ID: 341408
Sample Name: Doc.exe
Cookbook: default.jbs
Time: 10:22:14
Date: 19/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

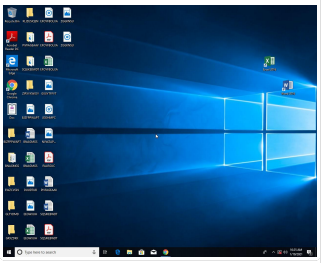
Analysis Report Doc.exe

Overview

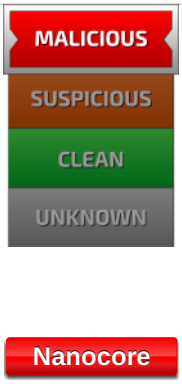
General Information

Sample Name:	Doc.exe
Analysis ID:	341408
MD5:	c853495818db3fd.
SHA1:	51dfa28d2bf0af4…
SHA256:	799087f4f62932d..
Tags:	exe NanoCore RAT Yahoo

Most interesting Screenshot:



Detection



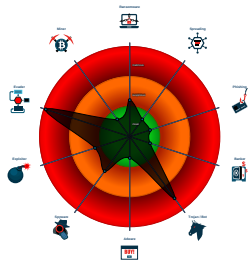
Nanocore

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

Signatures

- Detected Nanocore Rat
- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Binary contains a suspicious time st…

Classification



Startup

- **System is w10x64**
- Doc.exe (PID: 1460 cmdline: 'C:\Users\user\Desktop\Doc.exe' MD5: C853495818DB3FDDF333CE3EAF5E6CC3)
  - schtasks.exe (PID: 5744 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\dEkaSoUjP' /XML 'C:\Users\user\AppData\Local\Temp\tmp58A2.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6112 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Doc.exe (PID: 5784 cmdline: {path} MD5: C853495818DB3FDDF333CE3EAF5E6CC3)
  - Doc.exe (PID: 3848 cmdline: {path} MD5: C853495818DB3FDDF333CE3EAF5E6CC3)
    - schtasks.exe (PID: 5536 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpD558.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5336 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5316 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpD876.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5328 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Doc.exe (PID: 1112 cmdline: C:\Users\user\Desktop\Doc.exe 0 MD5: C853495818DB3FDDF333CE3EAF5E6CC3)
  - schtasks.exe (PID: 6476 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\dEkaSoUjP' /XML 'C:\Users\user\AppData\Local\Temp\tmpB420.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6484 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Doc.exe (PID: 6524 cmdline: {path} MD5: C853495818DB3FDDF333CE3EAF5E6CC3)
- dhcpmon.exe (PID: 3720 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: C853495818DB3FDDF333CE3EAF5E6CC3)
- dhcpmon.exe (PID: 6328 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: C853495818DB3FDDF333CE3EAF5E6CC3)
  - schtasks.exe (PID: 6848 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\dEkaSoUjP' /XML 'C:\Users\user\AppData\Local\Temp\tmpDD04.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6860 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 6928 cmdline: {path} MD5: C853495818DB3FDDF333CE3EAF5E6CC3)
- **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
0000001C.00000002.364409050.000000000456 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000001C.00000002.364409050.000000000456 1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x4ea7d:$a: NanoCore • 0x4ead6:$a: NanoCore • 0x4eb13:$a: NanoCore • 0x4eb8c:$a: NanoCore • 0x54121:$a: NanoCore • 0x5416b:$a: NanoCore • 0x54355:$a: NanoCore • 0x67c74:$a: NanoCore • 0x67c89:$a: NanoCore • 0x67cbe:$a: NanoCore • 0x80c13:$a: NanoCore • 0x80c28:$a: NanoCore • 0x80c5d:$a: NanoCore • 0x4eadf:$b: ClientPlugin • 0x4eb1c:$b: ClientPlugin • 0x4f41a:$b: ClientPlugin • 0x4f427:$b: ClientPlugin • 0x53eba:$b: ClientPlugin • 0x5412a:$b: ClientPlugin • 0x54174:$b: ClientPlugin • 0x67a30:$b: ClientPlugin
00000016.00000002.339391381.0000000003D2 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000016.00000002.339391381.0000000003D2 1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x4ea7d:$a: NanoCore • 0x4ead6:$a: NanoCore • 0x4eb13:$a: NanoCore • 0x4eb8c:$a: NanoCore • 0x54121:$a: NanoCore • 0x5416b:$a: NanoCore • 0x54355:$a: NanoCore • 0x67c74:$a: NanoCore • 0x67c89:$a: NanoCore • 0x67cbe:$a: NanoCore • 0x80c13:$a: NanoCore • 0x80c28:$a: NanoCore • 0x80c5d:$a: NanoCore • 0x4eadf:$b: ClientPlugin • 0x4eb1c:$b: ClientPlugin • 0x4f41a:$b: ClientPlugin • 0x4f427:$b: ClientPlugin • 0x53eba:$b: ClientPlugin • 0x5412a:$b: ClientPlugin • 0x54174:$b: ClientPlugin • 0x67a30:$b: ClientPlugin
0000001C.00000002.361008474.000000000040 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
Click to see the 38 entries				

Unpacked PEs

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

Source	Rule	Description	Author	Strings
28.2.dhcpmon.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:$j: #=q
6.2.Doc.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 7 entries				

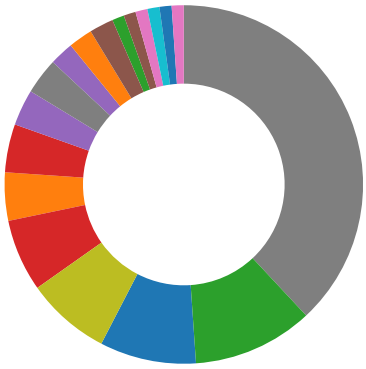
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



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

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Uses new MSVCR Dlls

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

Networking:

C2 URLs / IPs found in malware configuration

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)

PE file contains section with special chars

PE file has nameless sections

Data Obfuscation:

Detected unpacking (changes PE section rights)

.NET source code contains potential unpacker

Binary contains a suspicious time stamp

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)

Anti Debugging:

Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

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:

