,...}....+..#........}....*...0..M........#.......@.{.....{....ZZ#.......@.{.....{....ZZX#.......@. {.....{....ZZX.+..*....0............{.....{....Z.{....Z.+..*...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

\Device\ConDrv	
Entropy (8bit):	4.462201512373672
Encrypted:	false
SSDEEP:	24:zKLXkzPDObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0zPDQntKKH1MqJC
MD5:	46EBEB88876A00A52CC37B1F8E0D0438
SHA1:	5E5DB352F964E5F398301662FF558BD905798A65
SHA-256:	D65BD5A6CC112838AFE8FA70BF61FD13C1313BCE3EE3E76C50E454D7B581238B
SHA-512:	E713E6F304A469FB71235C598BC7E2C6F8458ABC61DAF3D1F364F66579CAFA4A7F3023E585BDA552FB400009E7805A8CA0311A50D5EDC9C2AD2D067772A071BE
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 2.0.50727.8922..Copyright (c) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [options] AssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp Expect an existing application... /tlb:<tlbfile> Filename for the exported type library... /appname:<name> Use the specified name for the target application... /parname:<name> Use the specified name or id for the target partition... /extlb Use an existing type library... /reconfig Reconfigure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo Suppress logo output... /quiet Suppress logo output and success output...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.913835302870024
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.98% • Win32 Executable (generic) a (10002005/4) 49.93% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	YoWPu2BQzA9FeDd.exe
File size:	393216
MD5:	d89532eebd77f5bcf86552e5178eb695
SHA1:	2905b1b7c9757266077d4c79a81cf410188aa9ee
SHA256:	619c9abd4165537a7e53c57f2c0a2ab9597c35f53a4bb0b9cdff82814ddd73cd
SHA512:	076391f8d60d3a4901469e0f16b4d3dd988848b587acb217bbb6c8a83fb4efa2956219aa3acdf267e835ec1f6704efe5ac4e1834e1b8729f9cfd35458d020af8
SSDEEP:	6144:vd1ZByWI+5c6hL1DNxNGmSMRTOenrUb89mBKAIB1bG3gmA6caIndoQ2NTWqDivu:zrEe7p1DVnrUIGKAIB1PR9dl2NTjD
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...9.5`..... .....@.. .....`.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4614ce
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60359A39 [Wed Feb 24 00:13:45 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4

General

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x61480	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x62000	0x600	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x64000	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	0x5f4d4	0x5f600	False	0.932080910059	data	7.92573751907	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x62000	0x600	0x600	False	0.442708333333	data	4.27871469905	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x64000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x62090	0x36c	data		
RT_MANIFEST	0x6240c	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

