ID: 338348
Sample Name:
Scan002.exe.exe
Cookbook: default.jbs
Time: 07:18:34
Date: 12/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

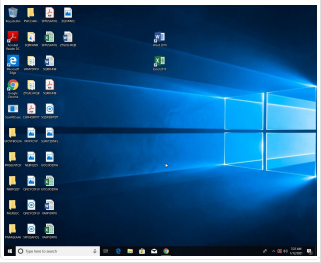
Analysis Report Scan002.exe.exe

Overview

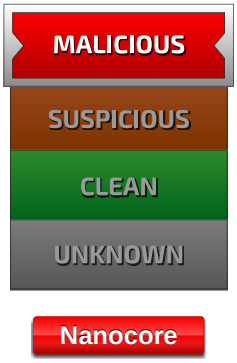
General Information

Sample Name:	Scan002.exe.exe
Analysis ID:	338348
MD5:	8e2315d05c47fef..
SHA1:	e56fe197d61518b.
SHA256:	dd647e98e0bd3b..
Tags:	exe NanoCore RAT Yahoo

Most interesting Screenshot:



Detection

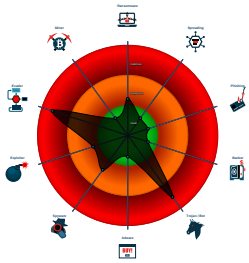


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…

Classification



Startup

- **System is w10x64**
- Scan002.exe.exe (PID: 2960 cmdline: 'C:\Users\user\Desktop\Scan002.exe.exe' MD5: 8E2315D05C47FEFDDDF0A686BF9E353E)
  - schtasks.exe (PID: 4564 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\UbebSiSIKndjd' /XML 'C:\Users\user\AppData\Local\Temp\tmp1945.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5348 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Scan002.exe.exe (PID: 4340 cmdline: {path} MD5: 8E2315D05C47FEFDDDF0A686BF9E353E)
    - schtasks.exe (PID: 4260 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp8ED7.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5412 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 976 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp91C6.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 4812 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Scan002.exe.exe (PID: 204 cmdline: C:\Users\user\Desktop\Scan002.exe.exe 0 MD5: 8E2315D05C47FEFDDDF0A686BF9E353E)
  - schtasks.exe (PID: 5876 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\UbebSiSIKndjd' /XML 'C:\Users\user\AppData\Local\Temp\tmp414F.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 2160 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - schtasks.exe (PID: 6608 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\UbebSiSIKndjd' /XML 'C:\Users\user\AppData\Local\Temp\tmp65AF.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
        - conhost.exe (PID: 6644 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - dhcpmon.exe (PID: 6712 cmdline: {path} MD5: 8E2315D05C47FEFDDDF0A686BF9E353E)
      - dhcpmon.exe (PID: 6744 cmdline: {path} MD5: 8E2315D05C47FEFDDDF0A686BF9E353E)
      - dhcpmon.exe (PID: 6764 cmdline: {path} MD5: 8E2315D05C47FEFDDDF0A686BF9E353E)
  - Scan002.exe.exe (PID: 4260 cmdline: {path} MD5: 8E2315D05C47FEFDDDF0A686BF9E353E)
- dhcpmon.exe (PID: 5396 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 8E2315D05C47FEFDDDF0A686BF9E353E)
- dhcpmon.exe (PID: 2160 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 8E2315D05C47FEFDDDF0A686BF9E353E)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "C2: ": [
    "172.111.249.15"
  ],
  "Version: ": "NanoCore Client, Version=1.2.2.0"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.274234683.000000000416 7000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1d8595:$x1: NanoCore.ClientPluginHost • 0x1d85d2:$x2: IClientNetworkHost • 0x1dc105:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcb w8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000A.00000002.274234683.000000000416 7000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000A.00000002.274234683.000000000416 7000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x1d82fd:$a: NanoCore • 0x1d830d:$a: NanoCore • 0x1d8541:$a: NanoCore • 0x1d8555:$a: NanoCore • 0x1d8595:$a: NanoCore • 0x1d835c:$b: ClientPlugin • 0x1d855e:$b: ClientPlugin • 0x1d859e:$b: ClientPlugin • 0x127a96:$c: ProjectData • 0x1d8483:$c: ProjectData • 0x128537:$d: DESCrypto • 0x1d8e8a:$d: DESCrypto • 0x1e0856:$e: KeepAlive • 0x1de844:$g: LogClientMessage • 0x1daa3f:$i: get_Connected • 0x1d91c0:$j: #=q • 0x1d91f0:$j: #=q • 0x1d920c:$j: #=q • 0x1d923c:$j: #=q • 0x1d9258:$j: #=q • 0x1d9274:$j: #=q
0000000D.00000002.286646772.000000000040 2000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000D.00000002.286646772.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 47 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
13.2.Scan002.exe.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
13.2.Scan002.exe.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
13.2.Scan002.exe.exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
13.2.Scan002.exe.exe.400000.0.unpack	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:$j: #=q
3.2.Scan002.exe.exe.6220000.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
Click to see the 17 entries				

Sigma Overview

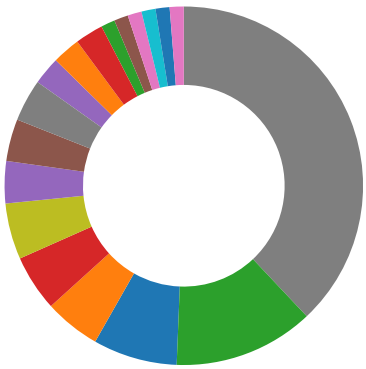
System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Sigma detected: Conhost Parent Proces Executions

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

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)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

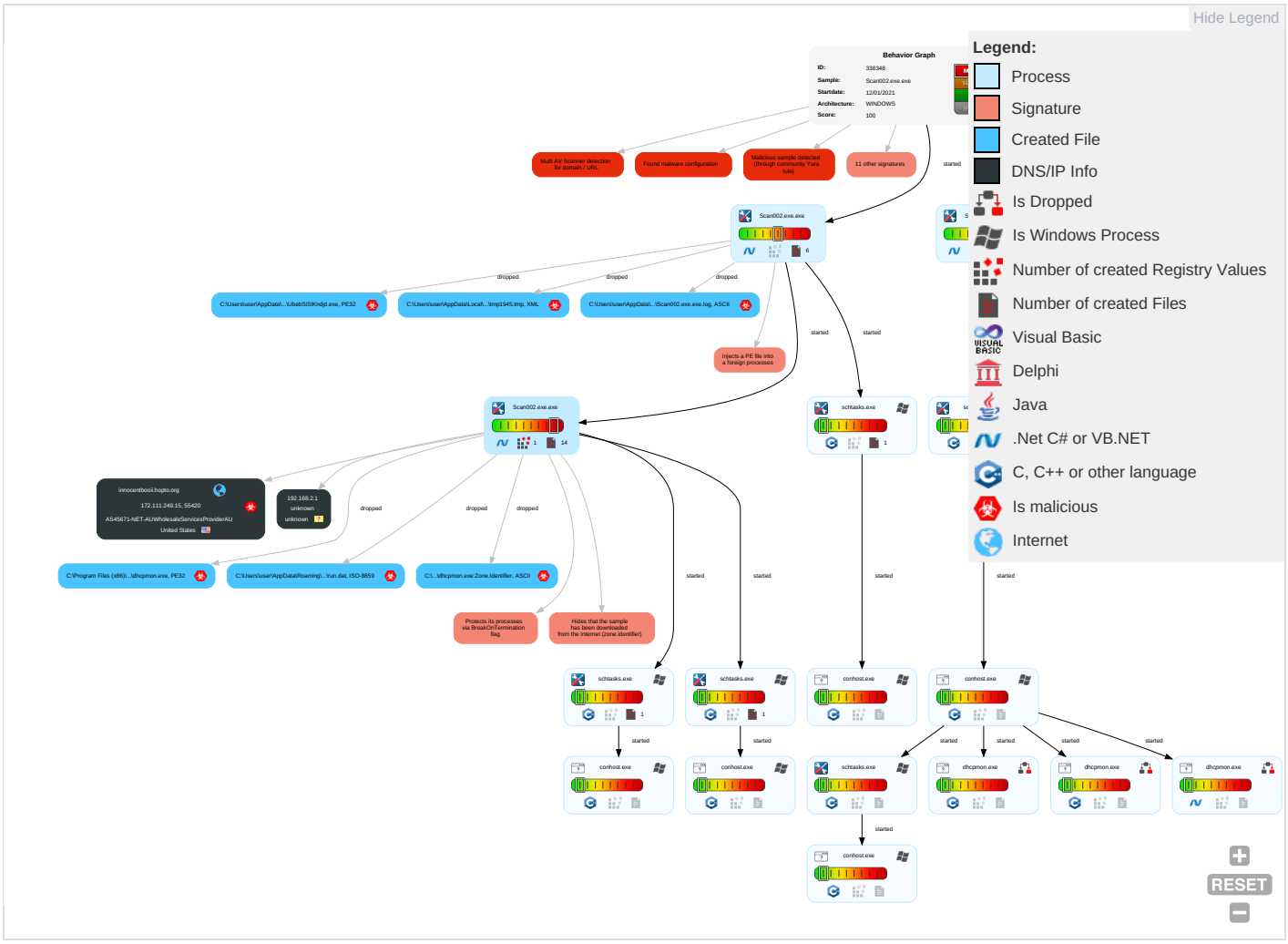
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Access Token Manipulation 1	Masquerading 2	Input Capture 2 1	Security Software Discovery 1 1 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Remote Access Software 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1 2	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 3	Proc Filesystem	File and Directory Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 1 3	/etc/passwd and /etc/shadow	System Information Discovery 1 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

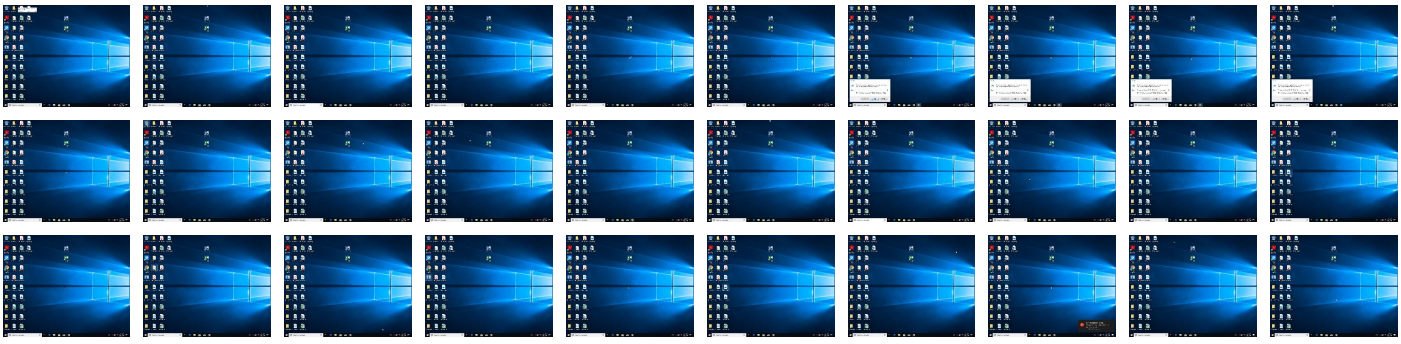
Behavior Graph



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
Scan002.exe.exe	100%	Joe Sandbox ML		

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.Scan002.exe.exe.6220000.6.unpack	100%	Avira	TR/NanoCore.fadte		Download File
13.2.Scan002.exe.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
27.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.2.Scan002.exe.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
innocentbooii.hopto.org	8%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comalsa	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0Y/	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.founder.com.cn/cnI	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/k/	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/N/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnorm	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Pogr	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cne-di.	0%	Avira URL Cloud	safe	
http://www.urwpp.deod	0%	Avira URL Cloud	safe	
http://www.urwpp.de2	0%	Avira URL Cloud	safe	
http://www.fontbureau.comN/	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comFk/	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/40	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnoftA.	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalsd	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/G/	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comcoma	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/Y0P	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.tiro.	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/k/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn8	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.urwpp.dei	0%	Avira URL Cloud	safe	
http://www.fonts.com4	0%	Avira URL Cloud	safe	
http://www.fontbureau.comTTFY/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
innocentbooii.hopto.org	172.111.249.15	true	true	• 8%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comalsa	Scan002.exe.exe, 00000000.00000003.236366761.0000000004EB6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	Scan002.exe.exe, 00000000.00000002.256151393.00000000050C0000.00000002.00000001.sdmp, Scan002.exe.exe, 00000008.00000002.278996252.00000000056E0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.275007588.00000000054A0000.00000002.00000001.sdmp, dhcpmon.exe, 00000F.00000002.306107796.0000000005AF0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	Scan002.exe.exe, 00000000.00000002.256151393.00000000050C0000.00000002.00000001.sdmp, Scan002.exe.exe, 00000008.00000002.278996252.00000000056E0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.275007588.00000000054A0000.00000002.00000001.sdmp, dhcpmon.exe, 00000F.00000002.306107796.0000000005AF0000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	Scan002.exe.exe, 00000000.00000002.256151393.00000000050C0000.00000002.00000001.sdmp, Scan002.exe.exe, 00000008.00000002.278996252.00000000056E0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.275007588.00000000054A0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.306107796.00000000005AF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Scan002.exe.exe, 00000000.00000002.256151393.00000000050C0000.00000002.00000001.sdmp, Scan002.exe.exe, 00000008.00000002.278996252.00000000056E0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.275007588.00000000054A0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.306107796.00000000005AF0000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/Y0Y/	Scan002.exe.exe, 00000000.00000003.231447812.0000000004EB6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	dhcpmon.exe, 0000000F.00000002.306107796.0000000005AF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	dhcpmon.exe, 0000000F.00000002.306107796.0000000005AF0000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	Scan002.exe.exe, 00000000.00000002.256151393.00000000050C0000.00000002.00000001.sdmp, Scan002.exe.exe, 00000008.00000002.278996252.00000000056E0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.275007588.00000000054A0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.306107796.00000000005AF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnI	Scan002.exe.exe, 00000000.00000003.228230964.0000000004EBE000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/k/	Scan002.exe.exe, 00000000.00000003.231098088.0000000004EB5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/N/	Scan002.exe.exe, 00000000.00000003.231280337.0000000004EB6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnorm	Scan002.exe.exe, 00000000.00000003.228156025.0000000004EB3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	Scan002.exe.exe, 00000000.00000002.256151393.00000000050C0000.00000002.00000001.sdmp, Scan002.exe.exe, 00000008.00000002.278996252.00000000056E0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.275007588.00000000054A0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.306107796.00000000005AF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Scan002.exe.exe, 00000000.00000002.256151393.00000000050C0000.00000002.00000001.sdmp, Scan002.exe.exe, 00000008.00000002.278996252.00000000056E0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.275007588.00000000054A0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.306107796.00000000005AF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

