ID: 713039
Sample Name:
Scancontract103.exe
Cookbook: default.jbs
Time: 22:57:49
Date: 29/09/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

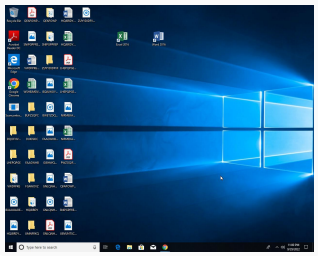
Windows Analysis Report

Scancontract103.exe

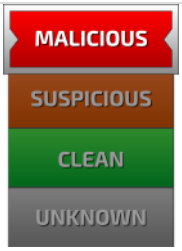
Overview

General Information

Sample Name:	Scancontract103.exe
Analysis ID:	713039
MD5:	9d2a2b596cd979..
SHA1:	015e8ae0f838e0..
SHA256:	c4a2c953833c8d..
Tags:	exe NanoCore RAT
Infos:	



Detection



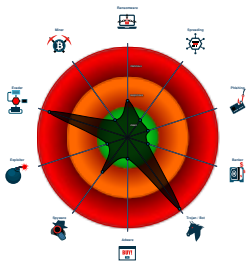
Nanocore

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Sigma detected: Scheduled temp fil…
- Multi AV Scanner detection for dom…
- Yara detected Nanocore RAT
- Protects its processes via BreakOn…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- Scancontract103.exe (PID: 3732 cmdline: "C:\Users\user\Desktop\Scancontract103.exe" MD5: 9D2A2B596CD979FC9674824D2AA731DF)
  - Scancontract103.exe (PID: 1760 cmdline: {path} MD5: 9D2A2B596CD979FC9674824D2AA731DF)
    - schtasks.exe (PID: 2636 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmpCA7.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 4744 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 2300 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp1090.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5056 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Scancontract103.exe (PID: 6052 cmdline: C:\Users\user\Desktop\Scancontract103.exe 0 MD5: 9D2A2B596CD979FC9674824D2AA731DF)
  - Scancontract103.exe (PID: 3988 cmdline: {path} MD5: 9D2A2B596CD979FC9674824D2AA731DF)
  - Scancontract103.exe (PID: 5588 cmdline: {path} MD5: 9D2A2B596CD979FC9674824D2AA731DF)
- dhcpmon.exe (PID: 5308 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: 9D2A2B596CD979FC9674824D2AA731DF)
  - dhcpmon.exe (PID: 4632 cmdline: {path} MD5: 9D2A2B596CD979FC9674824D2AA731DF)
  - dhcpmon.exe (PID: 2576 cmdline: {path} MD5: 9D2A2B596CD979FC9674824D2AA731DF)
- dhcpmon.exe (PID: 1012 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 9D2A2B596CD979FC9674824D2AA731DF)
  - dhcpmon.exe (PID: 2300 cmdline: {path} MD5: 9D2A2B596CD979FC9674824D2AA731DF)
  - dhcpmon.exe (PID: 5420 cmdline: {path} MD5: 9D2A2B596CD979FC9674824D2AA731DF)
  - dhcpmon.exe (PID: 408 cmdline: {path} MD5: 9D2A2B596CD979FC9674824D2AA731DF)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "c5cb65e3-79c3-43dc-bde0-43ed679c",
  "Group": "Default",
  "Domain1": "79.134.225.6",
  "Domain2": "",
  "Port": 60110,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Enable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Enable",
  "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 Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.547986042.0000000005900000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000006.00000002.547986042.0000000005900000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
00000006.00000002.547986042.0000000005900000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xe38:$x2: NanoCore.ClientPlugin • 0xe75:$x3: NanoCore.ClientPluginHost • 0xe5a:$i1: IClientApp • 0xe4e:$i2: IClientData • 0xe29:$i3: IClientNetwork • 0xec3:$i4: IClientAppHost • 0xe65:$i5: IClientDataHost • 0xeb0:$i6: IClientLoggingHost • 0xe8f:$i7: IClientNetworkHost • 0xea2:$i8: IClientUIHost • 0xed2:$i9: IClientNameObjectCollection • 0xef7:$i10: IClientReadOnlyNameObjectCollection • 0xe41:$s1: ClientPlugin • 0x177c:$s1: ClientPlugin • 0x1789:$s1: ClientPlugin • 0x11f9:$s6: get_ClientSettings • 0x1249:$s7: get_Connected
00000006.00000002.547986042.0000000005900000.00000004.08000000.00040000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xe75:$a1: NanoCore.ClientPluginHost • 0xe38:$a2: NanoCore.ClientPlugin • 0x120c:$b1: get_BuilderSettings • 0xec3:$b4: IClientAppHost • 0x127d:$b6: AddHostEntry • 0x12ec:$b7: LogClientException • 0x1261:$b8: PipeExists • 0xeb0:$b9: IClientLoggingHost
00000010.00000002.400735152.000000000334B000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 49 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
20.2.Scancontract103.exe.33695a4.0.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
20.2.Scancontract103.exe.33695a4.0.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
20.2.Scancontract103.exe.33695a4.0.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xe38:$x2: NanoCore.ClientPlugin • 0xe75:$x3: NanoCore.ClientPluginHost • 0xe5a:$i1: IClientApp • 0xe4e:$i2: IClientData • 0xe29:$i3: IClientNetwork • 0xec3:$i4: IClientAppHost • 0xe65:$i5: IClientDataHost • 0xeb0:$i6: IClientLoggingHost • 0xe8f:$i7: IClientNetworkHost • 0xea2:$i8: IClientUIHost • 0xed2:$i9: IClientNameObjectCollection • 0xef7:$i10: IClientReadOnlyNameObjectCollection • 0xe41:$s1: ClientPlugin • 0x177c:$s1: ClientPlugin • 0x1789:$s1: ClientPlugin • 0x11f9:$s6: get_ClientSettings • 0x1249:$s7: get_Connected
20.2.Scancontract103.exe.33695a4.0.raw.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xe75:$a1: NanoCore.ClientPluginHost • 0xe38:$a2: NanoCore.ClientPlugin • 0x120c:$b1: get_BuilderSettings • 0xec3:$b4: IClientAppHost • 0x127d:$b6: AddHostEntry • 0x12ec:$b7: LogClientException • 0x1261:$b8: PipeExists • 0xeb0:$b9: IClientLoggingHost
21.2.dhcpmon.exe.2dc9658.0.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
Click to see the 69 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Nanocore RAT

Operating System Destruction

Protects its processes via BreakOnTermination flag

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

Data Obfuscation

.NET source code contains potential unpacker

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

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

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

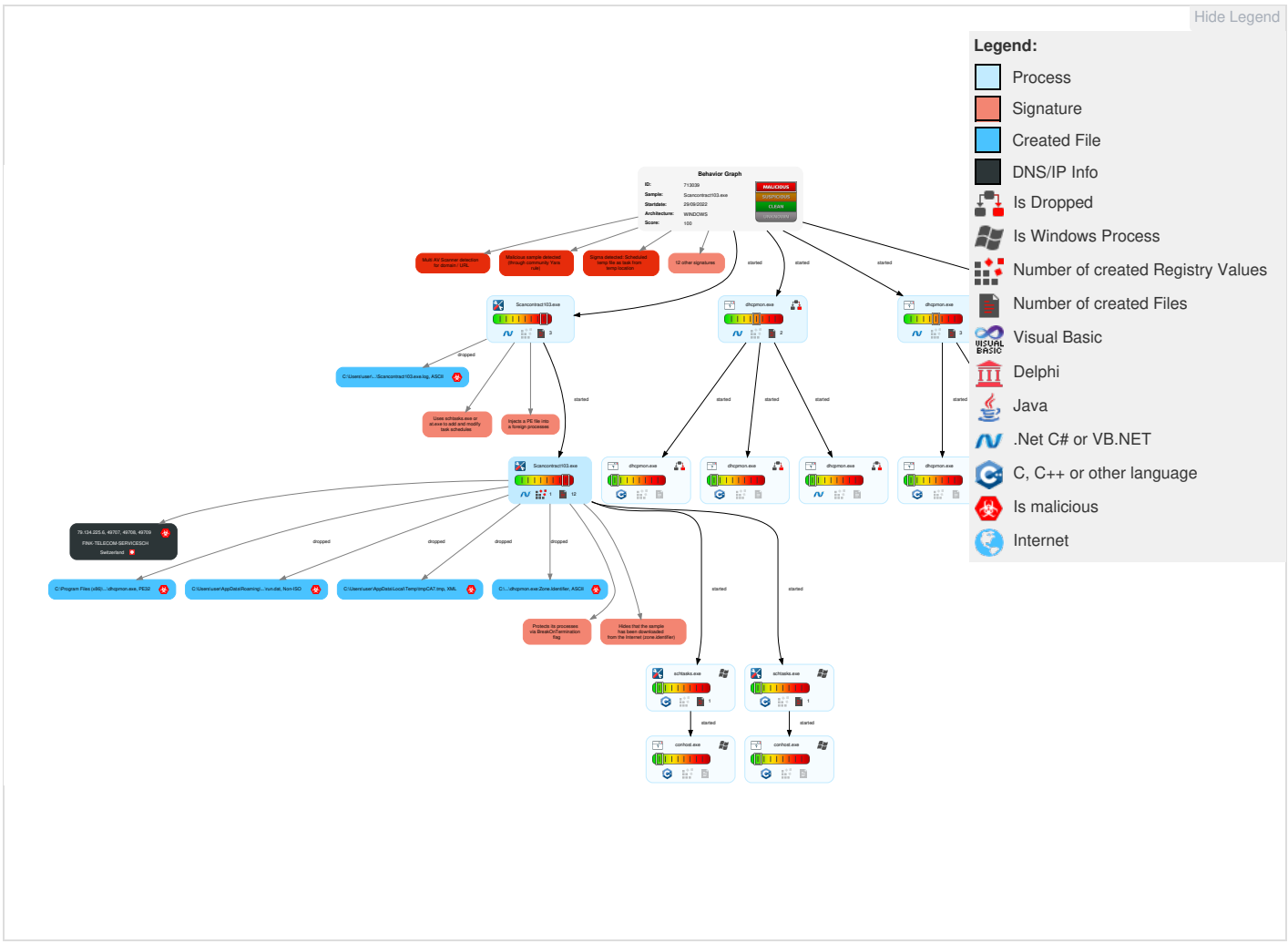
Detected Nanocore Rat

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	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scheduled Task/Job	1 Scheduled Task/Job	1 1 2 Process Injection	2 Masquerading	2 1 Input Capture	1 1 Security Software Discovery	Remote Services	2 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 2 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 2 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

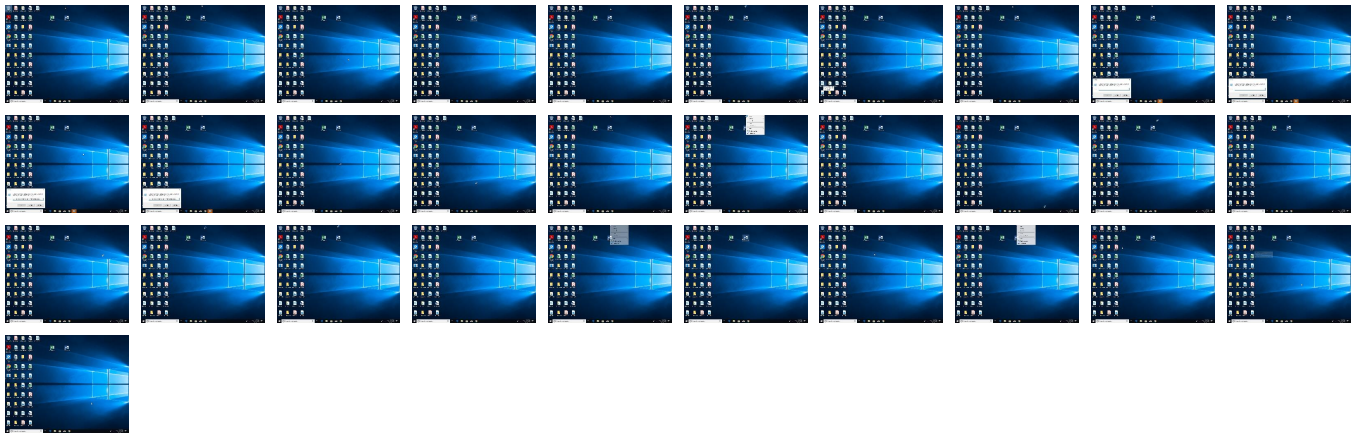
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Scancontract103.exe	40%	Virustotal		Browse
Scancontract103.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.Scancontract103.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.2.Scancontract103.exe.5910000.4.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fonts.comc	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cna-d	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://en.wikip	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comoitu	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.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
79.134.225.6	7%	Virustotal		Browse
http://www.sakkal.com	0%	URL Reputation	safe	
79.134.225.6	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cntyp9	0%	Avira URL Cloud	safe	
http://www.fontbureau.commv	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
79.134.225.6	true	• 7%, Virustotal, Browse • Avira URL Cloud: safe	unknown

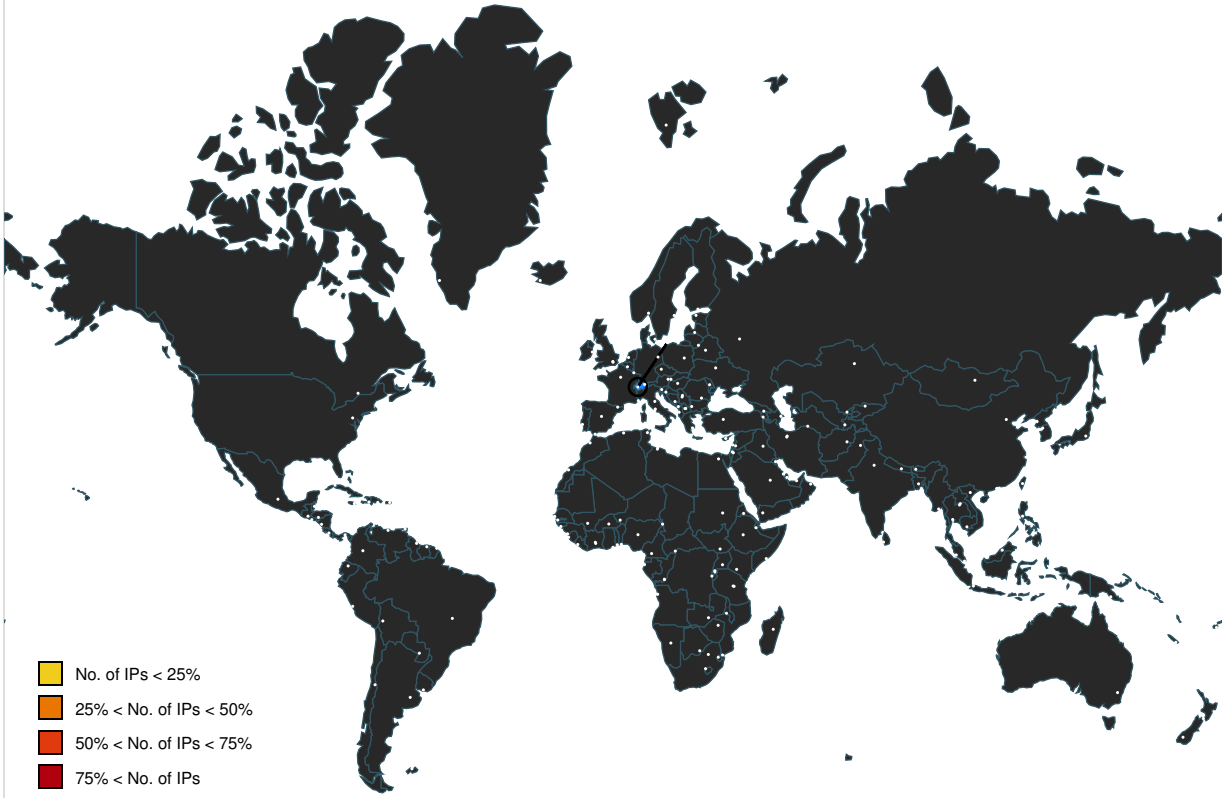
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	Scancontract103.exe, 00000000.00000002.3 18121730.0000000006C12000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Scancontract103.exe, 00000000.00000002.3 18121730.0000000006C12000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	Scancontract103.exe, 00000000.00000002.3 18121730.0000000006C12000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/	Scancontract103.exe, 00000000.00000003.2 72557005.00000000059C6000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	Scancontract103.exe, 00000000.00000002.3 18121730.0000000006C12000.00000004.00000 800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.comc	Scancontract103.exe, 00000000.00000003.2 60309270.00000000059A3000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/bThe	Scancontract103.exe, 00000000.00000002.3 18121730.0000000006C12000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Scancontract103.exe, 00000000.00000002.3 18121730.0000000006C12000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cntyp9	Scancontract103.exe, 00000000.00000003.2 63335099.0000000005985000.00000004.00000 800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cna-d	Scancontract103.exe, 00000000.00000003.2 63335099.0000000005985000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	Scancontract103.exe, 00000000.00000002.3 18121730.0000000006C12000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Scancontract103.exe, 00000000.00000002.3 18121730.0000000006C12000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	Scancontract103.exe, 00000000.00000002.3 18121730.0000000006C12000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://en.wikip	Scancontract103.exe, 00000000.00000003.2 65302103.000000000598D000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	Scancontract103.exe, 00000000.00000002.3 18121730.0000000006C12000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	Scancontract103.exe, 00000000.00000002.3 18121730.0000000006C12000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	Scancontract103.exe, 00000000.00000002.3 18121730.0000000006C12000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Scancontract103.exe, 00000000.00000002.3 18121730.0000000006C12000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Scancontract103.exe, 00000000.00000002.3 18121730.0000000006C12000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Scancontract103.exe, 00000000.00000002.3 18121730.0000000006C12000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Scancontract103.exe, 00000000.00000002.3 18121730.0000000006C12000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Scancontract103.exe, 00000000.00000003.2 63528849.0000000005986000.00000004.00000 800.00020000.00000000.sdmp, Scancontract103.exe, 00000000.00000003.263806579.000000000598E 000.00000004.00000800.00020000.00000000.sdmp, Scancontract103.exe, 00000000.00000002.31812 1730.0000000006C12000.00000004.00000800. 00020000.00000000.sdmp, Scancontract103.exe, 00000000.00000003.263335099.0000000005985000. 00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	Scancontract103.exe, 00000000.00000002.3 18121730.0000000006C12000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comoitu	Scancontract103.exe, 00000000.00000003.3 01534585.0000000005980000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	Scancontract103.exe, 00000000.00000002.3 18121730.0000000006C12000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Scancontract103.exe, 00000000.00000002.3 18121730.0000000006C12000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Scancontract103.exe, 00000000.00000002.3 18121730.0000000006C12000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.ascendercorp.com/typedesigners.html	Scancontract103.exe, 00000000.00000003.2 66935495.0000000005989000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	Scancontract103.exe, 00000000.00000002.3 18121730.0000000006C12000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Scancontract103.exe, 00000000.00000002.3 18121730.0000000006C12000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Scancontract103.exe, 00000000.00000002.3 18121730.0000000006C12000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Scancontract103.exe, 00000000.00000002.3 18121730.0000000006C12000.00000004.00000 800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.commv	Scancontract103.exe, 00000000.00000003.3 01534585.0000000005980000.00000004.00000 800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Scancontract103.exe, 00000006.00000002.5 30169744.0000000002E21000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	Scancontract103.exe, 00000000.00000003.2 66747836.00000000059C6000.00000004.00000 800.00020000.00000000.sdmp, Scancontract103.exe, 00000000.00000002.318121730.0000000006C12 000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/	Scancontract103.exe, 00000000.00000003.2 69009492.00000000059C5000.00000004.00000 800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.6	unknown	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	713039
Start date and time:	2022-09-29 22:57:49 +02:00

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Scancontract103.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	27
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@26/8@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): fs.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
22:58:48	API Interceptor	969x Sleep call for process: Scancontract103.exe modified
22:59:13	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
22:59:16	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\Scancontract103.exe" s>$(Arg0)
22:59:16	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
22:59:26	API Interceptor	255x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\Scancontract103.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	854528
Entropy (8bit):	7.084655686253337
Encrypted:	false
SSDEEP:	12288:sx9l2iNl/joW7EsJ2uM1DgC9tqGdpb5QyXYzvtMdADqjJ5ns:N1fEW7T4RDgvGdpHYzQjrs
MD5:	9D2A2B596CD979FC9674824D2AA731DF
SHA1:	015E8AE0F838E0FBA35643297530A5B9A66E4186
SHA-256:	C4A2C953833C8D6B5D2EF71B997700559ECC9F23573D89072D205F963E46956C
SHA-512:	768843F52697AC5A8E8FF71FF5A66BCA977CC6FAD9DA349CE77EEE431AA5252EC07187D52BCE92BD50BBCEC1A10B6CE1A9123DBAFA1E34D7A36AC2A9E511CEF3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....5c.....P..... ... .@.. .....`..... ..@.....O.... .....@..... ..... ..H.....text..... ..... ..`.rsrc..... .....@..@.rel oc.....@.....@..B.....H.....Z...W.....;..\|....a.....(....*&..(.....*.s.....s .....s!.....s".....s#.....*...0.....~....o$....+..*.0..... .....~....o%....+..*.0.....~....o&....+..*.0.....~....o'....+..*.0.....~....o(....+..*.0..<.....~.....()....,!r...p.....(*...o+...s,.....~.....+..*.0.....~.....+..*".....*.0..&.....(....r/..p~....o-...(.....t$....+..*...0..&.....(....rA..p~....o-...(.....

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

Process:	C:\Users\user\Desktop\Scancontract103.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Scancontract103.exe.log

Process:	C:\Users\user\Desktop\Scancontract103.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1302
Entropy (8bit):	5.3499841584777394
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84bE4KnKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxvbHKnYHKhQnoPtHoxH5
MD5:	A7D610296B11732FD61A88BC218783AC

SHA1:	EE89E72AF3A15DAB847055A9F9F88FD934113857
SHA-256:	7F3A7CE69B42D8C832F0FBB57C0523D6F098DC090D39616C05277F8DB9F4F9E9
SHA-512:	8C0AC1893FF0A7FE287D4FC650943D33D1546200A89C2A502FE9BCB11DA6227533FD8F966EE8651B7E7BD8B5EA11403AD930D022D1D75B3EAA6D24D625F779F
Malicious:	**true**
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..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",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.Configu

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:	dropped
Size (bytes):	1302
Entropy (8bit):	5.3499841584777394
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84bE4KnKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxvbHKnYHKhQnoPtHoxH5
MD5:	A7D610296B11732FD61A88BC218783AC
SHA1:	EE89E72AF3A15DAB847055A9F9F88FD934113857
SHA-256:	7F3A7CE69B42D8C832F0FBB57C0523D6F098DC090D39616C05277F8DB9F4F9E9
SHA-512:	8C0AC1893FF0A7FE287D4FC650943D33D1546200A89C2A502FE9BCB11DA6227533FD8F966EE8651B7E7BD8B5EA11403AD930D022D1D75B3EAA6D24D625F779F
Malicious:	false
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..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",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.Configu

C:\Users\user\AppData\Local\Temp\tmp1090.tmp

Process:	C:\Users\user\Desktop\Scancontract103.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755734
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\tmpCA7.tmp

Process:	C:\Users\user\Desktop\Scancontract103.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1305
Entropy (8bit):	5.103232147891814
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0hxtn:cbk4oL600QydbQxIYODOLedq3lj

MD5:	965D081052473031B1DA64E2A9CA6356
SHA1:	2CE6D29C2C4C5E0AAF98B74E3661A7C8A214B554
SHA-256:	81A542AC638DC1591CE04076330AAC190AA871FCD83AD2F3AB3C758BF6BB7713
SHA-512:	27338E725AB8992E95A77425347AED5878829AAEBBBFF14348E610DB2F8255F812CDAA636E11B1128C1637C982C4B8E58E670FD8D4F97E6694C8A4EDE849A8B4
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 />.. <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\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat

Process:	C:\Users\user\Desktop\Scancontract103.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:YRH/t:Yhl
MD5:	3D6AAF34F494EBB7AEE72D9F1E409974
SHA1:	AB6D9E593DF00E22315A1ED553CAFA40EFEE1FBA
SHA-256:	D1B3C5C1EB2839519CA0B0E4E5DCF6120D0A14E2D81056AC11F2057443740705
SHA-512:	14B3475E8E166D8351CC349F62EF6B1572793E07A6ADA611C2B4412A17951D4A3D08BC757F4D8542AB98E6A9024F4873F7417B7996B6B710BA2A8A54BF6087B5
Malicious:	**true**
Preview:	.I...H

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

Process:	C:\Users\user\Desktop\Scancontract103.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	42
Entropy (8bit):	4.350068910616443
Encrypted:	false
SSDEEP:	3:oNWXp5v2GOUDu:oNWXpF2/
MD5:	AA619EA44F715A3F4CF627DD80CFED11
SHA1:	5BFC5B8E726014C10FD0226AFAE783DEC203CB6B
SHA-256:	25186E981F6DA5CA846C5BC3A97592D4D39BA2F43AB7AA2A0B4088C5FA54AAB4
SHA-512:	2255746B212D29944BDA7AFD8294D5A3E073908670BFDA9038FB68C056302F4F01B757AC22F95A72076443690B6228B73A9A94CB5383E2CE510ED98910B43DA3
Malicious:	false
Preview:	C:\Users\user\Desktop\Scancontract103.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.084655686253337
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:	Scancontract103.exe
File size:	854528
MD5:	9d2a2b596cd979fc9674824d2aa731df
SHA1:	015e8ae0f838e0fba35643297530a5b9a66e4186
SHA256:	c4a2c953833c8d6b5d2ef71b997700559ecc9f23573d89072d205f963e46956c
SHA512:	768843f52697ac5a8e8ff71ff5a66bca977cc6fad9da349ce77eee431aa5252ec07187d52bce92bd50bbcec1a10b6ce1a9123dbafa1e34d7a36ac2a9e511cef3

SSDEEP:	12288:sx9I2iNl/joW7EsJ2uM1DgC9tqGdpb5QyXYzvtMdADqjJ5ns:N1fEW7T4RDgvGdpHYzQjrs
TLSH:	11054A2429EB922CF4B69BF95FC8F8FB4C5BFA61252960F624A153468B33E05CCD1435
File Content Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L.....5c..............P.................. ... .@.. ....`............@...............................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d13d6
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x63358100 [Thu Sep 29 11:26:56 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd1384	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd2000	0x11ec	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd4000	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	0xcf3dc	0xcf400	False	0.697853447300965	COM executable for DOS	7.0886542606348	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xd2000	0x11ec	0x1200	False	0.3947482638888889	data	5.057459517659846	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd4000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xd2090	0x330	data		
RT_MANIFEST	0xd23d0	0xe15	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF, LF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

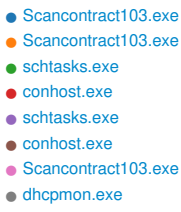
TCP Packets

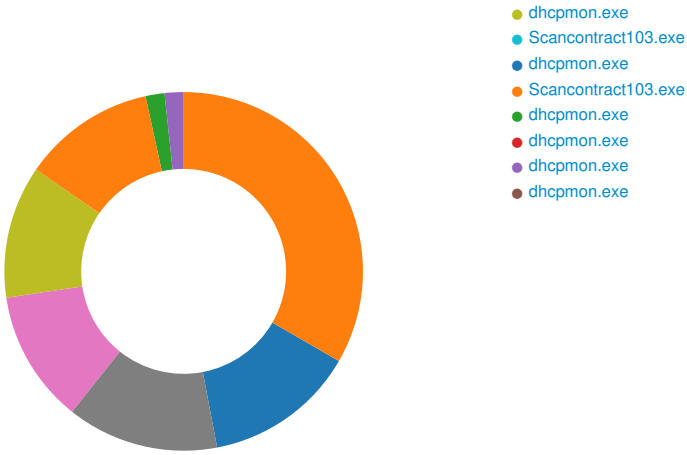
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 29, 2022 22:59:20.027470112 CEST	49707	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 22:59:20.040286064 CEST	60110	49707	79.134.225.6	192.168.2.3
Sep 29, 2022 22:59:20.590548992 CEST	49707	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 22:59:20.603280067 CEST	60110	49707	79.134.225.6	192.168.2.3
Sep 29, 2022 22:59:21.293834925 CEST	49707	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 22:59:21.306813955 CEST	60110	49707	79.134.225.6	192.168.2.3
Sep 29, 2022 22:59:26.231312990 CEST	49708	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 22:59:26.244163036 CEST	60110	49708	79.134.225.6	192.168.2.3
Sep 29, 2022 22:59:26.762944937 CEST	49708	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 22:59:26.775790930 CEST	60110	49708	79.134.225.6	192.168.2.3
Sep 29, 2022 22:59:27.372375965 CEST	49708	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 22:59:27.385637999 CEST	60110	49708	79.134.225.6	192.168.2.3
Sep 29, 2022 22:59:31.717842102 CEST	49709	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 22:59:31.732376099 CEST	60110	49709	79.134.225.6	192.168.2.3
Sep 29, 2022 22:59:32.294923067 CEST	49709	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 22:59:32.307845116 CEST	60110	49709	79.134.225.6	192.168.2.3
Sep 29, 2022 22:59:32.888734102 CEST	49709	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 22:59:32.901580095 CEST	60110	49709	79.134.225.6	192.168.2.3
Sep 29, 2022 22:59:37.211786985 CEST	49710	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 22:59:37.224678040 CEST	60110	49710	79.134.225.6	192.168.2.3
Sep 29, 2022 22:59:37.763921022 CEST	49710	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 22:59:37.776861906 CEST	60110	49710	79.134.225.6	192.168.2.3
Sep 29, 2022 22:59:38.373284101 CEST	49710	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 22:59:38.386439085 CEST	60110	49710	79.134.225.6	192.168.2.3
Sep 29, 2022 22:59:43.012607098 CEST	49711	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 22:59:43.025531054 CEST	60110	49711	79.134.225.6	192.168.2.3
Sep 29, 2022 22:59:43.592551947 CEST	49711	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 22:59:43.605590105 CEST	60110	49711	79.134.225.6	192.168.2.3
Sep 29, 2022 22:59:44.295752048 CEST	49711	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 22:59:44.308585882 CEST	60110	49711	79.134.225.6	192.168.2.3
Sep 29, 2022 22:59:48.728755951 CEST	49712	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 22:59:48.741656065 CEST	60110	49712	79.134.225.6	192.168.2.3
Sep 29, 2022 22:59:49.296158075 CEST	49712	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 22:59:49.309087992 CEST	60110	49712	79.134.225.6	192.168.2.3
Sep 29, 2022 22:59:49.983714104 CEST	49712	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 22:59:49.996527910 CEST	60110	49712	79.134.225.6	192.168.2.3
Sep 29, 2022 22:59:54.070527077 CEST	49713	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 22:59:54.083321095 CEST	60110	49713	79.134.225.6	192.168.2.3
Sep 29, 2022 22:59:54.765382051 CEST	49713	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 22:59:54.778515100 CEST	60110	49713	79.134.225.6	192.168.2.3
Sep 29, 2022 22:59:55.374838114 CEST	49713	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 22:59:55.387594938 CEST	60110	49713	79.134.225.6	192.168.2.3
Sep 29, 2022 22:59:59.943087101 CEST	49714	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 22:59:59.956547022 CEST	60110	49714	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:00.484608889 CEST	49714	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 23:00:00.499109030 CEST	60110	49714	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:01.094042063 CEST	49714	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 23:00:01.107193947 CEST	60110	49714	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:05.524106979 CEST	49715	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 23:00:05.537091970 CEST	60110	49715	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:06.082381010 CEST	49715	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 23:00:06.095248938 CEST	60110	49715	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:06.766412020 CEST	49715	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 23:00:06.779191971 CEST	60110	49715	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:10.834242105 CEST	49716	60110	192.168.2.3	79.134.225.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 29, 2022 23:00:10.847059965 CEST	60110	49716	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:11.464692116 CEST	49716	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 23:00:11.477426052 CEST	60110	49716	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:11.985686064 CEST	49716	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 23:00:11.998442888 CEST	60110	49716	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:16.608930111 CEST	49717	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 23:00:16.621793032 CEST	60110	49717	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:17.267476082 CEST	49717	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 23:00:17.280277967 CEST	60110	49717	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:17.876717091 CEST	49717	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 23:00:17.890031099 CEST	60110	49717	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:21.904520988 CEST	49718	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 23:00:21.918123960 CEST	60110	49718	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:22.486566067 CEST	49718	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 23:00:22.499701023 CEST	60110	49718	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:23.174092054 CEST	49718	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 23:00:23.187195063 CEST	60110	49718	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:27.675836086 CEST	49719	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 23:00:27.688648939 CEST	60110	49719	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:28.205789089 CEST	49719	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 23:00:28.218532085 CEST	60110	49719	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:28.721540928 CEST	49719	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 23:00:28.734438896 CEST	60110	49719	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:32.754986048 CEST	49720	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 23:00:32.768208027 CEST	60110	49720	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:33.268742085 CEST	49720	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 23:00:33.281815052 CEST	60110	49720	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:33.784370899 CEST	49720	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 23:00:33.797348976 CEST	60110	49720	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:37.803364038 CEST	49721	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 23:00:37.816562891 CEST	60110	49721	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:38.316065073 CEST	49721	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 23:00:38.329046965 CEST	60110	49721	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:38.831706047 CEST	49721	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 23:00:38.844505072 CEST	60110	49721	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:42.998397112 CEST	49722	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 23:00:43.011187077 CEST	60110	49722	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:43.597734928 CEST	49722	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 23:00:43.610474110 CEST	60110	49722	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:44.207194090 CEST	49722	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 23:00:44.220000029 CEST	60110	49722	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:48.225795031 CEST	49723	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 23:00:48.238611937 CEST	60110	49723	79.134.225.6	192.168.2.3
Sep 29, 2022 23:00:48.754570961 CEST	49723	60110	192.168.2.3	79.134.225.6
Sep 29, 2022 23:00:48.767365932 CEST	60110	49723	79.134.225.6	192.168.2.3

Statistics

Behavior





System Behavior

Analysis Process: Scancontract103.exe PID: 3732, Parent PID: 1952

General

Target ID:	0
Start time:	22:58:46
Start date:	29/09/2022
Path:	C:\Users\user\Desktop\Scancontract103.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Scancontract103.exe"
Imagebase:	0x170000
File size:	854528 bytes
MD5 hash:	9D2A2B596CD979FC9674824D2AA731DF
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: 00000000.00000002.308527260.0000000003571000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.308527260.0000000003571000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.308527260.0000000003571000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.308527260.0000000003571000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.303876077.00000000025BB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.311167352.00000000036BE000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.311167352.00000000036BE000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.311167352.00000000036BE000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.311167352.00000000036BE000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
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	6D1ACF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1ACF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Scancontract103.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D4BC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Scancontract103.exe.log	0	1302	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",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D4BC907	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	6D185705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D185705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D18CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D185705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D185705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFF1B4F	ReadFile

Analysis Process: Scancontract103.exe PID: **1760**, Parent PID: **3732**

General

Target ID:	6
Start time:	22:59:07
Start date:	29/09/2022

Path:	C:\Users\user\Desktop\Scancontract103.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x970000
File size:	854528 bytes
MD5 hash:	9D2A2B596CD979FC9674824D2AA731DF
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: 00000006.00000002.547986042.0000000005900000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.547986042.0000000005900000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000006.00000002.547986042.0000000005900000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000002.547986042.0000000005900000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000000.299936604.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000000.299936604.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000000.299936604.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000000.299936604.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.530169744.0000000002E21000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000002.530169744.0000000002E21000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.548040807.0000000005910000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.548040807.0000000005910000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.548040807.0000000005910000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000006.00000002.548040807.0000000005910000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000002.548040807.0000000005910000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
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	6D1ACF06	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	6D1ACF06	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	6BFFBEFF	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	6BFF1E60	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	6BFFBEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6BFFDD66	CopyFileW
C:\Program Files (x86)\DHCP Mo nitor\dhcpmon.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6BFFDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpCA7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BFF7038	GetTempFile NameW
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	6BFF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp1090.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6BFF7038	GetTempFile NameW
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	6BFFBEFF	CreateDirect oryW
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	6BFFBEFF	CreateDirect oryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpCA7.tmp	success or wait	1	6BFF6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp1090.tmp	success or wait	1	6BFF6A95	DeleteFileW
C:\Users\user\Desktop\Scancontract103.exe:Zone.Identifier	success or wait	1	53D8B06	DeleteFileA

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	0	8	fd 6c fd 22 fd 48	lH	success or wait	1	6BFF1B4F	WriteFile
C:\Program Files (x86)\DHCP Mo nitor\dhcpmon.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 00 fd 35 63 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 50 00 00 fd 0c 00 00 14 00 00 00 00 00 00 fd 13 0d 00 00 20 00 00 00 20 0d 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 60 0d 00 00 02 00 00 00 00 00 00 02 00 40 fd 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.$PEL5cP @ `@	success or wait	4	6BFFDD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	6BFFDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpCA7.tmp	0	1305	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	6BFF1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	0	42	43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 44 65 73 6b 74 6f 70 5c 53 63 61 6e 63 6f 6e 74 72 61 63 74 31 30 33 2e 65 78 65	C:\Users\user\Desktop\Scancontract103.exe	success or wait	1	6BFF1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmp1090.tmp	0	1310	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	6BFF1B4F	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	6D185705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D185705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D18CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D18CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D185705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D185705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFF1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D16D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D16D72F	unknown
C:\Users\user\Desktop\Scancontract103.exe	unknown	4096	success or wait	1	6D16D72F	unknown
C:\Users\user\Desktop\Scancontract103.exe	unknown	512	success or wait	1	6D16D72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	6BFF646A	RegSetValueExW

Analysis Process: schtasks.exe PID: **2636**, Parent PID: **1760**

General

Target ID:	11
Start time:	22:59:14
Start date:	29/09/2022
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\tmpCA7.tmp
Imagebase:	0x7ff745070000
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\tmpCA7.tmp	unknown	2	success or wait	1	116AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpCA7.tmp	unknown	1306	success or wait	1	116ABD9	ReadFile

Analysis Process: conhost.exe PID: **4744**, Parent PID: **2636**

General

Target ID:	12

Start time:	22:59:14
Start date:	29/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: **2300**, Parent PID: **1760**

General

Target ID:	13
Start time:	22:59:15
Start date:	29/09/2022
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\tmp1090.tmp
Imagebase:	0x1160000
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\tmp1090.tmp	unknown	2	success or wait	1	116AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp1090.tmp	unknown	1311	success or wait	1	116ABD9	ReadFile

Analysis Process: conhost.exe PID: **5056**, Parent PID: **2300**

General

Target ID:	14
Start time:	22:59:15
Start date:	29/09/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
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: Scancontract103.exe PID: **6052**, Parent PID: **1080**

General

Target ID:	15
Start time:	22:59:16
Start date:	29/09/2022
Path:	C:\Users\user\Desktop\Scancontract103.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Scancontract103.exe 0
Imagebase:	0xd50000
File size:	854528 bytes
MD5 hash:	9D2A2B596CD979FC9674824D2AA731DF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.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	6D1ACF06	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	6D1ACF06	unknown

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	6D185705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D185705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D18CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D185705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D185705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFF1B4F	ReadFile

Analysis Process: dhcpmon.exe PID: **5308**, Parent PID: **1080**

General

Target ID:	16
Start time:	22:59:16
Start date:	29/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0

Imagebase:	0xe90000
File size:	854528 bytes
MD5 hash:	9D2A2B596CD979FC9674824D2AA731DF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000010.00000002.400735152.000000000334B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
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	6D1ACF06	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	6D1ACF06	unknown
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	6D4BC78D	CreateFileW

File Written

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	0	1302	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",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D4BC907	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	6D185705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D185705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D18CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0E03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D185705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D185705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFF1B4F	ReadFile

Analysis Process: dhcpmon.exe PID: **1012**, Parent PID: **3452**

General

Target ID:	17
Start time:	22:59:22
Start date:	29/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0xa70000
File size:	854528 bytes
MD5 hash:	9D2A2B596CD979FC9674824D2AA731DF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.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	6D1ACF06	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	6D1ACF06	unknown

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	6D185705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D185705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D18CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D185705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D185705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFF1B4F	ReadFile

Analysis Process: Scancontract103.exe PID: **3988**, Parent PID: **6052**

General

Target ID:	18
Start time:	22:59:45
Start date:	29/09/2022
Path:	C:\Users\user\Desktop\Scancontract103.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x2a0000
File size:	854528 bytes
MD5 hash:	9D2A2B596CD979FC9674824D2AA731DF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: dhcpmon.exe PID: **4632**, Parent PID: **5308**

General

Target ID:	19
Start time:	22:59:45
Start date:	29/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x390000
File size:	854528 bytes
MD5 hash:	9D2A2B596CD979FC9674824D2AA731DF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Scancontract103.exe PID: **5588**, Parent PID: **6052**

General

Target ID:	20
Start time:	22:59:46
Start date:	29/09/2022
Path:	C:\Users\user\Desktop\Scancontract103.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xd50000
File size:	854528 bytes
MD5 hash:	9D2A2B596CD979FC9674824D2AA731DF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.442532353.0000000004309000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.442532353.0000000004309000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000014.00000002.442532353.0000000004309000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.440811827.0000000003301000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.440811827.0000000003301000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000014.00000002.440811827.0000000003301000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
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	6D1ACF06	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	6D1ACF06	unknown

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	6D185705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D185705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D18CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0E03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0E03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D185705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D185705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFF1B4F	ReadFile

Analysis Process: dhcpmon.exe PID: **2576**, Parent PID: **5308**

General

Target ID:	21
Start time:	22:59:46
Start date:	29/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x990000
File size:	854528 bytes
MD5 hash:	9D2A2B596CD979FC9674824D2AA731DF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.443127439.0000000002D61000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.443127439.0000000002D61000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000015.00000002.443127439.0000000002D61000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Analysis Process: dhcpmon.exe PID: **2300**, Parent PID: **1012**

General

Target ID:	22
Start time:	22:59:53
Start date:	29/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x180000
File size:	854528 bytes
MD5 hash:	9D2A2B596CD979FC9674824D2AA731DF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: dhcpmon.exe PID: **5420**, Parent PID: **1012**

General

Target ID:	23
Start time:	22:59:55
Start date:	29/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x50000
File size:	854528 bytes
MD5 hash:	9D2A2B596CD979FC9674824D2AA731DF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: dhcpmon.exe PID: **408**, Parent PID: **1012**

General

Target ID:	24
Start time:	22:59:55
Start date:	29/09/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x870000
File size:	854528 bytes
MD5 hash:	9D2A2B596CD979FC9674824D2AA731DF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

Disassembly

No disassembly