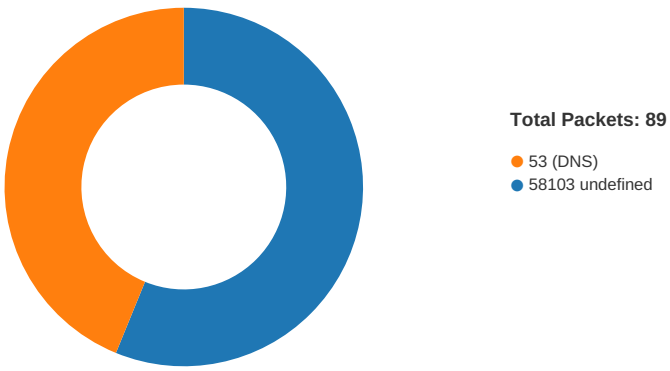
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Neudesic 2017
Assembly Version	1.0.0.0
InternalName	etaib.exe
FileVersion	1.0.0.0
CompanyName	Neudesic
LegalTrademarks	
Comments	
ProductName	VectorBasedDrawing
ProductVersion	1.0.0.0
FileDescription	VectorBasedDrawing
OriginalFilename	etaib.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 08:22:30.782995939 CET	49721	58103	192.168.2.5	87.237.165.78
Feb 24, 2021 08:22:30.838046074 CET	58103	49721	87.237.165.78	192.168.2.5
Feb 24, 2021 08:22:31.439275980 CET	49721	58103	192.168.2.5	87.237.165.78
Feb 24, 2021 08:22:31.494411945 CET	58103	49721	87.237.165.78	192.168.2.5
Feb 24, 2021 08:22:32.048032999 CET	49721	58103	192.168.2.5	87.237.165.78
Feb 24, 2021 08:22:32.102804899 CET	58103	49721	87.237.165.78	192.168.2.5
Feb 24, 2021 08:22:36.311920881 CET	49724	58103	192.168.2.5	87.237.165.78
Feb 24, 2021 08:22:36.369085073 CET	58103	49724	87.237.165.78	192.168.2.5
Feb 24, 2021 08:22:36.939038992 CET	49724	58103	192.168.2.5	87.237.165.78
Feb 24, 2021 08:22:36.993746042 CET	58103	49724	87.237.165.78	192.168.2.5
Feb 24, 2021 08:22:37.548553944 CET	49724	58103	192.168.2.5	87.237.165.78
Feb 24, 2021 08:22:37.605607033 CET	58103	49724	87.237.165.78	192.168.2.5
Feb 24, 2021 08:22:41.738549948 CET	49725	58103	192.168.2.5	87.237.165.78
Feb 24, 2021 08:22:41.793747902 CET	58103	49725	87.237.165.78	192.168.2.5
Feb 24, 2021 08:22:42.439625978 CET	49725	58103	192.168.2.5	87.237.165.78
Feb 24, 2021 08:22:42.494566917 CET	58103	49725	87.237.165.78	192.168.2.5
Feb 24, 2021 08:22:43.049822092 CET	49725	58103	192.168.2.5	87.237.165.78
Feb 24, 2021 08:22:43.105144024 CET	58103	49725	87.237.165.78	192.168.2.5
Feb 24, 2021 08:22:47.114248037 CET	49726	58103	192.168.2.5	79.134.225.43
Feb 24, 2021 08:22:47.193187952 CET	58103	49726	79.134.225.43	192.168.2.5
Feb 24, 2021 08:22:47.705701113 CET	49726	58103	192.168.2.5	79.134.225.43
Feb 24, 2021 08:22:47.782963037 CET	58103	49726	79.134.225.43	192.168.2.5
Feb 24, 2021 08:22:48.283792973 CET	49726	58103	192.168.2.5	79.134.225.43
Feb 24, 2021 08:22:48.360804081 CET	58103	49726	79.134.225.43	192.168.2.5
Feb 24, 2021 08:22:52.548042059 CET	49729	58103	192.168.2.5	79.134.225.43
Feb 24, 2021 08:22:52.629520893 CET	58103	49729	79.134.225.43	192.168.2.5
Feb 24, 2021 08:22:53.143534899 CET	49729	58103	192.168.2.5	79.134.225.43
Feb 24, 2021 08:22:53.223515987 CET	58103	49729	79.134.225.43	192.168.2.5
Feb 24, 2021 08:22:53.737364054 CET	49729	58103	192.168.2.5	79.134.225.43
Feb 24, 2021 08:22:53.817322016 CET	58103	49729	79.134.225.43	192.168.2.5
Feb 24, 2021 08:22:57.850348949 CET	49733	58103	192.168.2.5	79.134.225.43
Feb 24, 2021 08:22:57.929667950 CET	58103	49733	79.134.225.43	192.168.2.5
Feb 24, 2021 08:22:58.472224951 CET	49733	58103	192.168.2.5	79.134.225.43
Feb 24, 2021 08:22:58.553515911 CET	58103	49733	79.134.225.43	192.168.2.5
Feb 24, 2021 08:22:59.175331116 CET	49733	58103	192.168.2.5	79.134.225.43
Feb 24, 2021 08:22:59.252497911 CET	58103	49733	79.134.225.43	192.168.2.5
Feb 24, 2021 08:23:03.373195887 CET	49734	58103	192.168.2.5	87.237.165.78
Feb 24, 2021 08:23:03.427895069 CET	58103	49734	87.237.165.78	192.168.2.5
Feb 24, 2021 08:23:04.066615105 CET	49734	58103	192.168.2.5	87.237.165.78
Feb 24, 2021 08:23:04.121443987 CET	58103	49734	87.237.165.78	192.168.2.5
Feb 24, 2021 08:23:04.675764084 CET	49734	58103	192.168.2.5	87.237.165.78
Feb 24, 2021 08:23:04.730675936 CET	58103	49734	87.237.165.78	192.168.2.5
Feb 24, 2021 08:23:09.127697945 CET	49735	58103	192.168.2.5	87.237.165.78
Feb 24, 2021 08:23:09.182590008 CET	58103	49735	87.237.165.78	192.168.2.5
Feb 24, 2021 08:23:09.879338980 CET	49735	58103	192.168.2.5	87.237.165.78