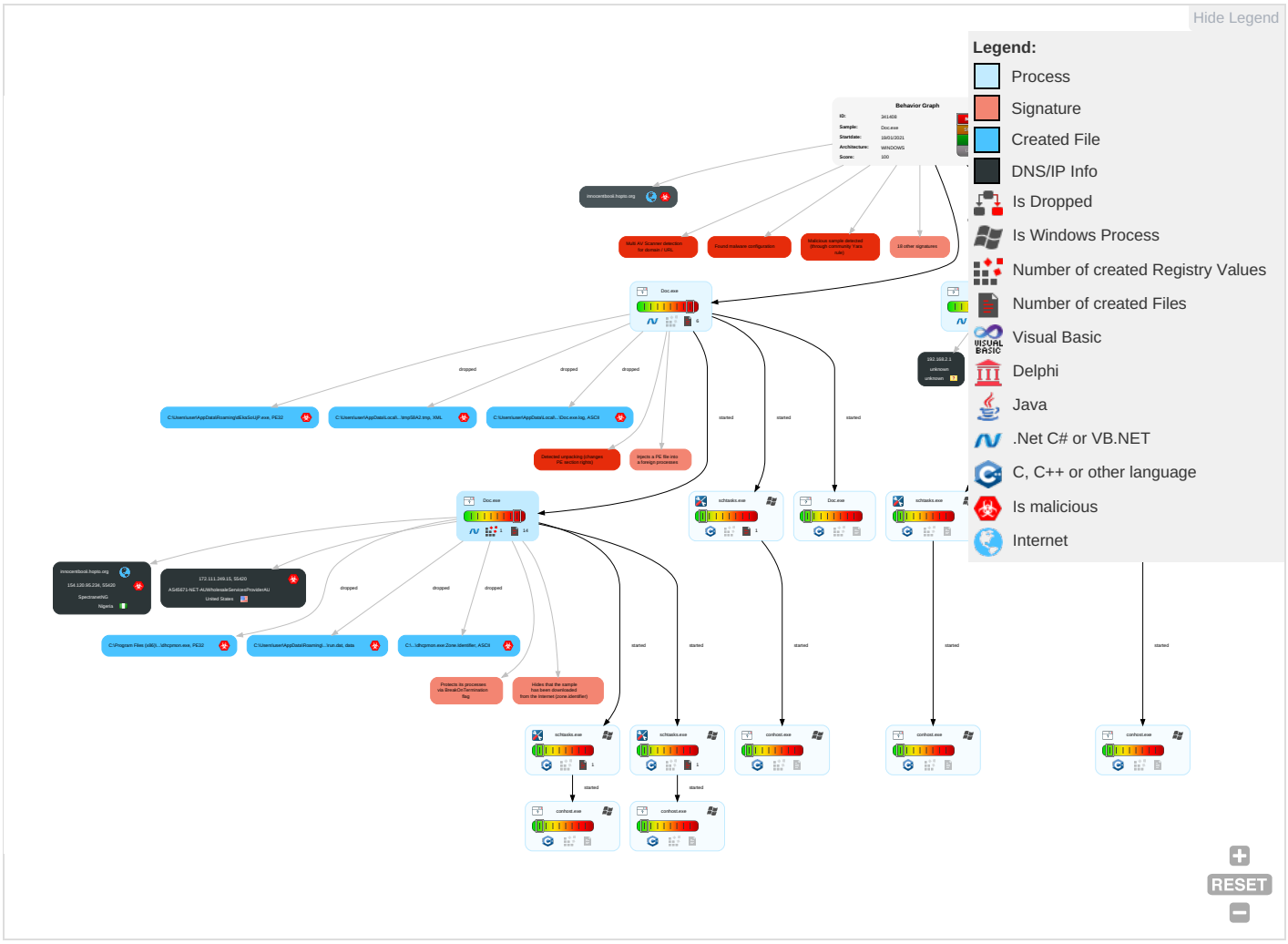
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comman and Cont
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Access Token Manipulation 1	Masquerading 2	Input Capture 2 1	Security Software Discovery 3 2 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Virtualization/Sandbox Evasion 4	LSASS Memory	Virtualization/Sandbox Evasion 4	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Stan Port 1
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	Remote A Software
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	Non-Applicatio Layer Protocol
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 1 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Applicatio Layer Protocol
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	System Information Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonl Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicatio Layer Pro
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 2 3	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Prot
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Timestomp 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Trans Protocols

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Doc.exe	33%	Virustotal		Browse
Doc.exe	39%	ReversingLabs	ByteCode-MSIL.Trojan.Tnega	
Doc.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\dEkaSoUjP.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	39%	ReversingLabs	ByteCode-MSIL.Trojan.Tnega	
C:\Users\user\AppData\Roaming\dEkaSoUjP.exe	39%	ReversingLabs	ByteCode-MSIL.Trojan.Tnega	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.Doc.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
19.2.dhcpmon.exe.680000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
22.2.Doc.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
15.2.dhcpmon.exe.4a0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.Doc.exe.dd0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.Doc.exe.e70000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
innocentbooii.hopto.org	10%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comI.TTF	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/H	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnX	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.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.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/6	0%	Avira URL Cloud	safe	
http://www.fontbureau.comrz	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.fontbureau.comoA	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comB.TTFe	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/6	0%	Avira URL Cloud	safe	
http://www.carterandcone.com7	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/n-u	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/l	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.carterandcone.comei	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/S	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.jiyu-kobo.co.jp/$	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	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.fontbureau.comoitul	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.carterandcone.com_	0%	Avira URL Cloud	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.carterandcone.come	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/S	0%	Avira URL Cloud	safe	
http://www.carterandcone.coms	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/A	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.zhongyicts.com.cne	0%	Avira URL Cloud	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://en.w	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.zhongyicts.com.cnk	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/k-s	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/w	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
innocentbooii.hopto.org	154.120.95.234	true	true	• 10%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	Doc.exe, 00000000.00000002.282380576.0000000008250000.00000002.00000001.sdmp, Doc.exe, 00000000D.00000002.333252045.0000000005D20000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.000000002.331234081.0000000005F40000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.357623628.0000000007B20000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comI.TTF	Doc.exe, 00000000.00000003.250034531.00000000080E5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	Doc.exe, 00000000.00000002.282380576.0000000008250000.00000002.00000001.sdmp, Doc.exe, 00000000D.00000002.333252045.0000000005D20000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.000000002.331234081.0000000005F40000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.357623628.0000000007B20000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Doc.exe, 00000000.00000002.282380576.0000000008250000.00000002.00000001.sdmp, Doc.exe, 00000000D.00000002.333252045.0000000005D20000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.000000002.331234081.0000000005F40000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.357623628.0000000007B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Doc.exe, 00000000.00000002.282380576.0000000008250000.00000002.00000001.sdmp, Doc.exe, 00000000D.00000002.333252045.0000000005D20000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.000000002.331234081.0000000005F40000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.357623628.0000000007B20000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/H	Doc.exe, 00000000.00000003.246604071.00000000080E5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnX	Doc.exe, 00000000.00000003.244615811.00000000080E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	dhcpmon.exe, 00000013.00000002.357623628.0000000007B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	dhcpmon.exe, 00000013.00000002.357623628.0000000007B20000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	Doc.exe, 00000000.00000002.282380576.0000000008250000.00000002.00000001.sdmp, Doc.exe, 00000000D.00000002.333252045.0000000005D20000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.000000002.331234081.0000000005F40000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.357623628.0000000007B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	Doc.exe, 00000000.00000003.245346506.00000000080E1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/6	Doc.exe, 00000000.00000003.246853689.00000000080DC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comrz	Doc.exe, 00000000.00000003.272311376.00000000080DC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	Doc.exe, 00000000.00000002.282380576.0000000008250000.00000002.00000001.sdmp, Doc.exe, 00000000D.00000002.333252045.0000000005D20000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.331234081.0000000005F40000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.357623628.0000000007B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Doc.exe, 00000000.00000002.282380576.0000000008250000.00000002.00000001.sdmp, Doc.exe, 00000000D.00000002.333252045.0000000005D20000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.331234081.0000000005F40000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.357623628.0000000007B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comoA	Doc.exe, 00000000.00000003.250034531.00000000080E5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/cThe	Doc.exe, 00000000.00000002.282380576.0000000008250000.00000002.00000001.sdmp, Doc.exe, 00000000D.00000002.333252045.0000000005D20000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.331234081.0000000005F40000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.357623628.0000000007B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Doc.exe, 00000000.00000002.282380576.0000000008250000.00000002.00000001.sdmp, Doc.exe, 00000000.00000003.251014283.00000000080E6000.00000004.00000001.sdmp, Doc.exe, 0000000D.00000002.333252045.0000000005D20000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.331234081.0000000005F40000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.357623628.0000000007B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Doc.exe, 00000000.00000002.282380576.0000000008250000.00000002.00000001.sdmp, Doc.exe, 00000000D.00000002.333252045.0000000005D20000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.331234081.0000000005F40000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.357623628.0000000007B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comB.TTFe	Doc.exe, 00000000.00000003.272311376.00000000080DC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/6	Doc.exe, 00000000.00000003.246604071.00000000080E5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.com7	Doc.exe, 00000000.00000003.245285187.00000000080E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/0	Doc.exe, 00000000.00000003.246604071.00000000080E5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/n-u	Doc.exe, 00000000.00000003.246604071.00000000080E5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/l	Doc.exe, 00000000.00000003.246604071.00000000080E5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

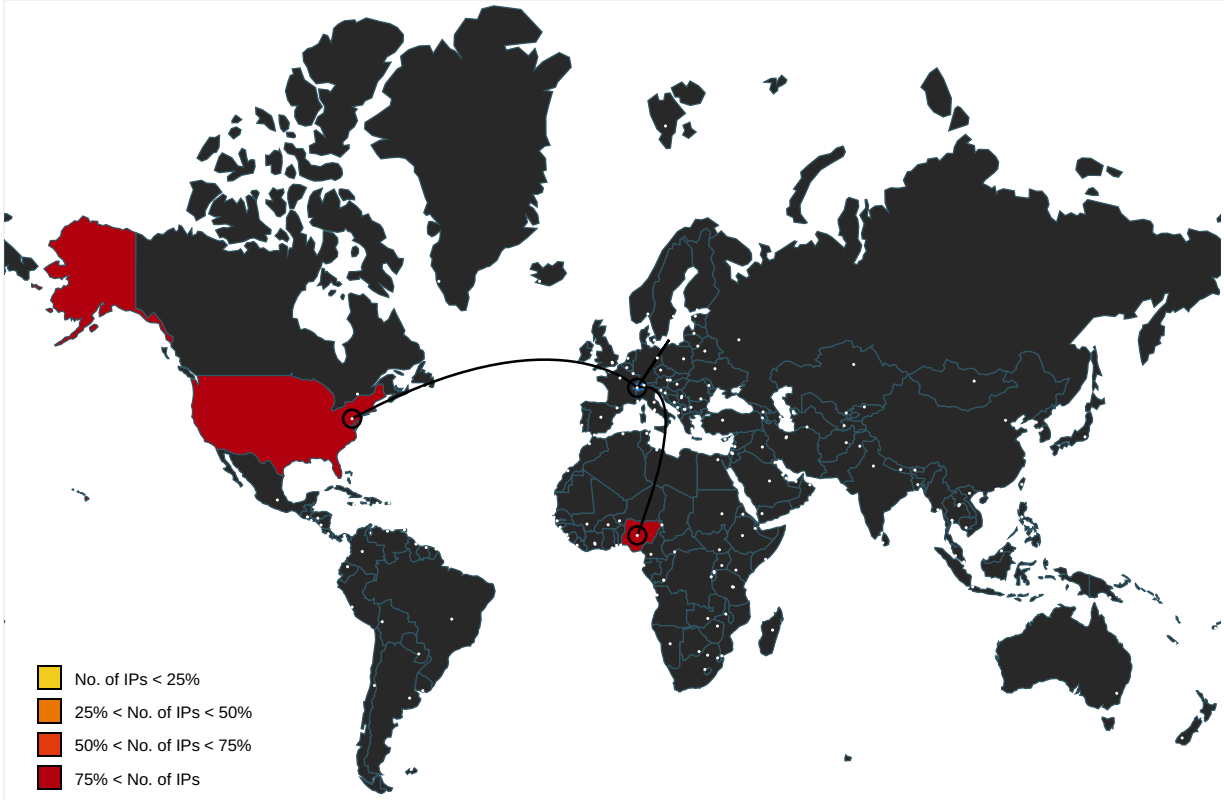
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/DPlease	Doc.exe, 00000000.00000002.282380576.0000000008250000.00000002.00000001.sdmp, Doc.exe, 00000000D.00000002.333252045.0000000005D20000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.331234081.0000000005F40000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.357623628.0000000007B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comei	Doc.exe, 00000000.00000003.245346506.00000000080E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	Doc.exe, 00000000.00000002.282380576.0000000008250000.00000002.00000001.sdmp, Doc.exe, 00000000D.00000002.333252045.0000000005D20000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.331234081.0000000005F40000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.357623628.0000000007B20000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	Doc.exe, 00000000.00000002.282380576.0000000008250000.00000002.00000001.sdmp, Doc.exe, 00000000D.00000002.333252045.0000000005D20000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.331234081.0000000005F40000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.357623628.0000000007B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/jp/S	Doc.exe, 00000000.00000003.246604071.00000000080E5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	Doc.exe, 00000000.00000002.282380576.0000000008250000.00000002.00000001.sdmp, Doc.exe, 00000000D.00000002.333252045.0000000005D20000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.331234081.0000000005F40000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.357623628.0000000007B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/$	Doc.exe, 00000000.00000003.246980374.00000000080DB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn	Doc.exe, 00000000.00000002.282380576.0000000008250000.00000002.00000001.sdmp, Doc.exe, 00000000D.00000002.333252045.0000000005D20000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.331234081.0000000005F40000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.357623628.0000000007B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.como.	Doc.exe, 00000000.00000003.245346506.00000000080E1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	Doc.exe, 00000000.00000002.282380576.0000000008250000.00000002.00000001.sdmp, Doc.exe, 00000000D.00000002.333252045.0000000005D20000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.331234081.0000000005F40000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.357623628.0000000007B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comoitul	Doc.exe, 00000000.00000003.250034531.00000000080E5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	Doc.exe, 00000000.00000002.282380576.0000000008250000.00000002.00000001.sdmp, Doc.exe, 00000000D.00000002.333252045.0000000005D20000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.331234081.0000000005F40000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.357623628.0000000007B20000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	Doc.exe, 00000000.00000002.282380576.0000000008250000.00000002.00000001.sdmp, Doc.exe, 00000000D.00000002.333252045.0000000005D20000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.331234081.0000000005F40000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.357623628.0000000007B20000.00000002.00000001.sdmp	false		high
http://www.galapagosdesign.com/	Doc.exe, 00000000.00000003.251014283.00000000080E6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com_	Doc.exe, 00000000.00000003.245346506.00000000080E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.come	Doc.exe, 00000000.00000003.245285187.00000000080E1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/S	Doc.exe, 00000000.00000003.246301474.00000000080D4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coms	Doc.exe, 00000000.00000003.245346506.00000000080E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/A	Doc.exe, 00000000.00000003.246853689.00000000080DC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	Doc.exe, 00000000.00000003.246853689.00000000080DC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.coma	Doc.exe, 00000000.00000003.272311376.00000000080DC000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cne	Doc.exe, 00000000.00000003.245099691.00000000080E0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comd	Doc.exe, 00000000.00000003.250034531.00000000080E5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://en.w	Doc.exe, 00000000.00000003.245606571.00000000080E5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	Doc.exe, 00000000.00000002.282380576.0000000008250000.00000002.00000001.sdmp, Doc.exe, 00000000D.00000002.333252045.0000000005D20000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.331234081.0000000005F40000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.357623628.0000000007B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cnk	Doc.exe, 00000000.00000003.245346506.00000000080E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/	Doc.exe, 00000000.00000003.244615811.00000000080E1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/k-s	Doc.exe, 00000000.00000003.246604071.00000000080E5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.htmlN	Doc.exe, 00000000.00000002.282380576.0000000008250000.00000002.00000001.sdmp, Doc.exe, 00000000D.00000002.333252045.0000000005D20000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.331234081.0000000005F40000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.357623628.0000000007B20000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/w	Doc.exe, 00000000.00000003.246604071.00000000080E5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	Doc.exe, 00000000.00000003.244615811.00000000080E1000.00000004.00000001.sdmp, Doc.exe, 00000000.00000003.244042748.00000000080E0000.00000004.00000001.sdmp, Doc.exe, 0000000D.00000002.333252045.0000000005D20000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.331234081.0000000005F40000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.357623628.0000000007B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn_	Doc.exe, 00000000.00000003.245099691.00000000080E0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designers/frere-jones.html	Doc.exe, 00000000.00000002.282380576.0000000008250000.00000002.00000001.sdmp, Doc.exe, 00000000D.00000002.333252045.0000000005D20000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.331234081.0000000005F40000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.357623628.0000000007B20000.00000002.00000001.sdmp	false		high
http://www.carterandcone.comy	Doc.exe, 00000000.00000003.245346506.00000000080E1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comm	Doc.exe, 00000000.00000003.250034531.00000000080E5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	Doc.exe, 00000000.00000003.246604071.00000000080E5000.00000004.00000001.sdmp, Doc.exe, 00000000D.00000002.333252045.0000000005D20000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.331234081.0000000005F40000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.357623628.0000000007B20000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/l	Doc.exe, 00000000.00000003.246461974.00000000080D7000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Doc.exe, 00000000.00000002.282380576.0000000008250000.00000002.00000001.sdmp, Doc.exe, 00000000D.00000002.333252045.0000000005D20000.00000002.00000001.sdmp, dhcpmon.exe, 0000000F.00000002.331234081.0000000005F40000.00000002.00000001.sdmp, dhcpmon.exe, 00000013.00000002.357623628.0000000007B20000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/i-f	Doc.exe, 00000000.00000003.246604071.00000000080E5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comals	Doc.exe, 00000000.00000003.250034531.00000000080E5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn&	Doc.exe, 00000000.00000003.244057616.00000000080E6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comitud	Doc.exe, 00000000.00000003.250034531.00000000080E5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://tempuri.org/CSMDataSet.xsd	dhcpmon.exe, 00000013.00000002.350486647.0000000003024000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Y0ldZ	Doc.exe, 00000000.00000003.246604071.00000000080E5000.00000004.00000001.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
154.120.95.234	unknown	Nigeria		37340	SpectranetNG	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	341408
Start date:	19.01.2021
Start time:	10:22:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 2s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	Doc.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@27/12@5/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 5.1% (good quality ratio 2.8%) • Quality average: 39.3% • Quality standard deviation: 39.3%
HCA Information:	• Successful, ratio: 89% • 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, HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.43.139.144, 92.122.144.200, 40.88.32.150, 51.103.5.159, 51.11.168.160, 92.122.213.194, 92.122.213.247, 20.54.26.129, 52.254.96.93 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, arc.msn.com.nsatc.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, bn2eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus16.cloudapp.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, ris.api.iris.microsoft.com, skypedataprdcoleus15.cloudapp.net, emea1.notify.windows.com.akadns.net, blobcollector.events.data.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, par02p.wns.notify.trafficmanager.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
10:23:16	API Interceptor	1148x Sleep call for process: Doc.exe modified
10:23:28	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\Doc.exe" s>$(Arg0)
10:23:30	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
10:23:30	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
10:23:43	API Interceptor	3x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.111.249.15	Scan002.exe.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
innocentbooii.hopto.org	Scan002.exe.exe	Get hash	malicious	Browse	• 172.111.249.15
	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	Scan002.exe.exe	Get hash	malicious	Browse	• 172.111.249.15
	http://s3-eu-west-1.amazonaws.com/hjdpjni/ogbim#qs=r-acacaeeikdgeadkieeefjaehbihababababaefahcaccajbiackdcagfkbkacb	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
	lRxIRaWSZK.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
SpectranetNG	0712020.exe	Get hash	malicious	Browse	• 41.217.69.179
	49221o3F5N.exe	Get hash	malicious	Browse	• 41.217.64.43
	0LGpT3WYf1.exe	Get hash	malicious	Browse	• 154.120.96.115

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PURCHASE ORDER TOUSE IMPORT& EXPORT CO. ,LTD.ZIP FILE.exe	Get hash	malicious	Browse	• 41.217.62.17
	INV9938884.exe	Get hash	malicious	Browse	• 154.118.49.103
	bedrapes.exe	Get hash	malicious	Browse	• 154.118.68.3
	5Shipment 09252018 - Ship REPORT WEEK 37.exe	Get hash	malicious	Browse	• 197.242.116.57
	7Statement of account.exe	Get hash	malicious	Browse	• 154.118.3.123
	26SHIPMENT PASSED-Draft BL, Packing list.exe	Get hash	malicious	Browse	• 197.242.99.110
	Property Enquiry Ref-00255487453342065334.exe	Get hash	malicious	Browse	• 154.120.125.40
	59Purchase order.exe	Get hash	malicious	Browse	• 197.242.11 9.100
	42Invoice.exe	Get hash	malicious	Browse	• 154.118.11.196
	DHL correction form.exe	Get hash	malicious	Browse	• 41.217.118.185
	3Doc_EZ19029587.js	Get hash	malicious	Browse	• 154.120.12 1.109
	3Doc_EZ19029587.js	Get hash	malicious	Browse	• 154.120.12 1.109

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\Doc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1530880
Entropy (8bit):	7.361237861080968
Encrypted:	false
SSDEEP:	24576:uPoF365K8SDEXOkK3xtBi2H+N/ntbYZ0PNK1XtCIix:uAF3UK8UEekcxi24lDlK5g
MD5:	C853495818DB3FDDF333CE3EAF5E6CC3
SHA1:	51DFA28D2BF0AF44DE903FA80E4458110155F34B
SHA-256:	799087F4F62932DBE6405946E5FC9215C9DF899909C15F0C1D876EC28E9436B0
SHA-512:	1015EF73002C3221F8386F6E39CA2806F1662650001BE1DD8ACDAC02652D876AB2DA55E07ECF9612F6FDD39F8962A38EB07A034332A13BD39882BA71A9CC7B2
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 39%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...z.....0.....T..... ....@.. ....@..... ...K.....H.....2)-..Lp$(.... .....@....text..... ..`.rsrc..... .....@..@.reloc.....X.....@..B.....Z..... ..` ....

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

Process:	C:\Users\user\Desktop\Doc.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**
Reputation:	high, very likely benign file

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Preview:	[ZoneTransfer]....ZoneId=0

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

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

C:\Users\user\AppData\Local\Temp\tmp58A2.tmp	
Process:	C:\Users\user\Desktop\Doc.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1646
Entropy (8bit):	5.168874231313252
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBW2tn:cbhC7ZlNQF/rydbz9I3YODOLNdq3QA
MD5:	CE1BE564A3A2FC5A84B77D871C48403A
SHA1:	72FCBAD1A719615F75EA5DB50F5E2C42C057B408
SHA-256:	E658B7A017F5F96155CFEEFB68260E340ACA2185A4C3CB59FA5933B327C93A15
SHA-512:	C91296EF7400A0B7597B11B1871672D3930E01B015C82E463EE47482D24D0B77272058FFA2B2ED252FAD13B087F4BC080630D8FA61628AE4E1FFBA74A73B35A7
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

C:\Users\user\AppData\Local\Temp\tmpB420.tmp	
Process:	C:\Users\user\Desktop\Doc.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1646
Entropy (8bit):	5.168874231313252

C:\Users\user\AppData\Local\Temp\tmpB420.tmp	
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBW2tn:cbhC7ZlNQF/rydbz9I3YODOLNdq3QA
MD5:	CE1BE564A3A2FC5A84B77D871C48403A
SHA1:	72FCBAD1A719615F75EA5DB50F5E2C42C057B408
SHA-256:	E658B7A017F5F96155CFEEFB68260E340ACA2185A4C3CB59FA5933B327C93A15
SHA-512:	C91296EF7400A0B7597B11B1871672D3930E01B015C82E463EE47482D24D0B77272058FFA2B2ED252FAD13B087F4BC080630D8FA61628AE4E1FFBA74A73B35A7
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>.. <StartWhenAvailable>t

C:\Users\user\AppData\Local\Temp\tmpD558.tmp	
Process:	C:\Users\user\Desktop\Doc.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1294
Entropy (8bit):	5.089166573730756
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0P8xtn:cbk4oL600QydbQxIYODOLedq3S8j
MD5:	A248EE7904DBB7192DE9B87A0C445935
SHA1:	46D3C56F28A5D6E8AE17F722D37D1F9A7E28D851
SHA-256:	A17BEEC25E493B9B4B2534770C25F2E667F84498910668191 13B6E5DB3FF68FA
SHA-512:	5BE95F18C4089084ED90FED40D52D23F9EE8CCC73F1B273F481EDCF194F0403C5C9BFB52674EB845BFDF2724AC558C5747988872EA7926E5CD310C0EC1D684D
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\tmpD876.tmp	
Process:	C:\Users\user\Desktop\Doc.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\Local\Temp\tmpDD04.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):	1646
Entropy (8bit):	5.168874231313252
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBW2tn:cbhC7ZlNQF/rydbz9I3YODOLNdq3QA
MD5:	CE1BE564A3A2FC5A84B77D871C48403A
SHA1:	72FCBAD1A719615F75EA5DB50F5E2C42C057B408

C:\Users\user\AppData\Local\Temp\tmpDD04.tmp	
SHA-256:	E658B7A017F5F96155CFEEFB68260E340ACA2185A4C3CB59FA5933B327C93A15
SHA-512:	C91296EF7400A0B7597B11B1871672D3930E01B015C82E463EE47482D24D0B77272058FFA2B2ED252FAD13B087F4BC080630D8FA61628AE4E1FFBA74A73B35A7
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>.. <StartWhenAvailable>t

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\Doc.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:JIDt:Gx
MD5:	0F537B5F4F20482B8B769AE429A9ACAE
SHA1:	1BD898059B9938529CFF3208C1FE31F641C84C2C
SHA-256:	CCFF37E420E56A6BB38FE3FFCE46C9CCA7C4FA64A4FA49F65925911D0680B693
SHA-512:	EDD9C694501661CB79C177E3D5059B46465287282B1125C2F55956748F68ECEB0F047A858BC7DF2EBA6DDC95B1E9E368C9E68AF9ACEE2FCF2ABE92CAE810BE2B
Malicious:	**true**
Preview:	Z..P...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\Doc.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	31
Entropy (8bit):	3.962103165155795
Encrypted:	false
SSDEEP:	3:oNUWJRWhKk:oNNJAck
MD5:	6DDAF09443278775838A4E5FC0A80DF6
SHA1:	9CD9265F32A1D9636E886A0D8D178C79F7D28026
SHA-256:	550B94662EDD56B552AE175CD834E72FDCB11F2F01EC1680797E251857F679E8
SHA-512:	27E6F50EABC36090A45B9438780CF407D8F8E8B5E6F1351118220CD732C18526CC72D46720D13FCF21C4A6E014BFAEE2A81CA8DD20585EB336B0026027FA03E
Malicious:	false
Preview:	C:\Users\user\Desktop\Doc.exe

C:\Users\user\AppData\Roaming\dEkaSoUjP.exe	
Process:	C:\Users\user\Desktop\Doc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1530880
Entropy (8bit):	7.361237861080968
Encrypted:	false
SSDEEP:	24576:uPoF365K8SDEXOkK3xtBi2H+N/ntbYZ0PNK1XtCIix:uAF3UK8UEekcxi24lDlK5g
MD5:	C853495818DB3FDDF333CE3EAF5E6CC3
SHA1:	51DFA28D2BF0AF44DE903FA80E4458110155F34B
SHA-256:	799087F4F62932DBE6405946E5FC9215C9DF899909C15F0C1D876EC28E9436B0
SHA-512:	1015EF73002C3221F8386F6E39CA2806F1662650001BE1DD8ACDAC02652D876AB2DA55E07ECF9612F6FDD39F8962A38EB07A034332A13BD39882BA71A9CC7B2
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 39%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...z.....0.....T..... ....@.. ....@..... ...K.....H.....2)-..Lp$(... .....@....text..... ..`.rsrc..... .....@..@.reloc.....X.....@..B.....Z..... ..`..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.361237861080968
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.96% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Doc.exe
File size:	1530880
MD5:	c853495818db3fddf333ce3eaf5e6cc3
SHA1:	51dfa28d2bf0af44de903fa80e4458110155f34b
SHA256:	799087f4f62932dbe6405946e5fc9215c9df899909c15f0c1d876ec28e9436b0
SHA512:	1015ef73002c3221f8386f6e39ca2806f1662650001be1dd8acdac02652d876ab2da55e07ecf9612f6fdd39f8962a38eb07a034332a13bd39882ba71a9cc7b2c
SSDEEP:	24576:uPoF365K8SDEXOkK3xtBi2H+N/ntbYZ0PNK1XtClix:uAF3UK8UEekcxi24lDlK5g
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...z.....0.....T..... ....@.. .....@.....

File Icon

Icon Hash:	8ae8ccccecece09a

Static PE Info

General

Entrypoint:	0x57c00a
Entrypoint Section:	
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:	0xC7A08D7A [Mon Feb 17 17:59:22 2076 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 [0057C000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xec920	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x15e000	0x1b0c8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x17a000	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	0x17c000	0x8	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0xec000	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
2)-Lp$	0x2000	0xe9e28	0xea000	False	1.00031404414	data	7.99982367826	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.text	0xec000	0x70018	0x70200	False	0.306355386009	data	4.75650322444	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x15e000	0x1b0c8	0x1b200	False	0.127538162442	data	3.74361062755	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x17a000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
	0x17c000	0x10	0x200	False	0.044921875	data	0.142635768149	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x15e220	0x1913	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x15fb34	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0x17035c	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_ICON	0x174584	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_ICON	0x176b2c	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_ICON	0x177bd4	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x17803c	0x5a	data		
RT_VERSION	0x178098	0x33a	data		
RT_MANIFEST	0x1783d4	0xcef	XML 1.0 document, UTF-8 Unicode (with BOM) text		

Imports

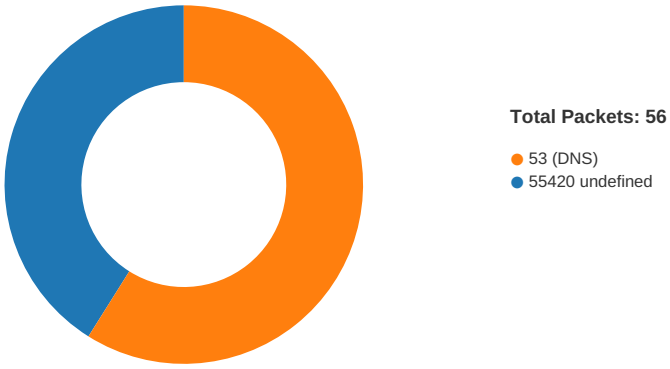
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2020 ITEL
Assembly Version	8.0.36.2
InternalName	.exe
FileVersion	8.0.37.2
CompanyName	ITEL Limited
LegalTrademarks	
Comments	
ProductName	CSM Project
ProductVersion	8.0.37.2
FileDescription	CSM Project
OriginalFilename	.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 10:23:30.951219082 CET	49714	55420	192.168.2.5	154.120.95.234

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 10:23:34.106537104 CET	49714	55420	192.168.2.5	154.120.95.234
Jan 19, 2021 10:23:40.107089996 CET	49714	55420	192.168.2.5	154.120.95.234
Jan 19, 2021 10:23:56.398092031 CET	49722	55420	192.168.2.5	154.120.95.234
Jan 19, 2021 10:23:59.406162024 CET	49722	55420	192.168.2.5	154.120.95.234
Jan 19, 2021 10:24:05.406017065 CET	49722	55420	192.168.2.5	154.120.95.234
Jan 19, 2021 10:24:17.939691067 CET	49730	55420	192.168.2.5	154.120.95.234
Jan 19, 2021 10:24:21.032339096 CET	49730	55420	192.168.2.5	154.120.95.234
Jan 19, 2021 10:24:27.032870054 CET	49730	55420	192.168.2.5	154.120.95.234
Jan 19, 2021 10:24:37.293370008 CET	49735	55420	192.168.2.5	172.111.249.15
Jan 19, 2021 10:24:40.299601078 CET	49735	55420	192.168.2.5	172.111.249.15
Jan 19, 2021 10:24:46.300118923 CET	49735	55420	192.168.2.5	172.111.249.15
Jan 19, 2021 10:24:55.309611082 CET	49738	55420	192.168.2.5	172.111.249.15
Jan 19, 2021 10:24:58.316715956 CET	49738	55420	192.168.2.5	172.111.249.15
Jan 19, 2021 10:25:04.317243099 CET	49738	55420	192.168.2.5	172.111.249.15
Jan 19, 2021 10:25:13.085031986 CET	49739	55420	192.168.2.5	172.111.249.15
Jan 19, 2021 10:25:16.099419117 CET	49739	55420	192.168.2.5	172.111.249.15
Jan 19, 2021 10:25:22.115677118 CET	49739	55420	192.168.2.5	172.111.249.15
Jan 19, 2021 10:25:31.900134087 CET	49740	55420	192.168.2.5	154.120.95.234
Jan 19, 2021 10:25:34.897878885 CET	49740	55420	192.168.2.5	154.120.95.234
Jan 19, 2021 10:25:40.898380041 CET	49740	55420	192.168.2.5	154.120.95.234
Jan 19, 2021 10:25:56.120098114 CET	49751	55420	192.168.2.5	154.120.95.234
Jan 19, 2021 10:25:59.122292042 CET	49751	55420	192.168.2.5	154.120.95.234

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 10:22:59.676734924 CET	49557	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:22:59.724585056 CET	53	49557	8.8.8.8	192.168.2.5
Jan 19, 2021 10:23:03.011400938 CET	61733	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:23:03.062161922 CET	53	61733	8.8.8.8	192.168.2.5
Jan 19, 2021 10:23:13.308800936 CET	65447	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:23:13.366452932 CET	53	65447	8.8.8.8	192.168.2.5
Jan 19, 2021 10:23:21.428308964 CET	52441	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:23:21.479062080 CET	53	52441	8.8.8.8	192.168.2.5
Jan 19, 2021 10:23:22.557158947 CET	62176	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:23:22.615228891 CET	53	62176	8.8.8.8	192.168.2.5
Jan 19, 2021 10:23:30.818375111 CET	59596	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:23:30.878221989 CET	53	59596	8.8.8.8	192.168.2.5
Jan 19, 2021 10:23:44.950850010 CET	65296	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:23:45.002350092 CET	53	65296	8.8.8.8	192.168.2.5
Jan 19, 2021 10:23:48.195247889 CET	63183	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:23:48.243144035 CET	53	63183	8.8.8.8	192.168.2.5
Jan 19, 2021 10:23:48.297032118 CET	60151	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:23:48.344970942 CET	53	60151	8.8.8.8	192.168.2.5
Jan 19, 2021 10:23:50.084479094 CET	56969	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:23:50.132464886 CET	53	56969	8.8.8.8	192.168.2.5
Jan 19, 2021 10:23:56.321463108 CET	55161	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:23:56.384004116 CET	53	55161	8.8.8.8	192.168.2.5
Jan 19, 2021 10:24:02.716928005 CET	54757	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:24:02.764775038 CET	53	54757	8.8.8.8	192.168.2.5
Jan 19, 2021 10:24:05.069717884 CET	49992	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:24:05.120398045 CET	53	49992	8.8.8.8	192.168.2.5
Jan 19, 2021 10:24:10.203083038 CET	60075	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:24:10.263900995 CET	53	60075	8.8.8.8	192.168.2.5
Jan 19, 2021 10:24:17.880350113 CET	55016	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:24:17.938066959 CET	53	55016	8.8.8.8	192.168.2.5
Jan 19, 2021 10:24:23.151571035 CET	64345	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:24:23.199763060 CET	53	64345	8.8.8.8	192.168.2.5
Jan 19, 2021 10:24:24.049966097 CET	57128	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:24:24.097898006 CET	53	57128	8.8.8.8	192.168.2.5
Jan 19, 2021 10:24:24.902646065 CET	54791	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:24:24.950527906 CET	53	54791	8.8.8.8	192.168.2.5
Jan 19, 2021 10:24:28.905478954 CET	50463	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:24:28.981370926 CET	53	50463	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 10:24:38.677479029 CET	50394	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:24:38.726584911 CET	53	50394	8.8.8.8	192.168.2.5
Jan 19, 2021 10:24:42.713869095 CET	58530	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:24:42.788130999 CET	53	58530	8.8.8.8	192.168.2.5
Jan 19, 2021 10:25:31.837795019 CET	53813	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:25:31.898233891 CET	53	53813	8.8.8.8	192.168.2.5
Jan 19, 2021 10:25:43.870352983 CET	63732	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:25:43.918276072 CET	53	63732	8.8.8.8	192.168.2.5
Jan 19, 2021 10:25:44.765908957 CET	57344	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:25:44.825380087 CET	53	57344	8.8.8.8	192.168.2.5
Jan 19, 2021 10:25:45.759581089 CET	54450	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:25:45.807430029 CET	53	54450	8.8.8.8	192.168.2.5
Jan 19, 2021 10:25:46.522767067 CET	59261	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:25:46.573513031 CET	53	59261	8.8.8.8	192.168.2.5
Jan 19, 2021 10:25:47.303802013 CET	57151	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:25:47.362200022 CET	53	57151	8.8.8.8	192.168.2.5
Jan 19, 2021 10:25:48.205671072 CET	59413	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:25:48.262279034 CET	53	59413	8.8.8.8	192.168.2.5
Jan 19, 2021 10:25:49.114852905 CET	60516	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:25:49.171040058 CET	53	60516	8.8.8.8	192.168.2.5
Jan 19, 2021 10:25:50.212817907 CET	51649	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:25:50.269519091 CET	53	51649	8.8.8.8	192.168.2.5
Jan 19, 2021 10:25:51.512135029 CET	65086	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:25:51.568703890 CET	53	65086	8.8.8.8	192.168.2.5
Jan 19, 2021 10:25:52.286628962 CET	56432	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:25:52.342928886 CET	53	56432	8.8.8.8	192.168.2.5
Jan 19, 2021 10:25:56.058824062 CET	52929	53	192.168.2.5	8.8.8.8
Jan 19, 2021 10:25:56.118586063 CET	53	52929	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 19, 2021 10:23:30.818375111 CET	192.168.2.5	8.8.8.8	0x7fa6	Standard query (0)	innocentbo oii.hopto.org	A (IP address)	IN (0x0001)
Jan 19, 2021 10:23:56.321463108 CET	192.168.2.5	8.8.8.8	0xc577	Standard query (0)	innocentbo oii.hopto.org	A (IP address)	IN (0x0001)
Jan 19, 2021 10:24:17.880350113 CET	192.168.2.5	8.8.8.8	0x5c38	Standard query (0)	innocentbo oii.hopto.org	A (IP address)	IN (0x0001)
Jan 19, 2021 10:25:31.837795019 CET	192.168.2.5	8.8.8.8	0x1870	Standard query (0)	innocentbo oii.hopto.org	A (IP address)	IN (0x0001)
Jan 19, 2021 10:25:56.058824062 CET	192.168.2.5	8.8.8.8	0x7845	Standard query (0)	innocentbo oii.hopto.org	A (IP address)	IN (0x0001)

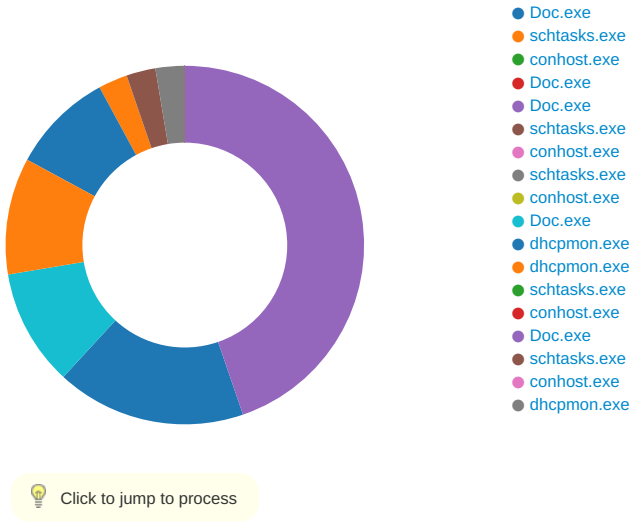
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 19, 2021 10:23:30.878221989 CET	8.8.8.8	192.168.2.5	0x7fa6	No error (0)	innocentbo oii.hopto.org		154.120.95.234	A (IP address)	IN (0x0001)
Jan 19, 2021 10:23:56.384004116 CET	8.8.8.8	192.168.2.5	0xc577	No error (0)	innocentbo oii.hopto.org		154.120.95.234	A (IP address)	IN (0x0001)
Jan 19, 2021 10:24:17.938066959 CET	8.8.8.8	192.168.2.5	0x5c38	No error (0)	innocentbo oii.hopto.org		154.120.95.234	A (IP address)	IN (0x0001)
Jan 19, 2021 10:25:31.898233891 CET	8.8.8.8	192.168.2.5	0x1870	No error (0)	innocentbo oii.hopto.org		154.120.95.234	A (IP address)	IN (0x0001)
Jan 19, 2021 10:25:56.118586063 CET	8.8.8.8	192.168.2.5	0x7845	No error (0)	innocentbo oii.hopto.org		154.120.95.234	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Doc.exe PID: 1460 Parent PID: 5608

General

Start time:	10:23:04
Start date:	19/01/2021
Path:	C:\Users\user\Desktop\Doc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Doc.exe'
Imagebase:	0xe70000
File size:	1530880 bytes
MD5 hash:	C853495818DB3FDDF333CE3EAF5E6CC3
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: 00000000.00000002.278969734.00000000073FA000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.278969734.00000000073FA000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.278969734.00000000073FA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72B860AC	unknown
C:\Users\user\AppData\Roaming\dEkaSoUjP.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	69C0B4F	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp58A2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	16CBC88	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Doc.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72B734A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp58A2.tmp	success or wait	1	69C17C6	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\dEkaSoUjP.exe	unknown	1530880	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 7a 8d a0 c7 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 04 07 00 00 54 10 00 00 00 00 00 0a c0 17 00 00 c0 0e 00 00 20 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 e0 17 00 00 04 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...z............ ....0......T............... ....@.. ....@................	success or wait	1	69C0DD7	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp58A2.tmp	unknown	1646	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationI	success or wait	1	69C0DD7	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Doc.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	72E5A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Users\user\Desktop\Doc.exe	unknown	1530880	success or wait	1	69C0DD7	ReadFile

Analysis Process: schtasks.exe PID: 5744 Parent PID: 1460

General

Start time:	10:23:20
Start date:	19/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\dEkaSoUjP' /XML 'C:\Users\user\AppData\Local\Temp\tmp58A2.tmp'
Imagebase:	0xbf0000
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\tmp58A2.tmp	unknown	2	success or wait	1	BFAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp58A2.tmp	unknown	1647	success or wait	1	BFABD9	ReadFile

Analysis Process: conhost.exe PID: 6112 Parent PID: 5744

General

Start time:	10:23:21
Start date:	19/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Doc.exe PID: 5784 Parent PID: 1460

General

Start time:	10:23:23
Start date:	19/01/2021
Path:	C:\Users\user\Desktop\Doc.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x3b0000
File size:	1530880 bytes
MD5 hash:	C853495818DB3FDDF333CE3EAF5E6CC3

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Doc.exe PID: 3848 Parent PID: 1460

General

Start time:	10:23:24
Start date:	19/01/2021
Path:	C:\Users\user\Desktop\Doc.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xcf0000
File size:	1530880 bytes
MD5 hash:	C853495818DB3FDDF333CE3EAF5E6CC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.595250143.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.595250143.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.595250143.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72B860AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72B860AC	unknown
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	31107A1	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	311089B	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	31107A1	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	3110B20	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	3110B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpD558.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	3110D1C	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	311089B	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpD876.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	3110D1C	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	31107A1	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	31107A1	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72B860AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72B860AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpD558.tmp	success or wait	1	152BF0E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpD876.tmp	success or wait	1	152BF0E	DeleteFileW
C:\Users\user\Desktop\Doc.exe:Zone.Identifier	success or wait	1	311114D	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	5a de 00 50 a7 bc d8 48	Z..P...H	success or wait	1	3110A53	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 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 05 00 7a 8d a0 c7 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 04 07 00 00 54 10 00 00 00 00 00 0a c0 17 00 00 c0 0e 00 00 20 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 00 e0 17 00 00 04 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...z..... ....0.....T..... ....@.. ....@.....	success or wait	6	3110B20	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	3110B20	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpD558.tmp	unknown	1294	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	3110A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	31	43 3a 5c 55 73 65 72 73 5c 61 6c 66 6f 6e 73 5c 44 65 73 6b 74 6f 70 5c 44 6f 63 2e 65 78 65	C:\Users\user\Desktop\Doc.exe	success or wait	1	3110A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpD876.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	3110A53	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	72C5BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	72C5BF06	unknown
C:\Users\user\Desktop\Doc.exe	unknown	4096	success or wait	1	72C5BF06	unknown
C:\Users\user\Desktop\Doc.exe	unknown	512	success or wait	1	72C5BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	3110A53	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	3110C12	RegSetValueExW

Analysis Process: schtasks.exe PID: 5536 Parent PID: 3848

General

Start time:	10:23:26
Start date:	19/01/2021
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\tmpD558.tmp'

Imagebase:	0x7ff797770000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpD558.tmp	unknown	2	success or wait	1	BFAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpD558.tmp	unknown	1295	success or wait	1	BFABD9	ReadFile

Analysis Process: conhost.exe PID: 5336 Parent PID: 5536

General

Start time:	10:23:26
Start date:	19/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 5316 Parent PID: 3848

General

Start time:	10:23:27
Start date:	19/01/2021
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\tmpD876.tmp'
Imagebase:	0xbf0000
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\tmpD876.tmp	unknown	2	success or wait	1	BFAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpD876.tmp	unknown	1311	success or wait	1	BFABD9	ReadFile

Analysis Process: conhost.exe PID: 5328 Parent PID: 5316

General

Start time:	10:23:27
Start date:	19/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Doc.exe PID: 1112 Parent PID: 904

General

Start time:	10:23:29
Start date:	19/01/2021
Path:	C:\Users\user\Desktop\Doc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Doc.exe 0
Imagebase:	0xdd0000
File size:	1530880 bytes
MD5 hash:	C853495818DB3FDDF333CE3EAF5E6CC3
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.00000002.330365901.00000000047AD000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.330365901.00000000047AD000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.330365901.00000000047AD000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000D.00000002.326488687.0000000003667000.00000004.00000001.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	72B860AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72B860AC	unknown
C:\Users\user\AppData\Local\Temp\tmpB420.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	170BC88	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpB420.tmp	success or wait	1	5AF16F6	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpB420.tmp	unknown	1646	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationI	success or wait	1	5AF13B3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile

Analysis Process: dhcpmon.exe PID: 3720 Parent PID: 904

General

Start time:	10:23:30
Start date:	19/01/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0

Imagebase:	0x4a0000
File size:	1530880 bytes
MD5 hash:	C853495818DB3FDDF333CE3EAF5E6CC3
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.00000002.328137753.0000000003EDD000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.328137753.0000000003EDD000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.328137753.0000000003EDD000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 39%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72B860AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72B860AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72B734A7	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

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	72E5A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile

Analysis Process: dhcpmon.exe PID: 6328 Parent PID: 3472

General

Start time:	10:23:38
Start date:	19/01/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x680000
File size:	1530880 bytes
MD5 hash:	C853495818DB3FDDF333CE3EAF5E6CC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000013.00000002.350701608.00000000030AC000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.355278131.0000000006CBA000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.355278131.0000000006CBA000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.355278131.0000000006CBA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72B860AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72B860AC	unknown
C:\Users\user\AppData\Local\Temp\tmpDD04.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	DBBC88	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpDD04.tmp	success or wait	1	52816F6	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpDD04.tmp	unknown	1646	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationI	success or wait	1	52813B3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile

Analysis Process: schtasks.exe PID: 6476 Parent PID: 1112

General

Start time:	10:23:44
Start date:	19/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\dEkaSoUjP' /XML 'C:\Users\user\AppData\Local\Temp\tmpB420.tmp'
Imagebase:	0xbf0000
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: 6484 Parent PID: 6476

General

Start time:	10:23:44
Start date:	19/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Doc.exe PID: 6524 Parent PID: 1112

General

Start time:	10:23:46
Start date:	19/01/2021
Path:	C:\Users\user\Desktop\Doc.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x5d0000
File size:	1530880 bytes
MD5 hash:	C853495818DB3FDDF333CE3EAF5E6CC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.339391381.0000000003D21000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.339391381.0000000003D21000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000002.335391118.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.335391118.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.335391118.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.339287751.0000000002D21000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.339287751.0000000002D21000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: schtasks.exe PID: 6848 Parent PID: 6328

General

Start time:	10:23:54
Start date:	19/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\dEkaSoUjP' /XML 'C:\Users\user\AppData\Local\Temp\tmpDD04.tmp'
Imagebase:	0xbf0000
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: 6860 Parent PID: 6848

General

Start time:	10:23:54
Start date:	19/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 6928 Parent PID: 6328

General

Start time:	10:23:55
Start date:	19/01/2021

Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xd00000
File size:	1530880 bytes
MD5 hash:	C853495818DB3FDDF333CE3EAF5E6CC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001C.00000002.364409050.0000000004561000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001C.00000002.364409050.0000000004561000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001C.00000002.361008474.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001C.00000002.361008474.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001C.00000002.361008474.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001C.00000002.364312350.0000000003561000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001C.00000002.364312350.0000000003561000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Disassembly

Code Analysis