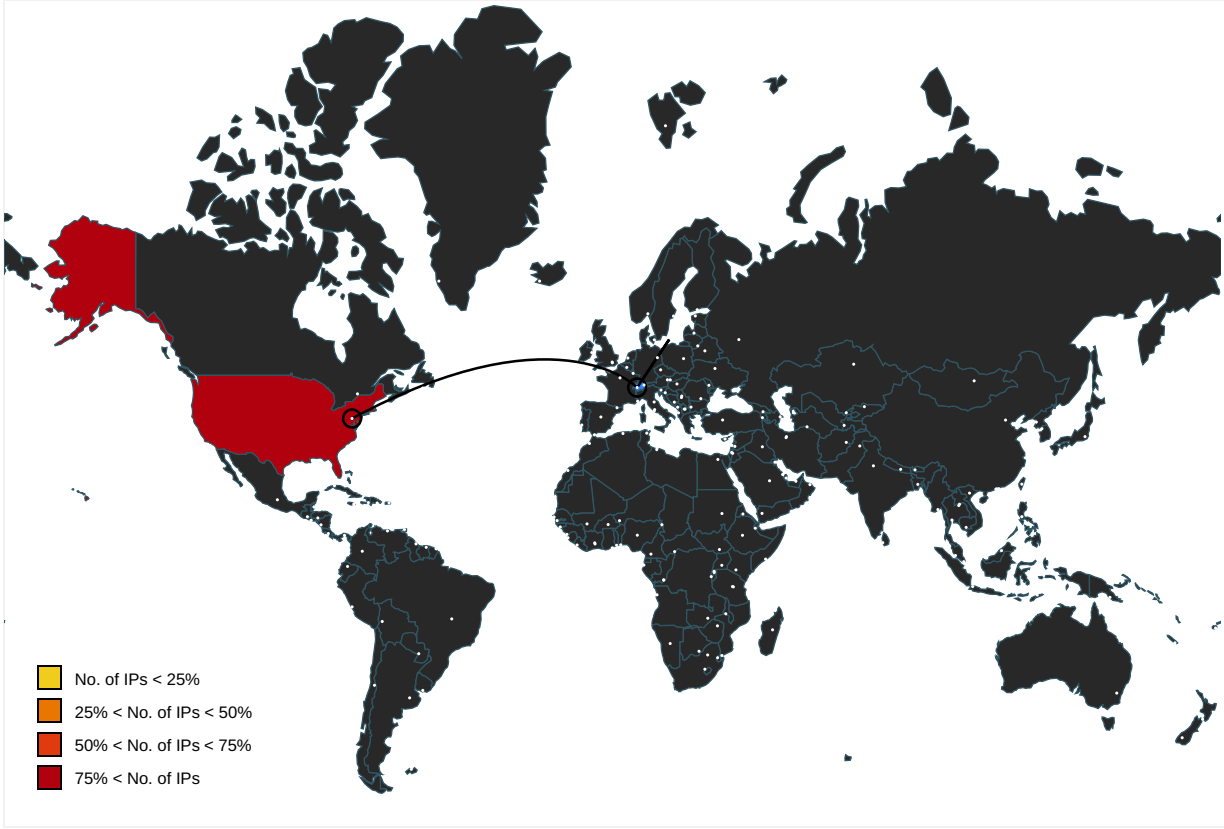
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/cThe	Scan002.exe.exe, 00000000.00000002.256151393.00000000050C0000.00000002.00000001.sdmp, Scan002.exe.exe, 00000008.00000002.278996252.00000000056E0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.275007588.00000000054A0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.306107796.00000000005AF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Pogr	Scan002.exe.exe, 00000000.00000003.231221602.0000000004EB6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Scan002.exe.exe, 00000000.00000002.256151393.00000000050C0000.00000002.00000001.sdmp, Scan002.exe.exe, 00000008.00000002.278996252.00000000056E0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.275007588.00000000054A0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.306107796.00000000005AF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Scan002.exe.exe, 00000000.00000002.256151393.00000000050C0000.00000002.00000001.sdmp, Scan002.exe.exe, 00000000.00000003.227051250.0000000004EED000.00000004.00000001.sdmp, Scan002.exe.exe, 00000008.00000002.278996252.00000000056E0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.275007588.00000000054A0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.306107796.000000005AF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cne-di.	Scan002.exe.exe, 00000000.00000003.228156025.0000000004EB3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deod	Scan002.exe.exe, 00000000.00000003.232418765.0000000004ECF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.de2	Scan002.exe.exe, 00000000.00000003.232418765.0000000004ECF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comN/	Scan002.exe.exe, 00000000.00000003.236366761.0000000004EB6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	Scan002.exe.exe, 00000000.00000002.256151393.00000000050C0000.00000002.00000001.sdmp, Scan002.exe.exe, 00000008.00000002.278996252.00000000056E0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.275007588.00000000054A0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.306107796.00000000005AF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comFk/	Scan002.exe.exe, 00000000.00000003.236366761.0000000004EB6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	Scan002.exe.exe, 00000000.00000003.226824848.0000000004EED000.00000004.00000001.sdmp, Scan002.exe.exe, 00000008.00000002.278996252.00000000056E0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.275007588.00000000054A0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.306107796.00000000005AF0000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sandoll.co.kr	Scan002.exe.exe, 00000000.00000002.256151393.00000000050C0000.00000002.00000001.sdmp, Scan002.exe.exe, 00000008.00000002.278996252.00000000056E0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.275007588.00000000054A0000.00000002.00000001.sdmp, dhcpmon.exe, 00000F.00000002.306107796.0000000005AF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/40	Scan002.exe.exe, 00000000.00000003.231221602.0000000004EB6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	Scan002.exe.exe, 00000000.00000002.256151393.00000000050C0000.00000002.00000001.sdmp, Scan002.exe.exe, 00000008.00000002.278996252.00000000056E0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.275007588.00000000054A0000.00000002.00000001.sdmp, dhcpmon.exe, 00000F.00000002.306107796.0000000005AF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.de	Scan002.exe.exe, 00000000.00000003.236674676.0000000004ECF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Scan002.exe.exe, 00000000.00000002.256151393.00000000050C0000.00000002.00000001.sdmp, Scan002.exe.exe, 00000008.00000002.278996252.00000000056E0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.275007588.00000000054A0000.00000002.00000001.sdmp, dhcpmon.exe, 00000F.00000002.306107796.0000000005AF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	Scan002.exe.exe, 00000000.00000002.256151393.00000000050C0000.00000002.00000001.sdmp, Scan002.exe.exe, 00000008.00000002.278996252.00000000056E0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.275007588.00000000054A0000.00000002.00000001.sdmp, dhcpmon.exe, 00000F.00000002.306107796.0000000005AF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnoftA.	Scan002.exe.exe, 00000000.00000003.228156025.0000000004EB3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designerss	Scan002.exe.exe, 00000000.00000003.236366761.0000000004EB6000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comalsd	Scan002.exe.exe, 00000000.00000003.236366761.0000000004EB6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/G/	Scan002.exe.exe, 00000000.00000003.231098088.0000000004EB5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Scan002.exe.exe, 00000000.00000002.256151393.00000000050C0000.00000002.00000001.sdmp, Scan002.exe.exe, 00000008.00000002.278996252.00000000056E0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.275007588.00000000054A0000.00000002.00000001.sdmp, dhcpmon.exe, 00000F.00000002.306107796.0000000005AF0000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com	Scan002.exe.exe, 00000000.00000002.256151393.00000000050C0000.00000002.00000001.sdmp, Scan002.exe.exe, 00000000.00000003.236366761.0000000004EB6000.00000004.00000001.sdmp, Scan002.exe.exe, 00000008.00000002.278996252.00000000056E0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.275007588.00000000054A0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.306107796.0000000005AF0000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/frere-jones.htmlh	Scan002.exe.exe, 00000000.00000003.235619449.0000000004EC2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comF	Scan002.exe.exe, 00000000.00000003.236366761.0000000004EB6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comcoma	Scan002.exe.exe, 00000000.00000002.255981298.0000000004EB0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Y0P	Scan002.exe.exe, 00000000.00000003.231280337.0000000004EB6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	Scan002.exe.exe, 00000000.00000003.231447812.0000000004EB6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.coma	Scan002.exe.exe, 00000000.00000002.255981298.0000000004EB0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	Scan002.exe.exe, 00000000.00000002.256151393.00000000050C0000.00000002.00000001.sdmp, Scan002.exe.exe, 00000008.00000002.278996252.00000000056E0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.275007588.00000000054A0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.306107796.0000000005AF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.	Scan002.exe.exe, 00000000.00000003.229248591.0000000004EB4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/	Scan002.exe.exe, 00000000.00000003.229248591.0000000004EB4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Scan002.exe.exe, 00000000.00000002.256151393.00000000050C0000.00000002.00000001.sdmp, Scan002.exe.exe, 00000008.00000002.278996252.00000000056E0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.275007588.00000000054A0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.306107796.0000000005AF0000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	Scan002.exe.exe, 00000000.00000003.228394731.0000000004EC1000.00000004.00000001.sdmp, Scan002.exe.exe, 00000008.00000002.278996252.00000000056E0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.275007588.00000000054A0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.306107796.0000000005AF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-jones.html	Scan002.exe.exe, 00000000.00000002.256151393.00000000050C0000.00000002.00000001.sdmp, Scan002.exe.exe, 00000008.00000002.278996252.00000000056E0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.275007588.00000000054A0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.306107796.0000000005AF0000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/k/	Scan002.exe.exe, 00000000.00000003.231447812.0000000004EB6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn8	Scan002.exe.exe, 00000000.00000003.228156025.0000000004EB3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	Scan002.exe.exe, 00000000.00000003.231098088.0000000004EB5000.00000004.00000001.sdmp, Scan002.exe.exe, 00000000.00000003.231221602.0000000004EB6000.00000004.00000001.sdmp, Scan002.exe.exe, 00000000.00000003.231280337.0000000004EB6000.00000004.00000001.sdmp, Scan002.exe.exe, 00000008.00000002.278996252.00000000056E0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.275007588.00000000054A0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.306107796.0000000005AF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Scan002.exe.exe, 00000000.00000002.256151393.00000000050C0000.00000002.00000001.sdmp, Scan002.exe.exe, 00000008.00000002.278996252.00000000056E0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000A.00000002.275007588.00000000054A0000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.306107796.0000000005AF0000.00000002.00000001.sdmp	false		high
http://www.urwpp.dei	Scan002.exe.exe, 00000000.00000003.232418765.0000000004ECF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com4	Scan002.exe.exe, 00000000.00000003.226884104.0000000004EED000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/	Scan002.exe.exe, 00000000.00000003.232966975.0000000004ECF000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comTTFY/	Scan002.exe.exe, 00000000.00000003.236366761.0000000004EB6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.111.249.15	unknown	United States		45671	AS45671-NET-AUWholesaleServicesProviderAU	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	338348
Start date:	12.01.2021
Start time:	07:18:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Scan002.exe.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:	40
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@29/12@6/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 13.88.21.125, 104.79.90.110, 51.104.139.180, 92.122.213.247, 92.122.213.194, 93.184.221.240, 51.103.5.186, 52.155.217.156, 20.54.26.129, 51.11.168.160 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, wu.azureedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net • 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 exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:19:29	API Interceptor	1267x Sleep call for process: Scan002.exe.exe modified
07:19:35	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\Scan002.exe.exe" s>$(Arg0)
07:19:38	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Time	Type	Description
07:19:39	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
07:19:40	API Interceptor	3x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
innocentbooii.hopto.org	File.exe	Get hash	malicious	Browse	• 194.5.98.108
	SWB copy.exe	Get hash	malicious	Browse	• 194.5.98.108
	0LGpT3WYf1.exe	Get hash	malicious	Browse	• 154.120.96.115

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS45671-NET-AUWholesaleServicesProviderAU	http://s3-eu-west-1.amazonaws.com/hjdpjni/ogbim#qs=r-acacaeeikdgeadkieeefjaehbihabababaefahcaccajbiackdcagfkbkacb	Get hash	malicious	Browse	• 203.26.196.25
	Check.vbs	Get hash	malicious	Browse	• 27.50.75.62
	ano.exe	Get hash	malicious	Browse	• 27.50.80.18
	jbs.exe	Get hash	malicious	Browse	• 221.121.151.3
	http://https://noosahealth.com/vnotice/w9k6dnqb128gjgj9oklfih2f.php?MTYwMTU2MDcyMGYwN2NlMDllN2Q1NTNlNWU1ODcwZGM1N2RhOWQ1ZWFkNDNiZTIxZTUxNGRkYjQ0MzNmNDNlNTRlNDgzMzI1YzM5NGZhODY4ZA==&data=a2lhbWV0dGlAY29leHBhbi5jb20=	Get hash	malicious	Browse	• 103.13.103.135
	http://https://rgmgalaxy.com/cgi/?email=cgarcia@dataxu.com	Get hash	malicious	Browse	• 180.92.196.41
	http://https://bnet.alpha-fem.com/rt/dmZpYWxsb3NAYmFjZmxvcmlkYS5jb20=	Get hash	malicious	Browse	• 45.74.14.19
	ali.exe	Get hash	malicious	Browse	• 27.50.80.18
	CZP44EvQFN.doc	Get hash	malicious	Browse	• 118.127.60.139
	svPo783mk8.doc	Get hash	malicious	Browse	• 118.127.60.139
	9NLNYxPRWg.doc	Get hash	malicious	Browse	• 118.127.60.139
	gN7CiLPI2w.doc	Get hash	malicious	Browse	• 118.127.60.139
	b8X9P4f011.doc	Get hash	malicious	Browse	• 118.127.60.139
	IRxIRaWSZK.doc	Get hash	malicious	Browse	• 118.127.60.139
	T08KQuKIgs.doc	Get hash	malicious	Browse	• 118.127.60.139
	GhM6Zmi4U1.doc	Get hash	malicious	Browse	• 118.127.60.139
	mhaoMky8ES.doc	Get hash	malicious	Browse	• 118.127.60.139
	LApPQ8KJHO.doc	Get hash	malicious	Browse	• 118.127.60.139
	Sv5mt8dv9I.doc	Get hash	malicious	Browse	• 118.127.60.139
	BIri1a275h.doc	Get hash	malicious	Browse	• 118.127.60.139

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\Scan002.exe.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	910848
Entropy (8bit):	7.69470592663904
Encrypted:	false
SSDEEP:	12288:YMbCszXQrmZDevwQoqqj7h8tT8kqfbPVdhZu9TitgOLdKYy02UB+4zgl:DbCszXvvcwXh5gYK3029Ag
MD5:	8E2315D05C47FEFDDDF0A686BF9E353E
SHA1:	E56FE197D61518B5EA20696677C3FB444E39860E
SHA-256:	DD647E98E0BD3B1627A0385970C38CD046883967F39DBF9FE416D5300E8E310A
SHA-512:	D052FADFE382F2910992677F65BFDD1C5CDABD50837925B6B5EA14038026EC49E30112DE25D3E88A78CE832CEE7D79AE66A0821C2570276C12FBCAD2676050C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....N.... .....@.. .....@..... ..@.....K..... ....H.....text...T.... ....`.rsrc.....@..@.reloc..... .....@..B.....0.....H.....t{..8.....0.....o.... ...._ .....,....8.....o....t..... . &.....o.....o....(.....o.....o.....o.....o....Z. Z.....(.....+E.....X.Y.....,.+*.....X.....X.....X.....X.....X.I.Z.....X.....i.....-.....(.....o.....+..*^..}.....(.....(....*.0.....s.....o.....(....*.".(....*....0.....s.....o..... (....*..0..+.....,..{.....+...,..{....o

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Scan002.exe.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Scan002.exe.exe.log	
Process:	C:\Users\user\Desktop\Scan002.exe.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_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	false
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_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp1945.tmp	
Process:	C:\Users\user\Desktop\Scan002.exe.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1662
Entropy (8bit):	5.1728135789612715
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBJtn:cbhH7MlNQ8/rydbz9I3YODOLNdq39
MD5:	AA28189D75A160986C9DDF1DE1CBD68C
SHA1:	5C5EA1B0C1CA0BDEB33320AABD86BA464E4D432B
SHA-256:	845906543657D1AB101D9B1819DF5CFF158C8F397F7506FEEC42891CD78A1A1B
SHA-512:	5DBB5CB20838D719F0B3532AE5DBAD235F78BC0DE8954783FB98344218D06083BAB808E29363C9901973FFDAF746FE06ACE3CF29D1CCEB623A94245DDE4FBB3
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAv

C:\Users\user\AppData\Local\Temp\tmp414F.tmp	
Process:	C:\Users\user\Desktop\Scan002.exe.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1662
Entropy (8bit):	5.1728135789612715
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBJtn:cbhH7MlNQ8/rydbz9I3YODOLNdq39
MD5:	AA28189D75A160986C9DDF1DE1CBD68C
SHA1:	5C5EA1B0C1CA0BDEB33320AABD86BA464E4D432B
SHA-256:	845906543657D1AB101D9B1819DF5CFF158C8F397F7506FEEC42891CD78A1A1B
SHA-512:	5DBB5CB20838D719F0B3532AE5DBAD235F78BC0DE8954783FB98344218D06083BAB808E29363C9901973FFDAF746FE06ACE3CF29D1CCEB623A94245DDE4FBB3
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>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAv

C:\Users\user\AppData\Local\Temp\tmp65AF.tmp	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1662
Entropy (8bit):	5.1728135789612715
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBJtn:cbhH7MlNQ8/rydbz9I3YODOLNdq39
MD5:	AA28189D75A160986C9DDF1DE1CBD68C
SHA1:	5C5EA1B0C1CA0BDEB33320AABD86BA464E4D432B
SHA-256:	845906543657D1AB101D9B1819DF5CFF158C8F397F7506FEEC42891CD78A1A1B
SHA-512:	5DBB5CB20838D719F0B3532AE5DBAD235F78BC0DE8954783FB98344218D06083BAB808E29363C9901973FFDAF746FE06ACE3CF29D1CCEB623A94245DDE4FBB3
Malicious:	false

C:\Users\user\AppData\Local\Temp\tmp65AF.tmp	
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAv

C:\Users\user\AppData\Local\Temp\tmp8ED7.tmp	
Process:	C:\Users\user\Desktop\Scan002.exe.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1305
Entropy (8bit):	5.096557144339906
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0XExtn:cbk4oL600QydbQxIYODOLedq3hj
MD5:	29C2992183264E85915470135EDB70C9
SHA1:	AE42A898163FDDD286F9CC036789BDEE76BBCA79
SHA-256:	BAEE5F35FF81D3654E18E7356CAEE7D51CD198CAB7DD368E8D5FF5C408CA2BCC
SHA-512:	C28C9C8D86D1A38915AC69E50183319DE9F08ACCBB576933B2F68C9FE7F925ADF4B031733279E9B7C7791890FA2701235D3DF6915A47A26879D5EC3910A26F8(
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\tmp91C6.tmp	
Process:	C:\Users\user\Desktop\Scan002.exe.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:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\Scan002.exe.exe
File Type:	ISO-8859 text, with CR line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:hat:hat
MD5:	2C91F0DF6F187C76EADD8473749B5E06
SHA1:	C5D523419059FC3AC148A041E7DCC3EAB4500677
SHA-256:	A20F2288309FC1823C655409F922A077422D2DCD0BDF75104064B8A97177180E
SHA-512:	E207A7B37E5B154F0C44D5506DDC62BDC1FA5FF19676549174F581DF6141EAE512DE559ABA585815A9418533A296352DD2B3089C9E0B32AAFF506FDAACE3305
Malicious:	**true**
Preview:	...w...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\Scan002.exe.exe

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	42
Entropy (8bit):	4.162520173864397
Encrypted:	false
SSDEEP:	3:oN0naRR2GiAIN:oNcSR2DAI
MD5:	5A95A542025A94567015BC5FB4638686
SHA1:	65939CC89B4611F466E62AA799325B72ED12FD71
SHA-256:	0D4F4D965CB445119C1A5D9266593A1081C4E97E3403905366B98ADC9D7709F7
SHA-512:	EE0A17A0DC7F4D3A815CBC4BA873E5661D7C51A6788CBBCDB5EF01415EC18EBED4740AE9839B704201EECC4B4FC1D6B2DF1D7EC1A1BA4346A386BE0D0BA7E40D
Malicious:	false
Preview:	C:\Users\user\Desktop\Scan002.exe.exe

C:\Users\user\AppData\Roaming\UbebSiSlKndjd.exe	
Process:	C:\Users\user\Desktop\Scan002.exe.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	910848
Entropy (8bit):	7.69470592663904
Encrypted:	false
SSDEEP:	12288:YMbCszXQrmZDevwQoqqj7h8tT8kqfbPVdhZu9TitgOLdKYy02UB+4zgl:DbCszXvvcwXh5gYK3029Ag
MD5:	8E2315D05C47FEFDDDF0A686BF9E353E
SHA1:	E56FE197D61518B5EA20696677C3FB444E39860E
SHA-256:	DD647E98E0BD3B1627A0385970C38CD046883967F39DBF9FE416D5300E8E310A
SHA-512:	D052FADFE382F2910992677F65BFDD1C5CDABD50837925B6B5EA14038026EC49E30112DE25D3E88A78CE832CEE7D79AE66A0821C2570276C12FBCAD2676050C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....N.... .....@.. .....@..... ..@.....K..... ....H.....text...T.... ....`.rsrc.....@..@.reloc..... .....@..B.....0.....H.....t{..8.....0.....o.... ...._ .....,....8.....o....t.... . &.....o.....o....(.....o.....o.....o.....o....Z. Z.....(.....+E.....X.Y.....,.+*.....X.....X.....X.....X.....X.I.Z.....X.....i.....-.....(.....o.....+...*^..}.....(.....(....*.0.....s.....o.....(....*."."(....*....0.....s.....o..... (....*..0..+.....,..{.....+...,...{....o

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.69470592663904
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	Scan002.exe.exe
File size:	910848
MD5:	8e2315d05c47fefdddf0a686bf9e353e
SHA1:	e56fe197d61518b5ea20696677c3fb444e39860e
SHA256:	dd647e98e0bd3b1627a0385970c38cd046883967f39dbf9fe416d5300e8e310a
SHA512:	d052fadfe382f2910992677f65bfdd1c5cdabd50837925b6b5ea14038026ec49e30112de25d3e88a78ce832cee7d79ae66a0821c2570276c12fbcad2676050cc
SSDEEP:	12288:YMbCszXQrmZDevwQoqqj7h8tT8kqfbPVdhZu9TitgOLdKYy02UB+4zgl:DbCszXvvcwXh5gYK3029Ag
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..... ._.....N.... .....@.. .....@..... ...@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4df84e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FFCCC88 [Mon Jan 11 22:09:12 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xdf800	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe0000	0x800	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xe2000	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	0xdd854	0xdda00	False	0.822365869994	data	7.70309811015	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xe0000	0x800	0x800	False	0.3330078125	data	3.49807917331	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe2000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xe0090	0x388	data		
RT_MANIFEST	0xe0428	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

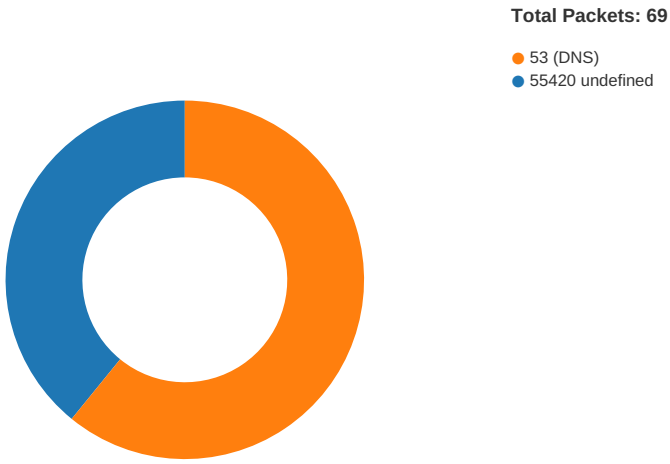
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Overwolf 2011 - 2020
Assembly Version	2.159.0.0
InternalName	Q.exe
FileVersion	2.159.0.0
CompanyName	Overwolf Ltd.
LegalTrademarks	
Comments	Overwolf Launcher
ProductName	OverwolfLauncher
ProductVersion	2.159.0.0
FileDescription	OverwolfLauncher
OriginalFilename	Q.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 12, 2021 07:19:40.595899105 CET	49727	55420	192.168.2.7	172.111.249.15
Jan 12, 2021 07:19:43.684853077 CET	49727	55420	192.168.2.7	172.111.249.15
Jan 12, 2021 07:19:49.721853018 CET	49727	55420	192.168.2.7	172.111.249.15
Jan 12, 2021 07:19:58.445087910 CET	49734	55420	192.168.2.7	172.111.249.15
Jan 12, 2021 07:20:01.500910044 CET	49734	55420	192.168.2.7	172.111.249.15
Jan 12, 2021 07:20:07.499305010 CET	49734	55420	192.168.2.7	172.111.249.15
Jan 12, 2021 07:20:15.415180922 CET	49738	55420	192.168.2.7	172.111.249.15
Jan 12, 2021 07:20:18.515856981 CET	49738	55420	192.168.2.7	172.111.249.15
Jan 12, 2021 07:20:24.516421080 CET	49738	55420	192.168.2.7	172.111.249.15
Jan 12, 2021 07:20:34.534430981 CET	49755	55420	192.168.2.7	172.111.249.15
Jan 12, 2021 07:20:37.564301014 CET	49755	55420	192.168.2.7	172.111.249.15
Jan 12, 2021 07:20:43.580476046 CET	49755	55420	192.168.2.7	172.111.249.15
Jan 12, 2021 07:20:52.333379030 CET	49756	55420	192.168.2.7	172.111.249.15
Jan 12, 2021 07:20:55.347028017 CET	49756	55420	192.168.2.7	172.111.249.15
Jan 12, 2021 07:21:01.347537994 CET	49756	55420	192.168.2.7	172.111.249.15
Jan 12, 2021 07:21:09.444519997 CET	49759	55420	192.168.2.7	172.111.249.15
Jan 12, 2021 07:21:12.457886934 CET	49759	55420	192.168.2.7	172.111.249.15
Jan 12, 2021 07:21:18.474034071 CET	49759	55420	192.168.2.7	172.111.249.15
Jan 12, 2021 07:21:26.655808926 CET	49760	55420	192.168.2.7	172.111.249.15
Jan 12, 2021 07:21:29.662377119 CET	49760	55420	192.168.2.7	172.111.249.15
Jan 12, 2021 07:21:35.678492069 CET	49760	55420	192.168.2.7	172.111.249.15
Jan 12, 2021 07:21:46.271538019 CET	49761	55420	192.168.2.7	172.111.249.15
Jan 12, 2021 07:21:49.273406982 CET	49761	55420	192.168.2.7	172.111.249.15
Jan 12, 2021 07:21:55.275988102 CET	49761	55420	192.168.2.7	172.111.249.15
Jan 12, 2021 07:22:07.603441954 CET	49762	55420	192.168.2.7	172.111.249.15
Jan 12, 2021 07:22:10.614824057 CET	49762	55420	192.168.2.7	172.111.249.15
Jan 12, 2021 07:22:16.646604061 CET	49762	55420	192.168.2.7	172.111.249.15

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 12, 2021 07:19:18.152117968 CET	54329	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:19:18.200064898 CET	53	54329	8.8.8.8	192.168.2.7
Jan 12, 2021 07:19:18.964063883 CET	58052	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:19:19.011945009 CET	53	58052	8.8.8.8	192.168.2.7
Jan 12, 2021 07:19:19.881375074 CET	54008	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:19:19.937824965 CET	53	54008	8.8.8.8	192.168.2.7
Jan 12, 2021 07:19:21.058495998 CET	59451	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:19:21.106384993 CET	53	59451	8.8.8.8	192.168.2.7
Jan 12, 2021 07:19:22.325422049 CET	52914	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:19:22.373280048 CET	53	52914	8.8.8.8	192.168.2.7
Jan 12, 2021 07:19:23.213429928 CET	64569	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:19:23.264168024 CET	53	64569	8.8.8.8	192.168.2.7
Jan 12, 2021 07:19:24.256078005 CET	52816	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:19:24.304791927 CET	53	52816	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 12, 2021 07:19:26.286309004 CET	50781	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:19:26.342607975 CET	53	50781	8.8.8.8	192.168.2.7
Jan 12, 2021 07:19:27.442418098 CET	54230	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:19:27.490415096 CET	53	54230	8.8.8.8	192.168.2.7
Jan 12, 2021 07:19:28.286562920 CET	54911	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:19:28.337373018 CET	53	54911	8.8.8.8	192.168.2.7
Jan 12, 2021 07:19:29.390938044 CET	49958	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:19:29.438986063 CET	53	49958	8.8.8.8	192.168.2.7
Jan 12, 2021 07:19:30.754242897 CET	50860	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:19:30.802162886 CET	53	50860	8.8.8.8	192.168.2.7
Jan 12, 2021 07:19:35.108879089 CET	50452	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:19:35.160171986 CET	53	50452	8.8.8.8	192.168.2.7
Jan 12, 2021 07:19:37.243352890 CET	59730	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:19:37.302474976 CET	53	59730	8.8.8.8	192.168.2.7
Jan 12, 2021 07:19:40.520523071 CET	59310	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:19:40.580750942 CET	53	59310	8.8.8.8	192.168.2.7
Jan 12, 2021 07:19:40.851744890 CET	51919	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:19:40.902472019 CET	53	51919	8.8.8.8	192.168.2.7
Jan 12, 2021 07:19:42.807303905 CET	64296	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:19:42.868114948 CET	53	64296	8.8.8.8	192.168.2.7
Jan 12, 2021 07:19:48.744684935 CET	56680	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:19:48.792726040 CET	53	56680	8.8.8.8	192.168.2.7
Jan 12, 2021 07:19:54.854744911 CET	58820	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:19:54.915824890 CET	53	58820	8.8.8.8	192.168.2.7
Jan 12, 2021 07:19:58.382730007 CET	60983	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:19:58.441404104 CET	53	60983	8.8.8.8	192.168.2.7
Jan 12, 2021 07:20:06.797521114 CET	49247	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:20:06.857518911 CET	53	49247	8.8.8.8	192.168.2.7
Jan 12, 2021 07:20:07.473124981 CET	52286	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:20:07.529843092 CET	53	52286	8.8.8.8	192.168.2.7
Jan 12, 2021 07:20:10.751045942 CET	56064	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:20:10.811461926 CET	53	56064	8.8.8.8	192.168.2.7
Jan 12, 2021 07:20:15.331238031 CET	63744	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:20:15.387641907 CET	53	63744	8.8.8.8	192.168.2.7
Jan 12, 2021 07:20:18.836529016 CET	61457	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:20:18.921111107 CET	53	61457	8.8.8.8	192.168.2.7
Jan 12, 2021 07:20:19.487760067 CET	58367	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:20:20.192961931 CET	60599	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:20:20.263411999 CET	53	60599	8.8.8.8	192.168.2.7
Jan 12, 2021 07:20:20.547858953 CET	58367	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:20:20.604576111 CET	53	58367	8.8.8.8	192.168.2.7
Jan 12, 2021 07:20:21.196160078 CET	59571	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:20:21.252669096 CET	53	59571	8.8.8.8	192.168.2.7
Jan 12, 2021 07:20:21.264338017 CET	52689	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:20:21.321696043 CET	53	52689	8.8.8.8	192.168.2.7
Jan 12, 2021 07:20:21.808481932 CET	50290	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:20:21.856370926 CET	53	50290	8.8.8.8	192.168.2.7
Jan 12, 2021 07:20:22.473449945 CET	60427	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:20:22.521362066 CET	53	60427	8.8.8.8	192.168.2.7
Jan 12, 2021 07:20:23.164798021 CET	56209	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:20:23.215529919 CET	53	56209	8.8.8.8	192.168.2.7
Jan 12, 2021 07:20:24.170682907 CET	59582	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:20:24.227459908 CET	53	59582	8.8.8.8	192.168.2.7
Jan 12, 2021 07:20:25.426131964 CET	60949	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:20:25.484685898 CET	53	60949	8.8.8.8	192.168.2.7
Jan 12, 2021 07:20:26.502346992 CET	58542	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:20:26.561548948 CET	53	58542	8.8.8.8	192.168.2.7
Jan 12, 2021 07:20:27.169562101 CET	59179	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:20:27.225817919 CET	53	59179	8.8.8.8	192.168.2.7
Jan 12, 2021 07:20:53.947197914 CET	60927	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:20:53.998007059 CET	53	60927	8.8.8.8	192.168.2.7
Jan 12, 2021 07:20:55.887434006 CET	57854	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:20:55.947515965 CET	53	57854	8.8.8.8	192.168.2.7
Jan 12, 2021 07:21:26.595901966 CET	62026	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 12, 2021 07:21:26.653759003 CET	53	62026	8.8.8.8	192.168.2.7
Jan 12, 2021 07:21:46.213160992 CET	59453	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:21:46.269490004 CET	53	59453	8.8.8.8	192.168.2.7
Jan 12, 2021 07:22:07.541016102 CET	62468	53	192.168.2.7	8.8.8.8
Jan 12, 2021 07:22:07.599673986 CET	53	62468	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 12, 2021 07:19:40.520523071 CET	192.168.2.7	8.8.8.8	0x3f71	Standard query (0)	innocentbo oii.hopto.org	A (IP address)	IN (0x0001)
Jan 12, 2021 07:19:58.382730007 CET	192.168.2.7	8.8.8.8	0x4a9b	Standard query (0)	innocentbo oii.hopto.org	A (IP address)	IN (0x0001)
Jan 12, 2021 07:20:15.331238031 CET	192.168.2.7	8.8.8.8	0x241b	Standard query (0)	innocentbo oii.hopto.org	A (IP address)	IN (0x0001)
Jan 12, 2021 07:21:26.595901966 CET	192.168.2.7	8.8.8.8	0xf9bb	Standard query (0)	innocentbo oii.hopto.org	A (IP address)	IN (0x0001)
Jan 12, 2021 07:21:46.213160992 CET	192.168.2.7	8.8.8.8	0x3240	Standard query (0)	innocentbo oii.hopto.org	A (IP address)	IN (0x0001)
Jan 12, 2021 07:22:07.541016102 CET	192.168.2.7	8.8.8.8	0xcfe2	Standard query (0)	innocentbo oii.hopto.org	A (IP address)	IN (0x0001)

DNS Answers

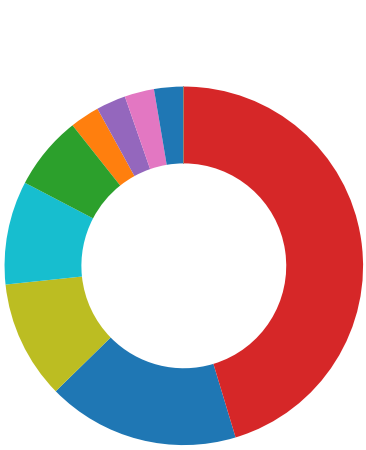
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 12, 2021 07:19:40.580750942 CET	8.8.8.8	192.168.2.7	0x3f71	No error (0)	innocentbo oii.hopto.org		172.111.249.15	A (IP address)	IN (0x0001)
Jan 12, 2021 07:19:58.441404104 CET	8.8.8.8	192.168.2.7	0x4a9b	No error (0)	innocentbo oii.hopto.org		172.111.249.15	A (IP address)	IN (0x0001)
Jan 12, 2021 07:20:15.387641907 CET	8.8.8.8	192.168.2.7	0x241b	No error (0)	innocentbo oii.hopto.org		172.111.249.15	A (IP address)	IN (0x0001)
Jan 12, 2021 07:21:26.653759003 CET	8.8.8.8	192.168.2.7	0xf9bb	No error (0)	innocentbo oii.hopto.org		172.111.249.15	A (IP address)	IN (0x0001)
Jan 12, 2021 07:21:46.269490004 CET	8.8.8.8	192.168.2.7	0x3240	No error (0)	innocentbo oii.hopto.org		172.111.249.15	A (IP address)	IN (0x0001)
Jan 12, 2021 07:22:07.599673986 CET	8.8.8.8	192.168.2.7	0xcfe2	No error (0)	innocentbo oii.hopto.org		172.111.249.15	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

- Scan002.exe.exe
- schtasks.exe
- conhost.exe
- Scan002.exe.exe
- schtasks.exe
- conhost.exe
- schtasks.exe
- conhost.exe
- Scan002.exe.exe
- dhcpmon.exe
- schtasks.exe
- conhost.exe
- Scan002.exe.exe
- dhcpmon.exe
- schtasks.exe
- conhost.exe
- dhcpmon.exe
- dhcpmon.exe



Click to jump to process

System Behavior

Analysis Process: Scan002.exe.exe PID: 2960 Parent PID: 5600

General

Start time:	07:19:21
Start date:	12/01/2021
Path:	C:\Users\user\Desktop\Scan002.exe.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Scan002.exe.exe'
Imagebase:	0x320000
File size:	910848 bytes
MD5 hash:	8E2315D05C47FEFDDDF0A686BF9E353E
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: 00000000.00000002.254700153.0000000003D97000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.254700153.0000000003D97000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.254700153.0000000003D97000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	724660AC	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	724660AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\UbebSiSIKndjd.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	4E70AC7	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp1945.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	719F9869	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Scan002.exe.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	724534A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1945.tmp	success or wait	1	4E717EE	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\UbebSiSIKndjd.exe	unknown	910848	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 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 88 cc fc 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 da 0d 00 00 0a 00 00 00 00 00 00 4e f8 0d 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 40 0e 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......_.......... ....N.... ....@.. ....@ ....@.................	success or wait	1	4E70D4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1945.tmp	unknown	1662	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </Registrati	success or wait	1	4E70D4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Scan002.exe.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	7273A33A	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	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72498738	ReadFile
C:\Users\user\Desktop\Scan002.exe.exe	unknown	910848	success or wait	1	4E70D4F	ReadFile

Analysis Process: schtasks.exe PID: 4564 Parent PID: 2960

General

Start time:	07:19:32
Start date:	12/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\UbebSiSIKndjd' /XML 'C:\Users\user\AppData\Local\Temp\tmp1945.tmp'
Imagebase:	0x12a0000
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\tmp1945.tmp	unknown	2	success or wait	1	12AAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp1945.tmp	unknown	1663	success or wait	1	12AABD9	ReadFile

Analysis Process: conhost.exe PID: 5348 Parent PID: 4564

General

Start time:	07:19:32
Start date:	12/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: Scan002.exe.exe PID: 4340 Parent PID: 2960

General

Start time:	07:19:33
Start date:	12/01/2021
Path:	C:\Users\user\Desktop\Scan002.exe.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xd30000
File size:	910848 bytes
MD5 hash:	8E2315D05C47FEFDDDF0A686BF9E353E

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: 00000003.00000002.596528786.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.596528786.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.596528786.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.609798776.0000000005F80000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.609798776.0000000005F80000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.607959083.0000000004717000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.607959083.0000000004717000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.609917775.00000000060D0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.609917775.00000000060D0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.610027032.0000000006220000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.610027032.0000000006220000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.610027032.0000000006220000.00000004.00000001.sdmp, Author: Joe Security
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	724660AC	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	724660AC	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	33407A1	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	334089B	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	33407A1	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	3340B20	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	3340B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp8ED7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	3340DCC	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	334089B	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp91C6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	3340DCC	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	33407A1	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	33407A1	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	724660AC	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	724660AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8ED7.tmp	success or wait	1	151BF0E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmp91C6.tmp	success or wait	1	151BF0E	DeleteFileW
C:\Users\user\Desktop\Scan002.exe.exe:Zone.Identifier	success or wait	1	33411FD	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	unknown	8	e5 f5 ce 77 0d b7 d8 48	...w...H	success or wait	1	3340A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 88 cc fc 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 da 0d 00 00 0a 00 00 00 00 00 00 4e f8 0d 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 0e 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......_.......... ....N.... ....@.. ....@ ....@.................	success or wait	4	3340B20	CopyFileW
C:\Program Files (x86)\DHCP Mo nitor\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	3340B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp8ED7.tmp	unknown	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.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveTo ken</LogonType>	success or wait	1	3340A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	42	43 3a 5c 55 73 65 72 73 5c 66 72 6f 6e 74 64 65 73 6b 5c 44 65 73 6b 74 6f 70 5c 53 63 61 6e 30 30 32 2e 65 78 65 2e 65 78 65	C:\Users\user\Desktop\Sc an002.exe.exe	success or wait	1	3340A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp91C6.tmp	unknown	1310	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	3340A53	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	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72498738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7253BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7253BF06	unknown
C:\Users\user\Desktop\Scan002.exe.exe	unknown	4096	success or wait	1	7253BF06	unknown
C:\Users\user\Desktop\Scan002.exe.exe	unknown	512	success or wait	1	7253BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	3340A53	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	3340C12	RegSetValueExW

Analysis Process: schtasks.exe PID: 4260 Parent PID: 4340

General

Start time:	07:19:34
Start date:	12/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp8ED7.tmp'

Imagebase:	0x12a0000
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\tmp8ED7.tmp	unknown	2	success or wait	1	12AAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp8ED7.tmp	unknown	1306	success or wait	1	12AABD9	ReadFile

Analysis Process: conhost.exe PID: 5412 Parent PID: 4260

General

Start time:	07:19:35
Start date:	12/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: 976 Parent PID: 4340

General

Start time:	07:19:35
Start date:	12/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp91C6.tmp'
Imagebase:	0x12a0000
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\tmp91C6.tmp	unknown	2	success or wait	1	12AAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp91C6.tmp	unknown	1311	success or wait	1	12AABD9	ReadFile

Analysis Process: conhost.exe PID: 4812 Parent PID: 976

General

Start time:	07:19:35
Start date:	12/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: Scan002.exe.exe PID: 204 Parent PID: 1104

General

Start time:	07:19:36
Start date:	12/01/2021
Path:	C:\Users\user\Desktop\Scan002.exe.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Scan002.exe.exe 0
Imagebase:	0xa00000
File size:	910848 bytes
MD5 hash:	8E2315D05C47FEFDDDF0A686BF9E353E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.278150561.0000000004427000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.278150561.0000000004427000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.278150561.0000000004427000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	724660AC	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	724660AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp414F.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	719F9869	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp414F.tmp	success or wait	1	6CF171E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp414F.tmp	unknown	1662	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </Registrati	success or wait	1	6CF13DB	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	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72498738	ReadFile

Analysis Process: dhcpmon.exe PID: 5396 Parent PID: 1104

General

Start time:	07:19:39
Start date:	12/01/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x7a0000
File size:	910848 bytes
MD5 hash:	8E2315D05C47FEFDDDF0A686BF9E353E
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: 0000000A.00000002.274234683.0000000004167000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.274234683.0000000004167000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.274234683.0000000004167000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000A.00000002.270860826.0000000002E41000.00000004.00000001.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	724660AC	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	724660AC	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	724534A7	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	7273A33A	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	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72498738	ReadFile

Analysis Process: schtasks.exe PID: 5876 Parent PID: 204

General

Start time:	07:19:42
Start date:	12/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\UbebSiSIKndjd' /XML 'C:\Users\user\AppData\Local\Temp\tmp414F.tmp'
Imagebase:	0x12a0000
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\tmp414F.tmp	unknown	2	success or wait	1	12AAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp414F.tmp	unknown	1663	success or wait	1	12AABD9	ReadFile

Analysis Process: conhost.exe PID: 2160 Parent PID: 5876

General

Start time:	07:19:43
Start date:	12/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: Scan002.exe.exe PID: 4260 Parent PID: 204

General

Start time:	07:19:43
Start date:	12/01/2021

Path:	C:\Users\user\Desktop\Scan002.exe.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x660000
File size:	910848 bytes
MD5 hash:	8E2315D05C47FEFDDDF0A686BF9E353E
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: 0000000D.00000002.286646772.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.286646772.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.286646772.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.287923771.0000000003D11000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.287923771.0000000003D11000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.287850073.0000000002D11000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.287850073.0000000002D11000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	724660AC	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	724660AC	unknown

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	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72498738	ReadFile

Analysis Process: dhcpmon.exe PID: 2160 Parent PID: 3292

General

Start time:	07:19:47
Start date:	12/01/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xe10000
File size:	910848 bytes
MD5 hash:	8E2315D05C47FEFDDDF0A686BF9E353E

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: 0000000F.00000002.303779219.00000000047B7000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.303779219.00000000047B7000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.303779219.00000000047B7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.302951058.0000000004491000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.302951058.0000000004491000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.302951058.0000000004491000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: schtasks.exe PID: 6608 Parent PID: 2160

General

Start time:	07:19:52
Start date:	12/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\UbebSiSIKndjd' /XML 'C:\Users\user\AppData\Local\Temp\tmp65AF.tmp'
Imagebase:	0x12a0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 6644 Parent PID: 6608

General

Start time:	07:19:52
Start date:	12/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: 6712 Parent PID: 2160

General

Start time:	07:19:53
Start date:	12/01/2021

Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x130000
File size:	910848 bytes
MD5 hash:	8E2315D05C47FEFDDDF0A686BF9E353E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: 6744 Parent PID: 2160

General

Start time:	07:19:53
Start date:	12/01/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x3f0000
File size:	910848 bytes
MD5 hash:	8E2315D05C47FEFDDDF0A686BF9E353E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: 6764 Parent PID: 2160

General

Start time:	07:19:54
Start date:	12/01/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xb90000
File size:	910848 bytes
MD5 hash:	8E2315D05C47FEFDDDF0A686BF9E353E
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: 0000001B.00000002.313206635.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000002.313206635.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000002.313206635.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000002.314650471.00000000043B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000002.314650471.00000000043B1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001B.00000002.314577877.00000000033B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001B.00000002.314577877.00000000033B1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Disassembly

Code Analysis