Feb 24, 2021 08:23:09.934106112 CET	58103	49735	87.237.165.78	192.168.2.5
Feb 24, 2021 08:23:10.569262981 CET	49735	58103	192.168.2.5	87.237.165.78
Feb 24, 2021 08:23:10.626955986 CET	58103	49735	87.237.165.78	192.168.2.5
Feb 24, 2021 08:23:14.746368885 CET	49736	58103	192.168.2.5	87.237.165.78
Feb 24, 2021 08:23:14.801103115 CET	58103	49736	87.237.165.78	192.168.2.5
Feb 24, 2021 08:23:15.302474976 CET	49736	58103	192.168.2.5	87.237.165.78
Feb 24, 2021 08:23:15.357213020 CET	58103	49736	87.237.165.78	192.168.2.5
Feb 24, 2021 08:23:15.864249945 CET	49736	58103	192.168.2.5	87.237.165.78
Feb 24, 2021 08:23:15.919167042 CET	58103	49736	87.237.165.78	192.168.2.5
Feb 24, 2021 08:23:19.929440022 CET	49738	58103	192.168.2.5	79.134.225.43
Feb 24, 2021 08:23:20.011518955 CET	58103	49738	79.134.225.43	192.168.2.5
Feb 24, 2021 08:23:20.520958900 CET	49738	58103	192.168.2.5	79.134.225.43
Feb 24, 2021 08:23:20.602849007 CET	58103	49738	79.134.225.43	192.168.2.5
Feb 24, 2021 08:23:21.115187883 CET	49738	58103	192.168.2.5	79.134.225.43
Feb 24, 2021 08:23:21.196707964 CET	58103	49738	79.134.225.43	192.168.2.5
Feb 24, 2021 08:23:25.241487980 CET	49739	58103	192.168.2.5	79.134.225.43
Feb 24, 2021 08:23:25.319788933 CET	58103	49739	79.134.225.43	192.168.2.5
Feb 24, 2021 08:23:25.833787918 CET	49739	58103	192.168.2.5	79.134.225.43
Feb 24, 2021 08:23:25.913105965 CET	58103	49739	79.134.225.43	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 08:23:26.427709103 CET	49739	58103	192.168.2.5	79.134.225.43
Feb 24, 2021 08:23:26.505489111 CET	58103	49739	79.134.225.43	192.168.2.5
Feb 24, 2021 08:23:30.523605108 CET	49740	58103	192.168.2.5	79.134.225.43
Feb 24, 2021 08:23:30.603581905 CET	58103	49740	79.134.225.43	192.168.2.5
Feb 24, 2021 08:23:31.115519047 CET	49740	58103	192.168.2.5	79.134.225.43
Feb 24, 2021 08:23:31.195658922 CET	58103	49740	79.134.225.43	192.168.2.5
Feb 24, 2021 08:23:31.709307909 CET	49740	58103	192.168.2.5	79.134.225.43
Feb 24, 2021 08:23:31.791932106 CET	58103	49740	79.134.225.43	192.168.2.5
Feb 24, 2021 08:23:35.948029995 CET	49743	58103	192.168.2.5	87.237.165.78
Feb 24, 2021 08:23:36.003094912 CET	58103	49743	87.237.165.78	192.168.2.5
Feb 24, 2021 08:23:36.506711006 CET	49743	58103	192.168.2.5	87.237.165.78
Feb 24, 2021 08:23:36.562042952 CET	58103	49743	87.237.165.78	192.168.2.5
Feb 24, 2021 08:23:37.069272041 CET	49743	58103	192.168.2.5	87.237.165.78
Feb 24, 2021 08:23:37.124191046 CET	58103	49743	87.237.165.78	192.168.2.5
Feb 24, 2021 08:23:41.241198063 CET	49744	58103	192.168.2.5	87.237.165.78
Feb 24, 2021 08:23:41.295802116 CET	58103	49744	87.237.165.78	192.168.2.5
Feb 24, 2021 08:23:41.803934097 CET	49744	58103	192.168.2.5	87.237.165.78
Feb 24, 2021 08:23:41.859724998 CET	58103	49744	87.237.165.78	192.168.2.5
Feb 24, 2021 08:23:42.366508961 CET	49744	58103	192.168.2.5	87.237.165.78
Feb 24, 2021 08:23:42.421324968 CET	58103	49744	87.237.165.78	192.168.2.5
Feb 24, 2021 08:23:46.646815062 CET	49745	58103	192.168.2.5	87.237.165.78
Feb 24, 2021 08:23:46.701983929 CET	58103	49745	87.237.165.78	192.168.2.5
Feb 24, 2021 08:23:47.210638046 CET	49745	58103	192.168.2.5	87.237.165.78
Feb 24, 2021 08:23:47.267636061 CET	58103	49745	87.237.165.78	192.168.2.5
Feb 24, 2021 08:23:47.773190022 CET	49745	58103	192.168.2.5	87.237.165.78
Feb 24, 2021 08:23:47.828268051 CET	58103	49745	87.237.165.78	192.168.2.5
Feb 24, 2021 08:23:51.837430000 CET	49746	58103	192.168.2.5	79.134.225.43
Feb 24, 2021 08:23:51.917613029 CET	58103	49746	79.134.225.43	192.168.2.5
Feb 24, 2021 08:23:52.425215960 CET	49746	58103	192.168.2.5	79.134.225.43
Feb 24, 2021 08:23:52.507610083 CET	58103	49746	79.134.225.43	192.168.2.5
Feb 24, 2021 08:23:53.008169889 CET	49746	58103	192.168.2.5	79.134.225.43
Feb 24, 2021 08:23:53.089534998 CET	58103	49746	79.134.225.43	192.168.2.5
Feb 24, 2021 08:23:57.104069948 CET	49747	58103	192.168.2.5	79.134.225.43
Feb 24, 2021 08:23:57.184240103 CET	58103	49747	79.134.225.43	192.168.2.5
Feb 24, 2021 08:23:57.695939064 CET	49747	58103	192.168.2.5	79.134.225.43
Feb 24, 2021 08:23:57.776223898 CET	58103	49747	79.134.225.43	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 08:21:52.260188103 CET	52212	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:21:52.322455883 CET	53	52212	8.8.8.8	192.168.2.5
Feb 24, 2021 08:21:52.366096020 CET	54302	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:21:52.414977074 CET	53	54302	8.8.8.8	192.168.2.5
Feb 24, 2021 08:21:53.000411034 CET	53784	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:21:53.022375107 CET	65307	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:21:53.050311089 CET	53	53784	8.8.8.8	192.168.2.5
Feb 24, 2021 08:21:53.082479954 CET	64344	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:21:53.094324112 CET	53	65307	8.8.8.8	192.168.2.5
Feb 24, 2021 08:21:53.133622885 CET	53	64344	8.8.8.8	192.168.2.5
Feb 24, 2021 08:21:53.230941057 CET	62060	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:21:53.233053923 CET	61805	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:21:53.279875994 CET	53	62060	8.8.8.8	192.168.2.5
Feb 24, 2021 08:21:53.282114983 CET	53	61805	8.8.8.8	192.168.2.5
Feb 24, 2021 08:21:53.415981054 CET	54795	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:21:53.469950914 CET	53	54795	8.8.8.8	192.168.2.5
Feb 24, 2021 08:21:54.392311096 CET	49557	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:21:54.442476988 CET	53	49557	8.8.8.8	192.168.2.5
Feb 24, 2021 08:21:55.281292915 CET	61733	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:21:55.330447912 CET	53	61733	8.8.8.8	192.168.2.5
Feb 24, 2021 08:21:56.149508953 CET	65447	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:21:56.201980114 CET	53	65447	8.8.8.8	192.168.2.5
Feb 24, 2021 08:21:56.260215998 CET	52441	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:21:56.310190916 CET	53	52441	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 08:21:57.048332930 CET	62176	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:21:57.098763943 CET	53	62176	8.8.8.8	192.168.2.5
Feb 24, 2021 08:21:58.168817997 CET	59596	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:21:58.233833075 CET	53	59596	8.8.8.8	192.168.2.5
Feb 24, 2021 08:21:59.152137041 CET	65296	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:21:59.212820053 CET	53	65296	8.8.8.8	192.168.2.5
Feb 24, 2021 08:22:00.361061096 CET	63183	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:22:00.412805080 CET	53	63183	8.8.8.8	192.168.2.5
Feb 24, 2021 08:22:01.188030005 CET	60151	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:22:01.241625071 CET	53	60151	8.8.8.8	192.168.2.5
Feb 24, 2021 08:22:02.242263079 CET	56969	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:22:02.294141054 CET	53	56969	8.8.8.8	192.168.2.5
Feb 24, 2021 08:22:03.690298080 CET	55161	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:22:03.743562937 CET	53	55161	8.8.8.8	192.168.2.5
Feb 24, 2021 08:22:23.757661104 CET	54757	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:22:23.833329916 CET	53	54757	8.8.8.8	192.168.2.5
Feb 24, 2021 08:22:30.604545116 CET	49992	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:22:30.663717031 CET	53	49992	8.8.8.8	192.168.2.5
Feb 24, 2021 08:22:33.373549938 CET	60075	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:22:33.424674988 CET	53	60075	8.8.8.8	192.168.2.5
Feb 24, 2021 08:22:36.250876904 CET	55016	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:22:36.310040951 CET	53	55016	8.8.8.8	192.168.2.5
Feb 24, 2021 08:22:41.677490950 CET	64345	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:22:41.736562014 CET	53	64345	8.8.8.8	192.168.2.5
Feb 24, 2021 08:22:48.257189035 CET	57128	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:22:48.306087971 CET	53	57128	8.8.8.8	192.168.2.5
Feb 24, 2021 08:22:48.452671051 CET	54791	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:22:48.513299942 CET	53	54791	8.8.8.8	192.168.2.5
Feb 24, 2021 08:22:53.427459955 CET	50463	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:22:53.482548952 CET	53	50463	8.8.8.8	192.168.2.5
Feb 24, 2021 08:22:57.695728064 CET	50394	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:22:57.755152941 CET	53	50394	8.8.8.8	192.168.2.5
Feb 24, 2021 08:23:03.313415051 CET	58530	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:23:03.370950937 CET	53	58530	8.8.8.8	192.168.2.5
Feb 24, 2021 08:23:09.045413971 CET	53813	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:23:09.108172894 CET	53	53813	8.8.8.8	192.168.2.5
Feb 24, 2021 08:23:14.686711073 CET	63732	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:23:14.744349003 CET	53	63732	8.8.8.8	192.168.2.5
Feb 24, 2021 08:23:17.985760927 CET	57344	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:23:18.058620930 CET	53	57344	8.8.8.8	192.168.2.5
Feb 24, 2021 08:23:33.511554003 CET	54450	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:23:33.563227892 CET	53	54450	8.8.8.8	192.168.2.5
Feb 24, 2021 08:23:33.975176096 CET	59261	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:23:34.032975912 CET	53	59261	8.8.8.8	192.168.2.5
Feb 24, 2021 08:23:35.872972965 CET	57151	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:23:35.933026075 CET	53	57151	8.8.8.8	192.168.2.5
Feb 24, 2021 08:23:41.178101063 CET	59413	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:23:41.238497972 CET	53	59413	8.8.8.8	192.168.2.5
Feb 24, 2021 08:23:46.545110941 CET	60516	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:23:46.604031086 CET	53	60516	8.8.8.8	192.168.2.5
Feb 24, 2021 08:24:07.702549934 CET	51649	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:24:07.764501095 CET	53	51649	8.8.8.8	192.168.2.5
Feb 24, 2021 08:24:12.964740038 CET	65086	53	192.168.2.5	8.8.8.8
Feb 24, 2021 08:24:13.028446913 CET	53	65086	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 24, 2021 08:22:30.604545116 CET	192.168.2.5	8.8.8.8	0xf3ad	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 08:22:36.250876904 CET	192.168.2.5	8.8.8.8	0x8e4e	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 08:22:41.677490950 CET	192.168.2.5	8.8.8.8	0xab8c	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 24, 2021 08:23:03.313415051 CET	192.168.2.5	8.8.8.8	0x19a1	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 08:23:09.045413971 CET	192.168.2.5	8.8.8.8	0x52d8	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 08:23:14.686711073 CET	192.168.2.5	8.8.8.8	0xa96a	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 08:23:35.872972965 CET	192.168.2.5	8.8.8.8	0xcb26	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 08:23:41.178101063 CET	192.168.2.5	8.8.8.8	0x7259	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 08:23:46.545110941 CET	192.168.2.5	8.8.8.8	0xf593	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 08:24:07.702549934 CET	192.168.2.5	8.8.8.8	0xe272	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)
Feb 24, 2021 08:24:12.964740038 CET	192.168.2.5	8.8.8.8	0xbe3d	Standard query (0)	strongodss .ddns.net	A (IP address)	IN (0x0001)

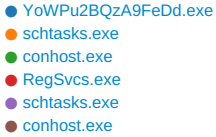
DNS Answers

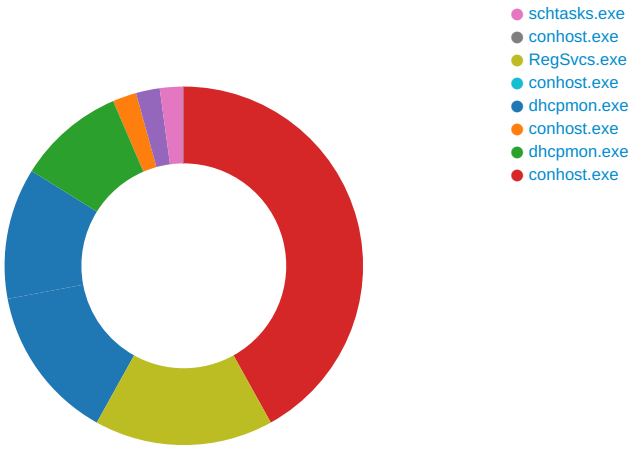
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 24, 2021 08:22:30.663717031 CET	8.8.8.8	192.168.2.5	0xf3ad	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 08:22:36.310040951 CET	8.8.8.8	192.168.2.5	0x8e4e	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 08:22:41.736562014 CET	8.8.8.8	192.168.2.5	0xab8c	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 08:23:03.370950937 CET	8.8.8.8	192.168.2.5	0x19a1	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 08:23:09.108172894 CET	8.8.8.8	192.168.2.5	0x52d8	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 08:23:14.744349003 CET	8.8.8.8	192.168.2.5	0xa96a	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 08:23:35.933026075 CET	8.8.8.8	192.168.2.5	0xcb26	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 08:23:41.238497972 CET	8.8.8.8	192.168.2.5	0x7259	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 08:23:46.604031086 CET	8.8.8.8	192.168.2.5	0xf593	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 08:24:07.764501095 CET	8.8.8.8	192.168.2.5	0xe272	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)
Feb 24, 2021 08:24:13.028446913 CET	8.8.8.8	192.168.2.5	0xbe3d	No error (0)	strongodss .ddns.net		87.237.165.78	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: YoWPu2BQzA9FeDd.exe PID: 4828 Parent PID: 5660

General

Start time:	08:22:00
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\YoWPu2BQzA9FeDd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\YoWPu2BQzA9FeDd.exe'
Imagebase:	0x50000
File size:	393216 bytes
MD5 hash:	D89532EEBD77F5BCF86552E5178EB695
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.283047547.0000000003821000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.283047547.0000000003821000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.283047547.0000000003821000.00000004.00000001.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	72B860AC	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	72B860AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\jVzJHCyF.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	4A21D1F	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpA75F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	69B5B8	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\YoWPu2BQzA9FeDd.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72B734A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA75F.tmp	success or wait	1	4A22996	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\jVzJHCyF.exe	unknown	393216	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 39 9a 35 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 f6 05 00 00 08 00 00 00 00 00 00 ce 14 06 00 00 20 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 60 06 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...9.5`.......... ....................... ........@.. .......................` ....@................	success or wait	1	4A21FA7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpA75F.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 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationI	success or wait	1	4A21FA7	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\YoWPu2BQzA9FeDd.exe.log	unknown	655	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 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	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\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	72E5A33A	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	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Users\user\Desktop\YoWPu2BQzA9FeDd.exe	unknown	393216	success or wait	1	4A21FA7	ReadFile

Analysis Process: schtasks.exe PID: 780 Parent PID: 4828

General

Start time:	08:22:23
Start date:	24/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\jVzJHCyF' /XML 'C:\Users\user\AppData\Local\Temp\tmpA75F.tmp'
Imagebase:	0x8b0000
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\tmpA75F.tmp	unknown	2	success or wait	1	8BAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpA75F.tmp	unknown	1646	success or wait	1	8BABD9	ReadFile

Analysis Process: conhost.exe PID: 3728 Parent PID: 780

General

Start time:	08:22:24
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 4544 Parent PID: 4828

General

Start time:	08:22:24
Start date:	24/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x7ff797770000
File size:	32768 bytes
MD5 hash:	71369277D09DA0830C8C59F9E22BB23A

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.506475973.00000000056F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.506475973.00000000056F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.505452740.0000000003DF7000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.505452740.0000000003DF7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.494649173.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.494649173.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.494649173.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.506530348.0000000005840000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.506530348.0000000005840000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.506614119.0000000005990000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000008.00000002.506614119.0000000005990000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.506614119.0000000005990000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72B860AC	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	72B860AC	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	4EF07A1	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	4EF089B	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	4EF07A1	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	4EF0B20	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp525A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4EF0D1C	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	4EF089B	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp5614.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4EF0D1C	GetTempFileNameW
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	4EF07A1	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	4EF07A1	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	72B860AC	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	72B860AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp525A.tmp	success or wait	1	DABF0E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp5614.tmp	success or wait	1	DABF0E	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	0a 4f f7 5f e0 d8 d8 48	.O._...H	success or wait	1	4EF0A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	32768	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 cf ce 7b 5a 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 08 00 00 50 00 00 00 20 00 00 00 00 00 00 de 6b 00 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 00 00 00 10 00 00 b1 5b 01 00 03 00 40 05 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......PE..L..... {Z.................P... ....k... ....@.. ....[....@................	success or wait	1	4EF0B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp525A.tmp	unknown	1320	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 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	4EF0A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	57	43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 5c 76 32 2e 30 2e 35 30 37 32 37 5c 52 65 67 53 76 63 73 2e 65 78 65	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	success or wait	1	4EF0A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp5614.tmp	unknown	1310	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 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	4EF0A53	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	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72BB8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	72C5BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	72C5BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	4096	success or wait	1	72C5BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegSvcs.exe	unknown	512	success or wait	1	72C5BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	4EF0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	success or wait	1	4EF0A53	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4096	end of file	1	4EF0A53	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	4EF0C12	RegSetValueExW

Analysis Process: schtasks.exe PID: 372 Parent PID: 4544

General

Start time:	08:22:26
Start date:	24/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp525A.tmp'
Imagebase:	0x8b0000
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\tmp525A.tmp	unknown	2	success or wait	1	8BAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp525A.tmp	unknown	1321	success or wait	1	8BABD9	ReadFile

Analysis Process: conhost.exe PID: 6172 Parent PID: 372

General

Start time:	08:22:27
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6284 Parent PID: 4544

General

Start time:	08:22:27
Start date:	24/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp5614.tmp'
Imagebase:	0x8b0000
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\tmp5614.tmp	unknown	2	success or wait	1	8BAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp5614.tmp	unknown	1311	success or wait	1	8BABD9	ReadFile

Analysis Process: conhost.exe PID: 6316 Parent PID: 6284

General

Start time:	08:22:28
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 6508 Parent PID: 904

General

Start time:	08:22:29
Start date:	24/02/2021
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 0
Imagebase:	0xac0000
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	72B860AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	72B860AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RegSvcs.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72B734A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	7219DCB3	unknown
\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	7219DFAB	unknown
\Device\ConDrv	unknown	45	0a 54 68 65 20 66 6f 6c 6c 6f 77 69 6e 67 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 65 72 72 6f 72 20 6f 63 63 75 72 72 65 64 3a 0d 0a	.The following installation error occurred:..	success or wait	1	7219DFAB	unknown
\Device\ConDrv	unknown	29	31 3a 20 41 73 73 65 6d 62 6c 79 20 6e 6f 74 20 66 6f 75 6e 64 3a 20 27 30 27 2e 0d 0a	1: Assembly not found: '0'...	success or wait	1	7219DFAB	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\RegSvcs.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	72E5A33A	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	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regsvcs.exe.config	unknown	8173	end of file	1	72BB8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile

Analysis Process: conhost.exe PID: 6520 Parent PID: 6508

General

Start time:	08:22:30
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 6532 Parent PID: 904

General

Start time:	08:22:30
Start date:	24/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x860000
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	72B860AC	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	72B860AC	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	72B734A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	7219DCB3	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\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	7219DFAB	unknown
\Device\ConDrv	unknown	45	0a 54 68 65 20 66 6f 6c 6c 6f 77 69 6e 67 20 69 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 65 72 72 6f 72 20 6f 63 63 75 72 72 65 64 3a 0d 0a	.The following installation error occurred:..	success or wait	1	7219DFAB	unknown
\Device\ConDrv	unknown	29	31 3a 20 41 73 73 65 6d 62 6c 79 20 6e 6f 74 20 66 6f 75 6e 64 3a 20 27 30 27 2e 0d 0a	1: Assembly not found: '0'...	success or wait	1	7219DFAB	unknown
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	72E5A33A	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	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile

Analysis Process: conhost.exe PID: 6548 Parent PID: 6532

General

Start time:	08:22:30
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 6684 Parent PID: 3472

General

Start time:	08:22:38
Start date:	24/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x540000
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	72B860AC	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	72B860AC	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	B1A53F	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	B1A53F	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 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 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 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 application, error if it already exists... /exapp	success or wait	3	B1A53F	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 53 75 70 70 72 65 73 73 20 6c 6f 67 6f 20 6f 75 74 70 75 74 20 61 6e 64 20 73 75 63 63 65 73 73 20 6f 75 74 70 75 74 2e 0d 0a 20 20 20 20 2f 63 6f 6d 70 6f 6e 6c 79 20 20 20 20 20 20 20 20 43 6f 6e 66 69 67 75 72 65 20 63 6f 6d 70 6f 6e 65 6e 74 73 20 6f 6e 6c 79 2c 20 6e 6f 20 6d 65 74 68 6f 64 73 20 6f 72 20 69 6e 74 65 72 66 61 63 65 73 2e 0d 0a 20 20 20 20 2f 61 70 70 64 69 72 3a 3c 70 61 74 68 3e 20 20 53 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 72 6f 6f 74 20 64 69 72 65 63 74 6f 72 79 20 74 6f 20 73 70 65 63 69 66 69 65 64 20 70 61 74 68 2e 0d 0a 0d 0a	Suppress logo output... /quiet Suppress logo output and success output... /componly Configure components only, no methods or inte rfaces... /appdir:<path> Set application root directory to specified path.....	success or wait	1	B1A53F	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	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile

Analysis Process: conhost.exe PID: 6692 Parent PID: 6684

General

Start time:	08:22:39
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis