ID: 383118
Sample Name:
ANS_309487487_#049844874.exe
Cookbook: default.jbs
Time: 09:05:04
Date: 07/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report ANS_309487487_#049844874.exe 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Startup 5
Malware Configuration 5
Threatname: NanoCore 5
Yara Overview 6
Memory Dumps 6
Unpacked PEs 6
Sigma Overview 7
System Summary: 7
Signature Overview 7
AV Detection: 7
Networking: 7
E-Banking Fraud: 7
System Summary: 7
Data Obfuscation: 7
Boot Survival: 8
Hooking and other Techniques for Hiding and Protection: 8
Malware Analysis System Evasion: 8
HIPS / PFW / Operating System Protection Evasion: 8
Stealing of Sensitive Information: 8
Remote Access Functionality: 8
Mitre Att&ck Matrix 8
Behavior Graph 9
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 12
Contacted IPs 13
Public 13
Private 13
General Information 14
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 15
IPs 15
Domains 16
ASN 16
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 17
Static File Info 21
General 21

File Icon 21
Static PE Info 21
General 21
Entrypoint Preview 21
Data Directories 23
Sections 23
Resources 23
Imports 24
Version Infos 24
Network Behavior 24
Snort IDS Alerts 24
Network Port Distribution 25
TCP Packets 25
UDP Packets 27
DNS Queries 28
DNS Answers 28
Code Manipulations 29
Statistics 29
Behavior 29
System Behavior 29
Analysis Process: ANS_309487487_#049844874.exe PID: 5688 Parent PID: 5840 29
General 29
File Activities 30
File Created 30
File Deleted 30
File Written 30
File Read 32
Analysis Process: schtasks.exe PID: 4012 Parent PID: 5688 32
General 32
File Activities 33
File Read 33
Analysis Process: conhost.exe PID: 5592 Parent PID: 4012 33
General 33
Analysis Process: RegSvcs.exe PID: 5404 Parent PID: 5688 33
General 33
File Activities 35
File Created 35
File Deleted 35
File Written 36
File Read 37
Registry Activities 38
Key Value Created 38
Analysis Process: schtasks.exe PID: 4904 Parent PID: 5404 38
General 38
File Activities 38
File Read 39
Analysis Process: conhost.exe PID: 5864 Parent PID: 4904 39
General 39
Analysis Process: schtasks.exe PID: 4132 Parent PID: 5404 39
General 39
File Activities 39
File Read 39
Analysis Process: conhost.exe PID: 4500 Parent PID: 4132 39
General 40
Analysis Process: RegSvcs.exe PID: 5400 Parent PID: 904 40
General 40
File Activities 40
File Created 40
File Written 40
File Read 41
Analysis Process: conhost.exe PID: 5564 Parent PID: 5400 41
General 41
Analysis Process: dhcpmon.exe PID: 5824 Parent PID: 904 41
General 42
File Activities 42
File Created 42
File Written 42
File Read 43
Analysis Process: conhost.exe PID: 5864 Parent PID: 5824 43
General 43
Analysis Process: dhcpmon.exe PID: 6360 Parent PID: 3472 43
General 43

File Activities 44
File Written 44
File Read 45
Analysis Process: conhost.exe PID: 6368 Parent PID: 6360 45
General 45
Disassembly 45
Code Analysis 45

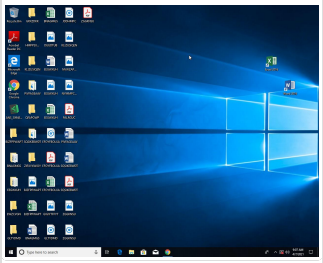
Analysis Report ANS_309487487_#049844874.exe

Overview

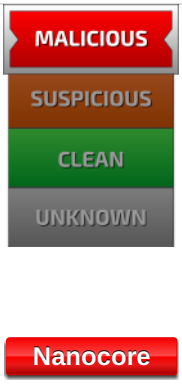
General Information

Sample Name:	ANS_309487487_#049844874.exe
Analysis ID:	383118
MD5:	203109ad6d2efdc.
SHA1:	471d5a99a2e8bfe.
SHA256:	5e7e5b02d1de0d..
Infos:	

Most interesting Screenshot:



Detection

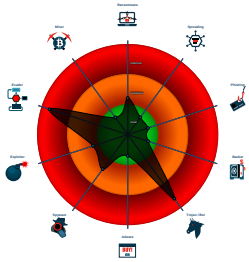


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains method …
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…

Classification



Startup

- **System is w10x64**
- ANS_309487487_#049844874.exe (PID: 5688 cmdline: 'C:\Users\user\Desktop\ANS_309487487_#049844874.exe' MD5: 203109AD6D2EFDCA0BF52CAB63A7CE6A)
  - schtasks.exe (PID: 4012 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\zgEmPmIdAWvDGJ' /XML 'C:\Users\user\AppData\Local\Temp\tmpDC3C.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5592 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 5404 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
    - schtasks.exe (PID: 4904 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp6007.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5864 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 4132 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp6940.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 4500 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegSvcs.exe (PID: 5400 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 5564 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 5824 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 5864 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 6360 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 6368 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "15fbba02-3f99-4e02-884c-0827498f",
  "Group": "1118",
  "Domain1": "myhustle.duckdns.org",
  "Domain2": "",
  "Port": 1118,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "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
00000004.00000002.497078079.0000000006CF0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x8ba5:$x1: NanoCore.ClientPluginHost • 0x8bd2:$x2: IClientNetworkHost
00000004.00000002.497078079.0000000006CF0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x8ba5:$x2: NanoCore.ClientPluginHost • 0x9b74:$s2: FileCommand • 0xe576:$s4: PipeCreated • 0x8bbf:$s5: IClientLoggingHost
00000004.00000002.497210658.0000000006D50000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x13a8:$x1: NanoCore.ClientPluginHost
00000004.00000002.497210658.0000000006D50000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x13a8:$x2: NanoCore.ClientPluginHost • 0x1486:$s4: PipeCreated • 0x13c2:$s5: IClientLoggingHost
00000004.00000002.497223355.0000000006D60000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x59eb:$x1: NanoCore.ClientPluginHost • 0x5b48:$x2: IClientNetworkHost
Click to see the 43 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.RegSvcs.exe.6d80000.25.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5b99:$x1: NanoCore.ClientPluginHost • 0x5bb3:$x2: IClientNetworkHost
4.2.RegSvcs.exe.6d80000.25.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x5b99:$x2: NanoCore.ClientPluginHost • 0x6bce:$s4: PipeCreated • 0x5b86:$s5: IClientLoggingHost
4.2.RegSvcs.exe.64e0000.14.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
4.2.RegSvcs.exe.64e0000.14.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
4.2.RegSvcs.exe.6df0000.30.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x41ee:$x1: NanoCore.ClientPluginHost • 0x422b:$x2: IClientNetworkHost

Source	Rule	Description	Author	Strings
Click to see the 104 entries				

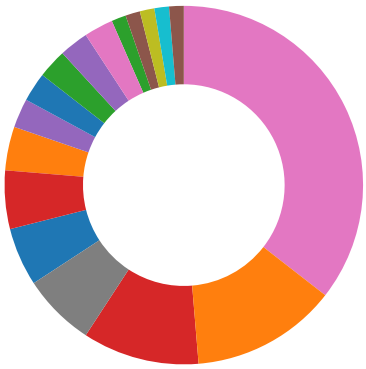
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains method to dynamically call methods (often used by packers)

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

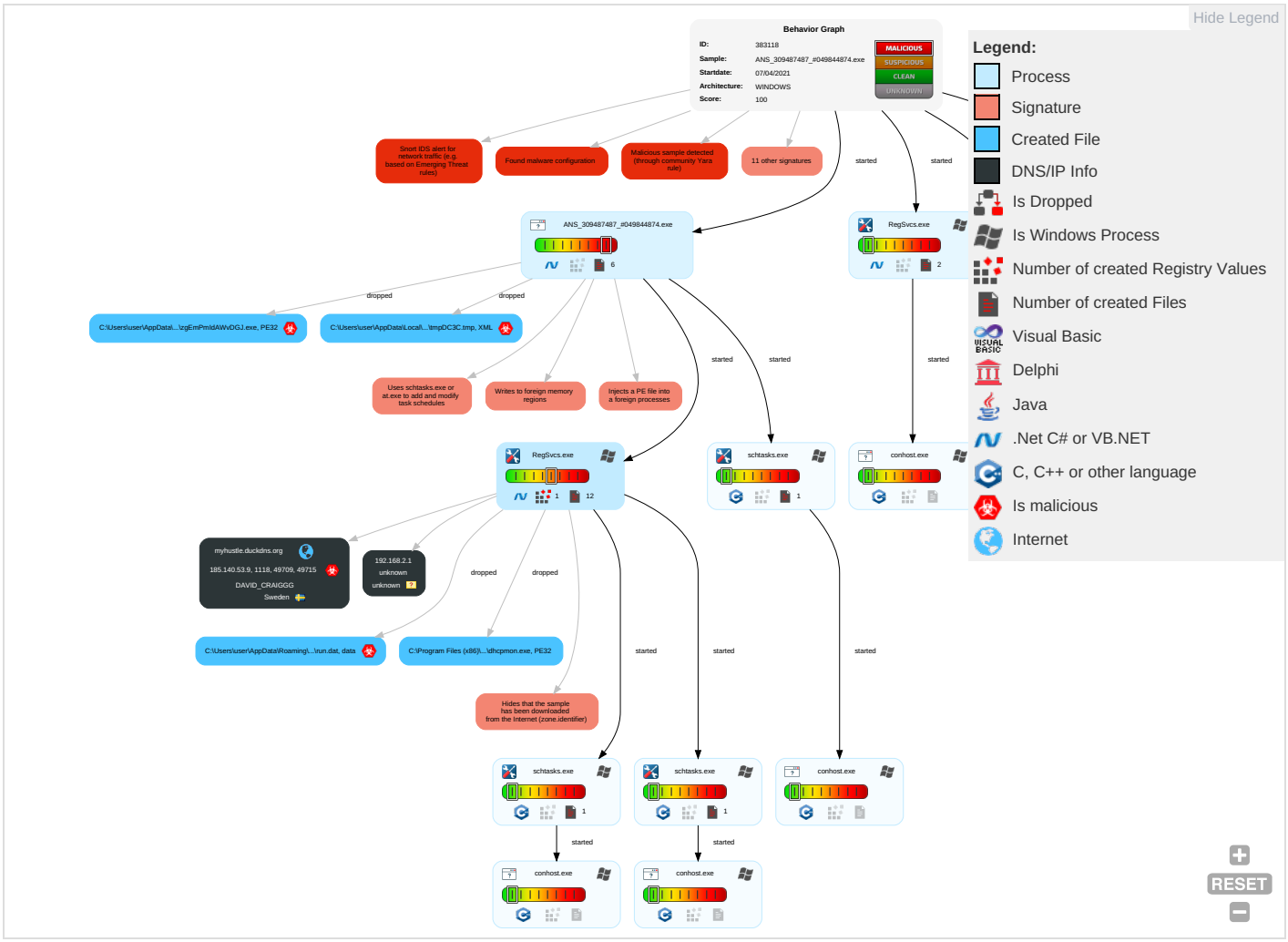
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 2 1 2	Masquerading 2	Input Capture 2 1	Security Software Discovery 2 1 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc

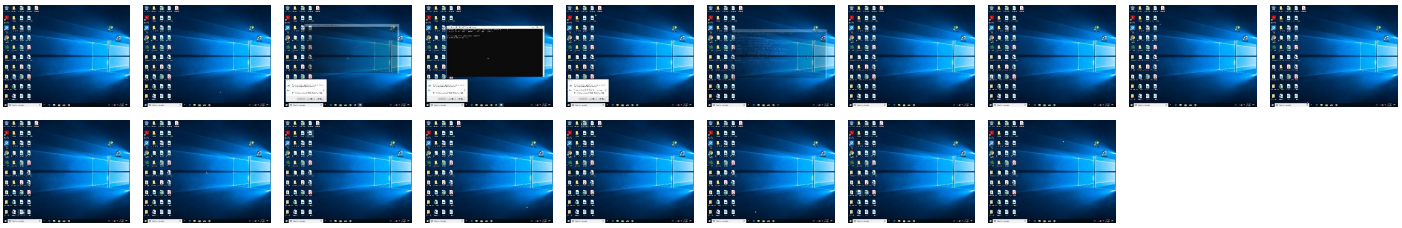
Behavior Graph



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

No Antivirus matches

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.2.RegSvcs.exe.6570000.15.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
	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.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
myhustle.duckdns.org	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.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.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
myhustle.duckdns.org	185.140.53.9	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low

Name	Malicious	Antivirus Detection	Reputation
myhustle.duckdns.org	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	ANS_309487487_#049844874.exe, 00000000.00000002.251783792.00000000006360000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	ANS_309487487_#049844874.exe, 00000000.00000002.251783792.00000000006360000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	ANS_309487487_#049844874.exe, 00000000.00000002.251783792.00000000006360000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	ANS_309487487_#049844874.exe, 00000000.00000002.251783792.00000000006360000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	ANS_309487487_#049844874.exe, 00000000.00000002.251783792.00000000006360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	ANS_309487487_#049844874.exe, 00000000.00000002.251783792.00000000006360000.00000002.00000001.sdmp	false		high
http://www.tiro.com	ANS_309487487_#049844874.exe, 00000000.00000002.251783792.00000000006360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	ANS_309487487_#049844874.exe, 00000000.00000002.251783792.00000000006360000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	ANS_309487487_#049844874.exe, 00000000.00000002.251783792.00000000006360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	ANS_309487487_#049844874.exe, 00000000.00000002.251783792.00000000006360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	ANS_309487487_#049844874.exe, 00000000.00000002.251783792.00000000006360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	ANS_309487487_#049844874.exe, 00000000.00000002.251783792.00000000006360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	ANS_309487487_#049844874.exe, 00000000.00000002.251783792.00000000006360000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	ANS_309487487_#049844874.exe, 00000000.00000002.251783792.00000000006360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	ANS_309487487_#049844874.exe, 00000000.00000002.251783792.00000000006360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	ANS_309487487_#049844874.exe, 00000000.00000002.251783792.00000000006360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	ANS_309487487_#049844874.exe, 00000000.00000002.251783792.00000000006360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	ANS_309487487_#049844874.exe, 00000000.00000002.251783792.00000000006360000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/	ANS_309487487_#049844874.exe, 00000000.00000002.251783792.00000000006360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	ANS_309487487_#049844874.exe, 00000000.00000002.251783792.00000000006360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	ANS_309487487_#049844874.exe, 00000000.00000002.251783792.00000000006360000.00000002.00000001.sdmp	false		high
http://www.fonts.com	ANS_309487487_#049844874.exe, 00000000.00000002.251783792.00000000006360000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	ANS_309487487_#049844874.exe, 00000000.00000002.251783792.00000000006360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	ANS_309487487_#049844874.exe, 00000000.00000002.251783792.00000000006360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	ANS_309487487_#049844874.exe, 00000000.00000002.251783792.00000000006360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	ANS_309487487_#049844874.exe, 00000000.00000002.257735814.00000000009877000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	ANS_309487487_#049844874.exe, 00000000.00000002.251783792.00000000006360000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.9	myhustle.duckdns.org	Sweden		209623	DAVID_CRAIGGG	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383118
Start date:	07.04.2021
Start time:	09:05:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ANS_309487487_#049844874.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@17/14@16/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.4% (good quality ratio 0.4%) • Quality average: 100% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 99% • 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, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 93.184.220.29, 104.42.151.234, 104.43.139.144, 95.100.54.203, 52.147.198.201, 13.64.90.137, 20.82.210.154, 23.10.249.26, 23.10.249.43, 20.54.26.129 • Excluded domains from analysis (whitelisted): www.bing.com, skypedataprdcolwus17.cloudapp.net, cs9.wac.phicdn.net, fs.microsoft.com, arc.msn.com.nsatc.net, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, blobcollector.events.data.trafficmanager.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, skypedataprdcolwus16.cloudapp.net • 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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/383118/sample/ANS_309487487_#049844874.exe

Simulations

Behavior and APIs

Time	Type	Description
09:05:57	API Interceptor	2x Sleep call for process: ANS_309487487_#049844874.exe modified
09:06:10	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe" s>$(Arg0)
09:06:10	API Interceptor	883x Sleep call for process: RegSvcs.exe modified
09:06:10	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
09:06:11	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.140.53.9	t5R60D503x.exe	Get hash	malicious	Browse	
	GT_0397337_03987638BNG.exe	Get hash	malicious	Browse	
	1PH37n4Gva.exe	Get hash	malicious	Browse	
	malwa.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	HDF_39837635_0398376HJD.exe	Get hash	malicious	Browse	
	E0029876556_209876689.exe	Get hash	malicious	Browse	
	BGD_03987365_0398736DSC.exe	Get hash	malicious	Browse	
	DHL_AWB #9855452108.exe	Get hash	malicious	Browse	
	Simo_Inquiry_FOB_Order_9820_xlsx.exe	Get hash	malicious	Browse	
	Summer_richiesta_di_preventivo_070820.exe	Get hash	malicious	Browse	
	RF172474228ES.exe	Get hash	malicious	Browse	
	MAJDALANI INOX S.A Pedido 050820.exe	Get hash	malicious	Browse	
	MAJDALANI INOX SA Pedido.exe	Get hash	malicious	Browse	
	Correos de Espa#U00f1a Recibo de impresi#U00f3n de paquete retrasado.exe	Get hash	malicious	Browse	
	PDF_Tosoh-Inquiry.exe	Get hash	malicious	Browse	
	Tosoh inquiry list 30072020_PDF.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	tmp2.exe	Get hash	malicious	Browse	• 185.140.53.71
	tmp.exe	Get hash	malicious	Browse	• 185.140.53.71
	NEW_ORDER.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138
	Doc_58YJ54-521DERG701-55YH701.exe	Get hash	malicious	Browse	• 185.140.53.230
	Quotation_Request.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138
	FRQ_05694 revised quantity.exe	Get hash	malicious	Browse	• 185.140.53.69
	INVOICE 15112021.xlsx	Get hash	malicious	Browse	• 185.140.53.130
	URGENT_ORDER.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138
	IMG-001982-AW00173-SSE73I.exe	Get hash	malicious	Browse	• 185.140.53.230
	FYI-Orderimg.exe	Get hash	malicious	Browse	• 185.140.53.67
	Purchase_Order.pdf.exe	Get hash	malicious	Browse	• 185.140.53.138
	PO-94765809570-Order pdf.exe	Get hash	malicious	Browse	• 185.140.53.7
	Commercial E-invoice.exe	Get hash	malicious	Browse	• 185.140.53.137
	Order23032021.xls	Get hash	malicious	Browse	• 185.140.53.130
	ZcQwvgqtuQ.exe	Get hash	malicious	Browse	• 91.193.75.245
	lKIPqaYkKB.exe	Get hash	malicious	Browse	• 185.140.53.161
	t5R60D503x.exe	Get hash	malicious	Browse	• 185.140.53.9
	Purchase OrderDated19032021.xls	Get hash	malicious	Browse	• 185.140.53.130
	0u1JLplwRo.exe	Get hash	malicious	Browse	• 185.140.53.139
	PO-21322.xlsm	Get hash	malicious	Browse	• 185.165.153.116

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Dekont_12VK2102526 VAKIF KATILIM.exe	Get hash	malicious	Browse	
	taiwan.exe	Get hash	malicious	Browse	
	SWIFT COPY.exe	Get hash	malicious	Browse	
	GS_ PO NO.1862021.exe	Get hash	malicious	Browse	
	purchase order.exe	Get hash	malicious	Browse	
	Payment Advice.exe	Get hash	malicious	Browse	
	Quotation.pdf...exe	Get hash	malicious	Browse	
	PURCHASE ORDER.exe	Get hash	malicious	Browse	
	money.exe	Get hash	malicious	Browse	
	TT COPY.exe	Get hash	malicious	Browse	
	$$$.exe	Get hash	malicious	Browse	
	ORDER.exe	Get hash	malicious	Browse	
	PO-0561.exe	Get hash	malicious	Browse	
	Encrypted Documents.exe	Get hash	malicious	Browse	
	Statement of Account.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PURCHASE ORDER COPY.exe	Get hash	malicious	Browse	
	GS_ PO NO.1862021.exe	Get hash	malicious	Browse	
	Wrong_Invoice.exe	Get hash	malicious	Browse	
	REQUEST FOR QUOTAION.exe	Get hash	malicious	Browse	
	New Order.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	768:bBbSoy+SdIBf0k2dsYyV6Iq87PiU9FViaLmf:EoOIBf0ddsYy8LUjVBC
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D B42
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: Dekont_12VK2102526 VAKIF KATILIM.exe, Detection: malicious, Browse • Filename: taiwan.exe, Detection: malicious, Browse • Filename: SWIFT COPY.exe, Detection: malicious, Browse • Filename: GS_ PO NO.1862021.exe, Detection: malicious, Browse • Filename: purchase order.exe, Detection: malicious, Browse • Filename: Payment Advice.exe, Detection: malicious, Browse • Filename: Quotation.pdf...exe, Detection: malicious, Browse • Filename: PURCHASE ORDER.exe, Detection: malicious, Browse • Filename: money.exe, Detection: malicious, Browse • Filename: TT COPY.exe, Detection: malicious, Browse • Filename: $$$.exe, Detection: malicious, Browse • Filename: ORDER.exe, Detection: malicious, Browse • Filename: PO-0561.exe, Detection: malicious, Browse • Filename: Encrypted Documents.exe, Detection: malicious, Browse • Filename: Statement of Account.exe, Detection: malicious, Browse • Filename: PURCHASE ORDER COPY.exe, Detection: malicious, Browse • Filename: GS_ PO NO.1862021.exe, Detection: malicious, Browse • Filename: Wrong_Invoice.exe, Detection: malicious, Browse • Filename: REQUEST FOR QUOTAION.exe, Detection: malicious, Browse • Filename: New Order.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zX.Z.....0..d.....V.... .....@.. .....".. ..`.....O.....8.....r..`>..... ....H.....text...\c... ...d..... ..`.rsrc...8.....f.....@..@.reloc..... .....p.....@..B.....8.....H.....+...S.....\|...P.....r...p(....*2.(....(....*z..r...p(....(....(.....}....*..{....*.s.....*.0..{.....Q.-.s.....+i~....o....(.... s.....o.....r!..p..(....Q.P,:.P.....(....o....o .....(....o!...o".....,..o#...t.....*..0..(..... ....s$.....o%....X..(....-..*.o&...*.0.....('.....&.....*.*.....0.....(.....&.....*..... .....0.....(.....(....~....,.(....~....o....9]...

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ANS_309487487_#049844874.exe.log	
Process:	C:\Users\user\Desktop\ANS_309487487_#049844874.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ANS_309487487_#049844874.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WglAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczlAFXMWTyAGCDLIP12MUAvvw
MD5:	8C0458BB9EA02D50565175E38D577E35
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0F
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

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

C:\Users\user\AppData\Local\Temp\tmp6007.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	5.135668813522653
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mXxtn:cbk4oL600QydbQxIYODOLedq3ZXj
MD5:	8CAD1B41587CED0F1E74396794F31D58
SHA1:	11054BF74FCF5E8E412768035E4DAE43AA7B710F
SHA-256:	3086D914F6B23268F8A12CB1A05516CD5465C2577E1D1E449F1B45C8E5E8F83C
SHA-512:	99C2EF89029DE51A866DF932841684B7FC912DF21E10E2DD0D09E400203BBDC6CBA6319A31780B7BF8B286D2CEA8EA3FC7D084348BF2F002AB4F5A34218CCBF
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\tmp6940.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310

C:\Users\user\AppData\Local\Temp\tmp6940.tmp	
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\tmpDC3C.tmp	
Process:	C:\Users\user\Desktop\ANS_309487487_#049844874.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1651
Entropy (8bit):	5.180198443688216
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBVtn:cbhC7ZlNQF/rydbz9I3YODOLNdq3d
MD5:	F59A4E52C5AF4407199142EDC5E26377
SHA1:	387755BD484FE5E07A8A7657955E9F15D0F08117
SHA-256:	6A9F77E90593E194E33E1F09D2543B640322912192AA07DB8599B5F1D4ED39A8
SHA-512:	3D407381E8E3C6ABE283BFE5DE37C1A2995C81A3C99A728D72A7B62FD56331464428EAD8C19DBC020AC59EB573180284A50D585840C5F87E87345815DD3DC22
Malicious:	**true**
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\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	2088
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrw8:flC0IlC0IlC0IlC0IlC0IlC0IlC0IlCe
MD5:	0D6805D12813A857D50D42D6EE2CCAB0
SHA1:	78D83F009D842F21FE2AB0EAFFD00E5AAD1776F4
SHA-256:	182E0F8AA959549D61C66D049645BA8445D86AEAD2B8C3552A9836FA1E5BD484
SHA-512:	5B29496F3AB3CCB915CF37042F4956BB00E577B5F15457A5A739BE1BD50C481FB7E3297EED575DCA7A7BD30ECBC140DD3666CD7DEDD25DFB7AEB41A1B5BEI A4A
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7.." .hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E..... {...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Pc9t:U
MD5:	19B475F1566BC5B63E8B39713E96CB7B
SHA1:	A3FEBA3421A1F88CDE6AF68D8632DF38C14A3D31

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
SHA-256:	49EE73A5135A3D3F5E3B25060369447755F89024BE23483C13B60FF47F657C4A
SHA-512:	F42BB7118C1E49DF91E55928E6B146B8AC11F7B42932B760E6D12673E0290CFE37F2F463747BDE79044210B04635C26A2AB6C18D036F7FDE35E3A579FA263219
Malicious:	**true**
Preview:	.Id....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.830795005765378
Encrypted:	false
SSDEEP:	3:oMty8WddSWA1KMNn:oMLW6WA1j
MD5:	08E799E8E9B4FDA648F2500A40A11933
SHA1:	AC76B5E20DED247803448A2F586731ED7D84B9F3
SHA-256:	D46E34924067EB071D1F031C0BC015F4B711EDCE64D8AE00F24F29E73ECB71DB
SHA-512:	5C5701A86156D573BE274E73615FD6236AC89630714863A4CB2639EEC8EC1BE746839EBF8A9AEBA0A9BE326AF6FA02D8F9BD7A93D3FFB139BADE945572DF5FE9
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

C:\Users\user\AppData\Roaming\zgEmPmIdAWvDGJ.exe	
Process:	C:\Users\user\Desktop\ANS_309487487_#049844874.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	988672
Entropy (8bit):	7.599577245128144
Encrypted:	false
SSDEEP:	24576:m1izcvE+woErFNL01jT9p6fUyCbTEUSOWPy6bwSc:mU+wBB9S6fFQrSX6g
MD5:	203109AD6D2EFDCA0BF52CAB63A7CE6A
SHA1:	471D5A99A2E8BFE03A9E119B327C45B6994FFAF6
SHA-256:	5E7E5B02D1DE0DA6B91520884A92AF6F7597FD2E39EC5B714BA089815785AD74
SHA-512:	8B567CEEB8EB7158495659687FAD6B74AE8F889604D8CC8AF7BF7FE8A6C4C931EF3622B55A6C7D8C16C5F8C6A25DE398ACBB8A245596DAA94AB3C72A6ACB0F55
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 38%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Xl`.....0.....(.....*.... ... ....@.. ..... ..@.....O.... ...%.....`..... ....H.....text...0.... ....`.rsrc....%... ...&.....@..@.rel oc.....`.....@..B.....H.....g..\Q.....Z...P....P.....0..n.....}.....(.....(.....r...p.(....(....o.....{.....(....o.....{....r...p.(....(....o.....{..... (....o.....*...0..`.....(.....(.....o.....,*....t.....o....r-..p(.....,...o.....+..(....o....(.....+...*.0.....(....o ...o!...o"....+..*...0..;.....(.....(.....o.....,..r-..p.+....t....o#....+..*..0.. ;.....(.....(.....o.....,..r-..p.+....t....o$.

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1141
Entropy (8bit):	4.44831826838854
Encrypted:	false
SSDEEP:	24:zKLXkb4DObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0b4DQntKKH1MqJC
MD5:	1AEB3A784552CFD2AEDEDC1D43A97A4F
SHA1:	804286AB9F8B3DE053222826A69A7CDA3492411A
SHA-256:	0BC438F4B1208E1390C12D375B6CBB08BF47599D1F24BD07799BB1DF384AA293
SHA-512:	5305059BA86D5C2185E590EC036044B2A17ED9FD9863C2E3C7E7D8035EF0C79E53357AF5AE735F7D432BC70156D4BD3ACB42D100CFB05C2FB669EA22368F141
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [options] AssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp Expect an existing application... /tlb:<tlbfile> Filename for the exported type library... /appname:<name> Use the specified name for the target application... /parname:<name> Use the specified name or id for the target partition... /extlb Use an existing type library... /reconfig Re configure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo S uppress logo output... /quiet Suppress logo output and success output... /c

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.599577245128144
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	ANS_309487487_#049844874.exe
File size:	988672
MD5:	203109ad6d2efdca0bf52cab63a7ce6a
SHA1:	471d5a99a2e8bfe03a9e119b327c45b6994ffaf6
SHA256:	5e7e5b02d1de0da6b91520884a92af6f7597fd2e39ec5b714ba089815785ad74
SHA512:	8b567ceeb8eb7158495659687fad6b74ae8f889604d8cc8af7bf7fe8a6c4c931ef3622b55a6c7d8c16c5f8c6a25de398acbb8a245596daa94ab3c72a6acb0f55
SSDEEP:	24576:m1izcvE+woErFNL01jT9p6fUyCbTEUSOWPy6bwSc:mU+wBB9S6fFQrSX6g
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Xl`.....0.....(.....*.... ... .@.. .....@.....

File Icon

Icon Hash:	60c2d2d89484dc1c

Static PE Info

General

Entrypoint:	0x4c0a2a
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:	0x606C5803 [Tue Apr 6 12:45:55 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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	0xc09d8	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc2000	0x325e8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xf6000	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	0xbea30	0xbec00	False	0.93988445077	data	7.9483521266	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc2000	0x325e8	0x32600	False	0.303916912221	data	4.85960749449	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xf6000	0xc	0x200	False	0.041015625	data	0.0776331623432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xc22e0	0x7006	PNG image data, 512 x 512, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xc92e8	0x3580	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		

Name	RVA	Size	Type	Language	Country
RT_ICON	0xcc868	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xdd090	0x94a8	data		
RT_ICON	0xe6538	0x5488	data		
RT_ICON	0xeb9c0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 4294967295, next used block 4294902776		
RT_ICON	0xefbe8	0x25a8	data		
RT_ICON	0xf2190	0x10a8	data		
RT_ICON	0xf3238	0x988	data		
RT_ICON	0xf3bc0	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xf4028	0x92	data		
RT_VERSION	0xf40bc	0x33e	data		
RT_MANIFEST	0xf43fc	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 2013 - 2021
Assembly Version	1.9.0.21
InternalName	U.exe
FileVersion	1.9.0.21
CompanyName	
LegalTrademarks	
Comments	
ProductName	Layered Styler
ProductVersion	1.9.0.21
FileDescription	Layered Styler
OriginalFilename	U.exe

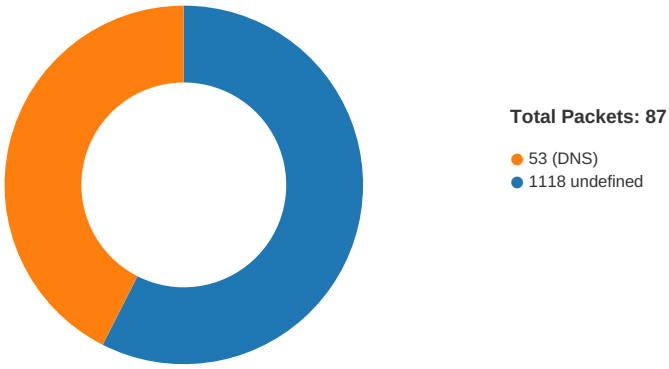
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/07/21-09:06:13.508131	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49709	1118	192.168.2.5	185.140.53.9
04/07/21-09:06:22.447080	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49715	1118	192.168.2.5	185.140.53.9
04/07/21-09:06:28.206968	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49719	1118	192.168.2.5	185.140.53.9
04/07/21-09:06:34.440086	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49720	1118	192.168.2.5	185.140.53.9
04/07/21-09:06:40.461048	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49722	1118	192.168.2.5	185.140.53.9
04/07/21-09:06:46.536426	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49723	1118	192.168.2.5	185.140.53.9
04/07/21-09:06:52.466731	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49724	1118	192.168.2.5	185.140.53.9
04/07/21-09:06:57.696674	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49726	1118	192.168.2.5	185.140.53.9
04/07/21-09:07:20.316455	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49735	1118	192.168.2.5	185.140.53.9
04/07/21-09:07:26.457068	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49736	1118	192.168.2.5	185.140.53.9
04/07/21-09:07:32.604394	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49738	1118	192.168.2.5	185.140.53.9
04/07/21-09:07:41.176968	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49740	1118	192.168.2.5	185.140.53.9

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/07/21-09:07:47.966544	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49741	1118	192.168.2.5	185.140.53.9
04/07/21-09:07:54.950513	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49742	1118	192.168.2.5	185.140.53.9

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 09:06:13.071259022 CEST	49709	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:13.345798016 CEST	1118	49709	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:13.345900059 CEST	49709	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:13.508131027 CEST	49709	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:13.774518013 CEST	1118	49709	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:13.794981003 CEST	1118	49709	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:13.806773901 CEST	49709	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:14.085242033 CEST	1118	49709	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:14.085453987 CEST	49709	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:14.314754009 CEST	1118	49709	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:14.534962893 CEST	49709	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:14.657521009 CEST	49709	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:14.817023039 CEST	49709	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:14.925762892 CEST	1118	49709	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:14.933578014 CEST	49709	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:14.964658976 CEST	1118	49709	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:14.968367100 CEST	49709	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:15.005408049 CEST	1118	49709	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:15.005661964 CEST	49709	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:15.035629034 CEST	1118	49709	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:15.035814047 CEST	49709	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:15.055413008 CEST	1118	49709	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:15.055608988 CEST	49709	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:19.236116886 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:22.348040104 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:22.446363926 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:22.446463108 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:22.447079897 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:22.648147106 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:22.734726906 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:22.735241890 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:22.922859907 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:22.923072100 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:23.121344090 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:23.123116970 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:23.368674040 CEST	1118	49715	185.140.53.9	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 09:06:23.441032887 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:23.453001976 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:23.453195095 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:23.482443094 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:23.494613886 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:23.494749069 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:23.651871920 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:23.663697958 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:23.663873911 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:23.675789118 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:23.696500063 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:23.696646929 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:23.715296984 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:23.723474026 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:23.723654032 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:23.742367983 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:23.754738092 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:23.754905939 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:23.833262920 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:23.870568991 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:23.870687008 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:23.884780884 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:23.884848118 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:23.898178101 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:23.898327112 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:23.911798954 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:23.911887884 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:23.925776958 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:23.925849915 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:23.938056946 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:23.938142061 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:23.964909077 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:23.965002060 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:23.973136902 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:23.973215103 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:23.981427908 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:23.981513977 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:23.994460106 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:23.994529963 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:24.025948048 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:24.026071072 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:24.036422014 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:24.036499023 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:24.061844110 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:24.061902046 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:24.067998886 CEST	1118	49715	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:24.068068027 CEST	49715	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:27.963238001 CEST	49719	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:28.206032038 CEST	1118	49719	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:28.206212044 CEST	49719	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:28.206968069 CEST	49719	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:28.465496063 CEST	1118	49719	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:28.486905098 CEST	1118	49719	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:28.487360001 CEST	49719	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:28.871505022 CEST	1118	49719	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:28.872925043 CEST	49719	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:29.060480118 CEST	1118	49719	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:29.135443926 CEST	49719	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:29.142662048 CEST	1118	49719	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:29.142817974 CEST	49719	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:29.146958113 CEST	1118	49719	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:29.147099972 CEST	49719	1118	192.168.2.5	185.140.53.9
Apr 7, 2021 09:06:29.151454926 CEST	1118	49719	185.140.53.9	192.168.2.5
Apr 7, 2021 09:06:29.151568890 CEST	49719	1118	192.168.2.5	185.140.53.9

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 09:05:43.285545111 CEST	62060	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:05:43.298794031 CEST	53	62060	8.8.8.8	192.168.2.5
Apr 7, 2021 09:05:43.314178944 CEST	65307	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:05:43.327506065 CEST	53	65307	8.8.8.8	192.168.2.5
Apr 7, 2021 09:05:43.362580061 CEST	61805	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:05:43.374855042 CEST	53	61805	8.8.8.8	192.168.2.5
Apr 7, 2021 09:05:47.394865990 CEST	54795	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:05:47.407481909 CEST	53	54795	8.8.8.8	192.168.2.5
Apr 7, 2021 09:05:48.378079891 CEST	49557	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:05:48.393063068 CEST	53	49557	8.8.8.8	192.168.2.5
Apr 7, 2021 09:05:50.323812008 CEST	61733	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:05:50.336774111 CEST	53	61733	8.8.8.8	192.168.2.5
Apr 7, 2021 09:05:55.078866959 CEST	65447	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:05:55.091243029 CEST	53	65447	8.8.8.8	192.168.2.5
Apr 7, 2021 09:06:11.759711027 CEST	52441	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:06:12.778274059 CEST	52441	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:06:12.791774035 CEST	53	52441	8.8.8.8	192.168.2.5
Apr 7, 2021 09:06:13.459623098 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:06:13.477528095 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 7, 2021 09:06:16.342705011 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:06:16.355904102 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 7, 2021 09:06:17.039968014 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:06:17.052984953 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 7, 2021 09:06:17.537570953 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:06:17.550870895 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 7, 2021 09:06:19.049269915 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:06:19.229712009 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 7, 2021 09:06:21.596417904 CEST	56969	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:06:21.608889103 CEST	53	56969	8.8.8.8	192.168.2.5
Apr 7, 2021 09:06:22.647125959 CEST	55161	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:06:22.660080910 CEST	53	55161	8.8.8.8	192.168.2.5
Apr 7, 2021 09:06:24.949235916 CEST	54757	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:06:24.964416981 CEST	53	54757	8.8.8.8	192.168.2.5
Apr 7, 2021 09:06:27.948117018 CEST	49992	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:06:27.961658955 CEST	53	49992	8.8.8.8	192.168.2.5
Apr 7, 2021 09:06:34.214905024 CEST	60075	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:06:34.227855921 CEST	53	60075	8.8.8.8	192.168.2.5
Apr 7, 2021 09:06:35.420773029 CEST	55016	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:06:35.439161062 CEST	53	55016	8.8.8.8	192.168.2.5
Apr 7, 2021 09:06:40.253118992 CEST	64345	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:06:40.266549110 CEST	53	64345	8.8.8.8	192.168.2.5
Apr 7, 2021 09:06:46.295386076 CEST	57128	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:06:46.307823896 CEST	53	57128	8.8.8.8	192.168.2.5
Apr 7, 2021 09:06:52.268774986 CEST	54791	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:06:52.282419920 CEST	53	54791	8.8.8.8	192.168.2.5
Apr 7, 2021 09:06:55.857532024 CEST	50463	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:06:55.890573025 CEST	53	50463	8.8.8.8	192.168.2.5
Apr 7, 2021 09:06:57.263880968 CEST	50394	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:06:57.446436882 CEST	53	50394	8.8.8.8	192.168.2.5
Apr 7, 2021 09:06:58.466825008 CEST	58530	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:06:58.480253935 CEST	53	58530	8.8.8.8	192.168.2.5
Apr 7, 2021 09:06:59.214893103 CEST	53813	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:06:59.227873087 CEST	53	53813	8.8.8.8	192.168.2.5
Apr 7, 2021 09:06:59.622144938 CEST	63732	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:06:59.640738010 CEST	53	63732	8.8.8.8	192.168.2.5
Apr 7, 2021 09:07:03.308799982 CEST	57344	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:07:03.322525978 CEST	53	57344	8.8.8.8	192.168.2.5
Apr 7, 2021 09:07:19.901367903 CEST	54450	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:07:20.084091902 CEST	53	54450	8.8.8.8	192.168.2.5
Apr 7, 2021 09:07:26.252872944 CEST	59261	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:07:26.265705109 CEST	53	59261	8.8.8.8	192.168.2.5
Apr 7, 2021 09:07:30.485004902 CEST	57151	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 7, 2021 09:07:30.497556925 CEST	53	57151	8.8.8.8	192.168.2.5
Apr 7, 2021 09:07:32.351288080 CEST	59413	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:07:32.364850998 CEST	53	59413	8.8.8.8	192.168.2.5
Apr 7, 2021 09:07:36.925448895 CEST	60516	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:07:36.957753897 CEST	53	60516	8.8.8.8	192.168.2.5
Apr 7, 2021 09:07:40.743916988 CEST	51649	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:07:40.926371098 CEST	53	51649	8.8.8.8	192.168.2.5
Apr 7, 2021 09:07:47.746645927 CEST	65086	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:07:47.759985924 CEST	53	65086	8.8.8.8	192.168.2.5
Apr 7, 2021 09:07:54.722879887 CEST	56432	53	192.168.2.5	8.8.8.8
Apr 7, 2021 09:07:54.735752106 CEST	53	56432	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 7, 2021 09:06:11.759711027 CEST	192.168.2.5	8.8.8.8	0x2a45	Standard query (0)	myhustle.duckdns.org	A (IP address)	IN (0x0001)
Apr 7, 2021 09:06:12.778274059 CEST	192.168.2.5	8.8.8.8	0x2a45	Standard query (0)	myhustle.duckdns.org	A (IP address)	IN (0x0001)
Apr 7, 2021 09:06:19.049269915 CEST	192.168.2.5	8.8.8.8	0xb260	Standard query (0)	myhustle.duckdns.org	A (IP address)	IN (0x0001)
Apr 7, 2021 09:06:27.948117018 CEST	192.168.2.5	8.8.8.8	0x3471	Standard query (0)	myhustle.duckdns.org	A (IP address)	IN (0x0001)
Apr 7, 2021 09:06:34.214905024 CEST	192.168.2.5	8.8.8.8	0xd042	Standard query (0)	myhustle.duckdns.org	A (IP address)	IN (0x0001)
Apr 7, 2021 09:06:40.253118992 CEST	192.168.2.5	8.8.8.8	0x64aa	Standard query (0)	myhustle.duckdns.org	A (IP address)	IN (0x0001)
Apr 7, 2021 09:06:46.295386076 CEST	192.168.2.5	8.8.8.8	0x8f51	Standard query (0)	myhustle.duckdns.org	A (IP address)	IN (0x0001)
Apr 7, 2021 09:06:52.268774986 CEST	192.168.2.5	8.8.8.8	0xd64	Standard query (0)	myhustle.duckdns.org	A (IP address)	IN (0x0001)
Apr 7, 2021 09:06:57.263880968 CEST	192.168.2.5	8.8.8.8	0x3a08	Standard query (0)	myhustle.duckdns.org	A (IP address)	IN (0x0001)
Apr 7, 2021 09:07:03.308799982 CEST	192.168.2.5	8.8.8.8	0x99f4	Standard query (0)	myhustle.duckdns.org	A (IP address)	IN (0x0001)
Apr 7, 2021 09:07:19.901367903 CEST	192.168.2.5	8.8.8.8	0xe1c9	Standard query (0)	myhustle.duckdns.org	A (IP address)	IN (0x0001)
Apr 7, 2021 09:07:26.252872944 CEST	192.168.2.5	8.8.8.8	0xd4b6	Standard query (0)	myhustle.duckdns.org	A (IP address)	IN (0x0001)
Apr 7, 2021 09:07:32.351288080 CEST	192.168.2.5	8.8.8.8	0xfd97	Standard query (0)	myhustle.duckdns.org	A (IP address)	IN (0x0001)
Apr 7, 2021 09:07:40.743916988 CEST	192.168.2.5	8.8.8.8	0x4306	Standard query (0)	myhustle.duckdns.org	A (IP address)	IN (0x0001)
Apr 7, 2021 09:07:47.746645927 CEST	192.168.2.5	8.8.8.8	0x1b09	Standard query (0)	myhustle.duckdns.org	A (IP address)	IN (0x0001)
Apr 7, 2021 09:07:54.722879887 CEST	192.168.2.5	8.8.8.8	0x43d1	Standard query (0)	myhustle.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

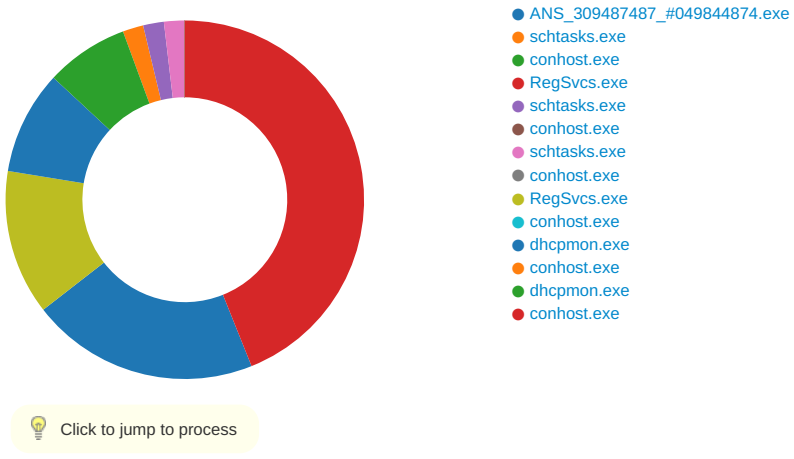
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 7, 2021 09:06:12.791774035 CEST	8.8.8.8	192.168.2.5	0x2a45	No error (0)	myhustle.duckdns.org		185.140.53.9	A (IP address)	IN (0x0001)
Apr 7, 2021 09:06:19.229712009 CEST	8.8.8.8	192.168.2.5	0xb260	No error (0)	myhustle.duckdns.org		185.140.53.9	A (IP address)	IN (0x0001)
Apr 7, 2021 09:06:27.961658955 CEST	8.8.8.8	192.168.2.5	0x3471	No error (0)	myhustle.duckdns.org		185.140.53.9	A (IP address)	IN (0x0001)
Apr 7, 2021 09:06:34.227855921 CEST	8.8.8.8	192.168.2.5	0xd042	No error (0)	myhustle.duckdns.org		185.140.53.9	A (IP address)	IN (0x0001)
Apr 7, 2021 09:06:40.266549110 CEST	8.8.8.8	192.168.2.5	0x64aa	No error (0)	myhustle.duckdns.org		185.140.53.9	A (IP address)	IN (0x0001)
Apr 7, 2021 09:06:46.307823896 CEST	8.8.8.8	192.168.2.5	0x8f51	No error (0)	myhustle.duckdns.org		185.140.53.9	A (IP address)	IN (0x0001)
Apr 7, 2021 09:06:52.282419920 CEST	8.8.8.8	192.168.2.5	0xd64	No error (0)	myhustle.duckdns.org		185.140.53.9	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 7, 2021 09:06:57.446436882 CEST	8.8.8.8	192.168.2.5	0x3a08	No error (0)	myhustle.duckdns.org		185.140.53.9	A (IP address)	IN (0x0001)
Apr 7, 2021 09:07:03.322525978 CEST	8.8.8.8	192.168.2.5	0x99f4	No error (0)	myhustle.duckdns.org		185.140.53.9	A (IP address)	IN (0x0001)
Apr 7, 2021 09:07:20.084091902 CEST	8.8.8.8	192.168.2.5	0xe1c9	No error (0)	myhustle.duckdns.org		185.140.53.9	A (IP address)	IN (0x0001)
Apr 7, 2021 09:07:26.265705109 CEST	8.8.8.8	192.168.2.5	0xd4b6	No error (0)	myhustle.duckdns.org		185.140.53.9	A (IP address)	IN (0x0001)
Apr 7, 2021 09:07:32.364850998 CEST	8.8.8.8	192.168.2.5	0xfd97	No error (0)	myhustle.duckdns.org		185.140.53.9	A (IP address)	IN (0x0001)
Apr 7, 2021 09:07:40.926371098 CEST	8.8.8.8	192.168.2.5	0x4306	No error (0)	myhustle.duckdns.org		185.140.53.9	A (IP address)	IN (0x0001)
Apr 7, 2021 09:07:47.759985924 CEST	8.8.8.8	192.168.2.5	0x1b09	No error (0)	myhustle.duckdns.org		185.140.53.9	A (IP address)	IN (0x0001)
Apr 7, 2021 09:07:54.735752106 CEST	8.8.8.8	192.168.2.5	0x43d1	No error (0)	myhustle.duckdns.org		185.140.53.9	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: ANS_309487487_#049844874.exe PID: 5688 Parent PID: 5840

General

Start time:	09:05:49
Start date:	07/04/2021
Path:	C:\Users\user\Desktop\ANS_309487487_#049844874.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\Desktop\ANS_309487487_#049844874.exe'
Imagebase:	0xdc0000
File size:	988672 bytes
MD5 hash:	203109AD6D2EFDCA0BF52CAB63A7CE6A
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: 00000000.00000002.245770427.0000000004612000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.245770427.0000000004612000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.245770427.0000000004612000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.245029737.0000000004459000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.245029737.0000000004459000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.245029737.0000000004459000.00000004.00000001.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	6DCCCF06	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	6DCCCF06	unknown
C:\Users\user\AppData\Roaming\zgEmPmIdAWvDGJ.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CB11E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpDC3C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CB17038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ANS_309487487_#049844874.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DFDC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpDC3C.tmp	success or wait	1	6CB16A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\zgEmPmIdAWvDGJ.exe	unknown	988672	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 03 58 6c 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 ec 0b 00 00 28 03 00 00 00 00 00 2a 0a 0c 00 00 20 00 00 00 20 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 0f 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....Xl`.......... ....0......(......*.... ... .@.. ....@................	success or wait	1	6CB11B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmpDC3C.tmp	unknown	1651	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.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationI	success or wait	1	6CB11B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ANS_309487487_#049844874.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 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 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DFDC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB11B4F	ReadFile
C:\Users\user\Desktop\ANS_309487487_#049844874.exe	unknown	988672	success or wait	1	6CB11B4F	ReadFile

Analysis Process: schtasks.exe PID: 4012 Parent PID: 5688

General

Start time:	09:06:00
Start date:	07/04/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\zgEmPmIdAWvDGJ' /XML 'C:\Users\user\AppData\Local\Temp\tmpDC3C.tmp'
Imagebase:	0x13c0000
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\tmpDC3C.tmp	unknown	2	success or wait	1	13CAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpDC3C.tmp	unknown	1652	success or wait	1	13CABD9	ReadFile

Analysis Process: conhost.exe PID: 5592 Parent PID: 4012

General

Start time:	09:06:00
Start date:	07/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 5404 Parent PID: 5688

General

Start time:	09:06:01
Start date:	07/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xc60000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.497078079.0000000006CF0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.497078079.0000000006CF0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.497210658.0000000006D50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.497210658.0000000006D50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.497223355.0000000006D60000.00000004.00000001.sdmp, Author: Florian Roth

- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.497223355.0000000006D60000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.484801611.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.484801611.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000002.484801611.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.496231866.0000000006570000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.496231866.0000000006570000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.496231866.0000000006570000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000002.492533618.0000000004168000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.497316492.0000000006DB0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.497316492.0000000006DB0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.497195825.0000000006D40000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.497195825.0000000006D40000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.497368728.0000000006DF0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.497368728.0000000006DF0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.497254796.0000000006D80000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.497254796.0000000006D80000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.495352573.0000000005810000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.495352573.0000000005810000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.493121486.00000000043CC000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000002.493121486.00000000043CC000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.488658155.0000000002FA1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.497240382.0000000006D70000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.497240382.0000000006D70000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.497299959.0000000006DA0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.497299959.0000000006DA0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.490957634.0000000003FE9000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000002.490957634.0000000003FE9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.496076693.00000000064E0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.496076693.00000000064E0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.497154583.0000000006D20000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source:

	00000004.00000002.497154583.0000000006D20000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.497176371.0000000006D30000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.497176371.0000000006D30000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCCCF06	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	6DCCCF06	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	6CB1BEFF	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	6CB11E60	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	6CB1BEFF	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	6CB1DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp6007.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CB17038	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	6CB11E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp6940.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CB17038	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	6CB1BEFF	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	6CB1BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	10	6CB11E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp6007.tmp	success or wait	1	6CB16A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp6940.tmp	success or wait	1	6CB16A95	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	06 49 64 0c df f9 d8 48	.Id....H	success or wait	1	6CB11B4F	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	45152	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 7a 58 8e 5a 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 64 00 00 00 0c 00 00 00 00 00 00 56 83 00 00 00 20 00 00 00 a0 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 e0 00 00 00 02 00 00 a9 22 01 00 03 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...zX.Z.......... ....0..d..........V.... ....@.. ...."....`................	success or wait	1	6CB1DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp6007.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	6CB11B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 34 2e 30 2e 33 30 33 31 39 5c 52 65 67 53 76 63 73 2e 65 78 65	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe	success or wait	1	6CB11B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp6940.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 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 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	6CB11B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	Gj.h\.3..A...5.x..&...i+...c(1.P..P.cLT....A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V.....B.....].P...W.4C}uL.....s~..F...}.....E.....E....6E.....{....{..yS...7..".hK.!.x.2..i...zJ.... ....f...?._...0.:e[7w{1.!.4.....&.	success or wait	9	6CB11B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6DCA5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6DCACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6DCACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4096	end of file	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0 .0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6DC8D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0 .0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6DC8D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe	unknown	4096	success or wait	1	6DC8D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe	unknown	512	success or wait	1	6DC8D72F	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0 .0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	6DC8D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0 .0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6DC8D72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WO W6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Mo nitor\dhcpmon.exe	success or wait	1	6CB1646A	RegSetValueExW

Analysis Process: schtasks.exe PID: 4904 Parent PID: 5404

General

Start time:	09:06:06
Start date:	07/04/2021
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\tmp600 7.tmp'
Imagebase:	0xdd0000
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\tmp6007.tmp	unknown	2	success or wait	1	DDAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp6007.tmp	unknown	1321	success or wait	1	DDABD9	ReadFile

Analysis Process: conhost.exe PID: 5864 Parent PID: 4904

General

Start time:	09:06:07
Start date:	07/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 4132 Parent PID: 5404

General

Start time:	09:06:08
Start date:	07/04/2021
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\tmp6940.tmp'
Imagebase:	0x7ff797770000
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\tmp6940.tmp	unknown	2	success or wait	1	DDAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp6940.tmp	unknown	1311	success or wait	1	DDABD9	ReadFile

Analysis Process: conhost.exe PID: 4500 Parent PID: 4132

General

Start time:	09:06:09
Start date:	07/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 5400 Parent PID: 904

General

Start time:	09:06:10
Start date:	07/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe 0
Imagebase:	0xb30000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DFDC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	6CB11B4F	WriteFile
\Device\ConDrv	unknown	141	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 53 65 72 76 69 63 65 73 20 49 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 56 65 72 73 69 6f 6e 20 34 2e 37 2e 33 30 35 36 2e 30 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....	success or wait	1	6CB11B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\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	6CB11B4F	WriteFile
\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	6CB11B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log	unknown	142	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 45 6e 74 65 72 70 72 69 73 65 53 65 72 76 69 63 65 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..	success or wait	1	6DFDC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	4095	success or wait	1	6DCACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\regsvcs.exe.config	unknown	8173	end of file	1	6DCACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCACA54	ReadFile

Analysis Process: conhost.exe PID: 5564 Parent PID: 5400

General

Start time:	09:06:11
Start date:	07/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 5824 Parent PID: 904

General

Start time:	09:06:11
Start date:	07/04/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x40000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DFDC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	6CB11B4F	WriteFile
\Device\ConDrv	unknown	141	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 53 65 72 76 69 63 65 73 20 49 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 56 65 72 73 69 6f 6e 20 34 2e 37 2e 33 30 35 36 2e 30 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....	success or wait	1	6CB11B4F	WriteFile
\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	6CB11B4F	WriteFile
\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	6CB11B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	unknown	142	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 45 6e 74 65 72 70 72 69 73 65 53 65 72 76 69 63 65 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..	success or wait	1	6DFDC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCACA54	ReadFile

Analysis Process: conhost.exe PID: 5864 Parent PID: 5824

General

Start time:	09:06:11
Start date:	07/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 6360 Parent PID: 3472

General

Start time:	09:06:19
Start date:	07/04/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x2a0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	6CB11B4F	WriteFile
\Device\ConDrv	unknown	141	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 53 65 72 76 69 63 65 73 20 49 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 55 74 69 6c 69 74 79 20 56 65 72 73 69 6f 6e 20 34 2e 37 2e 33 30 35 36 2e 30 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....	success or wait	1	6CB11B4F	WriteFile
\Device\ConDrv	unknown	256	55 53 41 47 45 3a 20 72 65 67 73 76 63 73 2e 65 78 65 20 5b 6f 70 74 69 6f 6e 73 5d 20 41 73 73 65 6d 62 6c 79 4e 61 6d 65 0d 0a 4f 70 74 69 6f 6e 73 3a 0d 0a 20 20 20 20 2f 3f 20 6f 72 20 2f 68 65 6c 70 20 20 20 20 20 44 69 73 70 6c 61 79 20 74 68 69 73 20 75 73 61 67 65 20 6d 65 73 73 61 67 65 2e 0d 0a 20 20 20 20 2f 66 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 46 69 6e 64 20 6f 72 20 63 72 65 61 74 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 28 64 65 66 61 75 6c 74 29 2e 0d 0a 20 20 20 20 2f 63 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 43 72 65 61 74 65 20 74 61 72 67 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 2c 20 65 72 72 6f 72 20 69 66 20 69 74 20 61 6c 72 65 61 64 79 20 65 78 69 73 74 73 2e 0d 0a 20 20 20 20 2f 65 78 61 70 70 20	USAGE: regsvcs.exe [options] A ssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp	success or wait	3	6CB11B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	232	53 75 70 70 72 65 73 73 20 6c 6f 67 6f 20 6f 75 74 70 75 74 2e 0d 0a 20 20 20 20 2f 71 75 69 65 74 20 20 20 20 20 20 20 20 20 20 53 75 70 70 72 65 73 73 20 6c 6f 67 6f 20 6f 75 74 70 75 74 20 61 6e 64 20 73 75 63 63 65 73 73 20 6f 75 74 70 75 74 2e 0d 0a 20 20 20 20 2f 63 6f 6d 70 6f 6e 6c 79 20 20 20 20 20 20 20 20 43 6f 6e 66 69 67 75 72 65 20 63 6f 6d 70 6f 6e 65 6e 74 73 20 6f 6e 6c 79 2c 20 6e 6f 20 6d 65 74 68 6f 64 73 20 6f 72 20 69 6e 74 65 72 66 61 63 65 73 2e 0d 0a 20 20 20 20 2f 61 70 70 64 69 72 3a 3c 70 61 74 68 3e 20 20 53 65 74 20 61 70 70 6c 69 63 61 74 69 6f 6e 20 72 6f 6f 74 20 64 69 72 65 63 74 6f 72 79 20 74 6f 20 73 70 65 63 69 66 69 65 64 20 70 61 74 68 2e 0d 0a 0d 0a	Suppress logo output... /quiet Suppress logo output and success output... /componly Configure components only, no methods or interfaces... /appdir:<path> Set application root directory to specified path.....	success or wait	1	6CB11B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCACA54	ReadFile

Analysis Process: conhost.exe PID: 6368 Parent PID: 6360

General

Start time:	09:06:19
Start date:	07/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis