ID: 342778
Sample Name: PROOF OF PAYMENT.exe
Cookbook: default.jbs
Time: 18:19:11
Date: 21/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

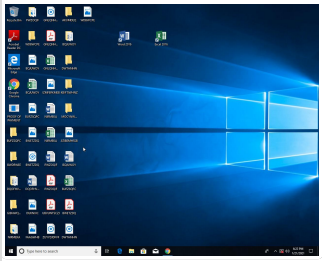
Analysis Report PROOF OF PAYMENT.exe

Overview

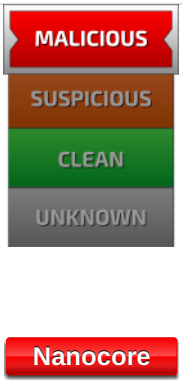
General Information

Sample Name:	PROOF OF PAYMENT.exe
Analysis ID:	342778
MD5:	dcf168394ef0a6d..
SHA1:	565c77fa9f7f222…
SHA256:	373e294fccf1cbc…
Tags:	exe NanoCore RAT

Most interesting Screenshot:



Detection



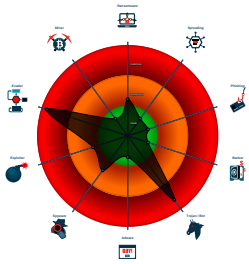
Nanocore

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 …
- 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…
- C2 URLs / IPs found in malware con…
- Contains functionality to check if a d…
- Hides that the sample has been dow…

Classification



Startup

- **System is w10x64**
- PROOF OF PAYMENT.exe (PID: 7064 cmdline: 'C:\Users\user\Desktop\PROOF OF PAYMENT.exe' MD5: DCF168394EF0A6D6774B099DD8493B75)
  - schtasks.exe (PID: 6012 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\pJrVfPlhXgkUp' /XML 'C:\Users\user\AppData\Local\Temp\tmpE52C.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5700 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - PROOF OF PAYMENT.exe (PID: 6816 cmdline: {path} MD5: DCF168394EF0A6D6774B099DD8493B75)
- dhcpmon.exe (PID: 5820 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: DCF168394EF0A6D6774B099DD8493B75)
  - schtasks.exe (PID: 2208 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\pJrVfPlhXgkUp' /XML 'C:\Users\user\AppData\Local\Temp\tmp5106.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 2044 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 6780 cmdline: {path} MD5: DCF168394EF0A6D6774B099DD8493B75)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "C2: ": [
    "185.140.53.131"
  ],
  "Version: ": "NanoCore Client, Version=1.2.2.0"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000011.00000002.770483355.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Source	Rule	Description	Author	Strings
00000011.00000002.770483355.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000011.00000002.770483355.000000000040 2000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000007.00000002.1026361866.00000000004 02000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000007.00000002.1026361866.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 34 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.PROOF OF PAYMENT.exe.5f70000.5.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
7.2.PROOF OF PAYMENT.exe.5f70000.5.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
7.2.PROOF OF PAYMENT.exe.5f70000.5.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
7.2.PROOF OF PAYMENT.exe.5ee0000.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
7.2.PROOF OF PAYMENT.exe.5ee0000.4.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
Click to see the 11 entries				

Sigma Overview

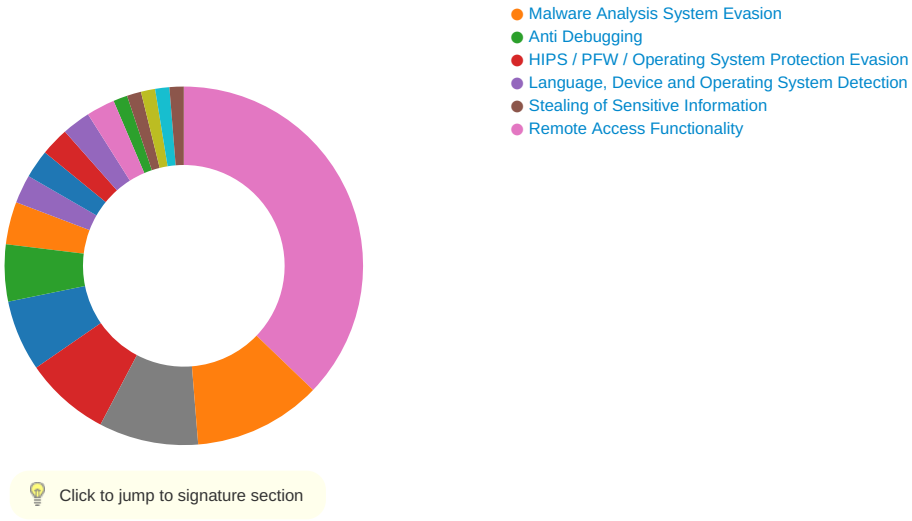
System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview

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



AV Detection:

- Found malware configuration
- Yara detected Nanocore RAT
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Compliance:

- Uses 32bit PE files
- 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
- Uses dynamic DNS services

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)
- Initial sample is a PE file and has a suspicious name
- 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)

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

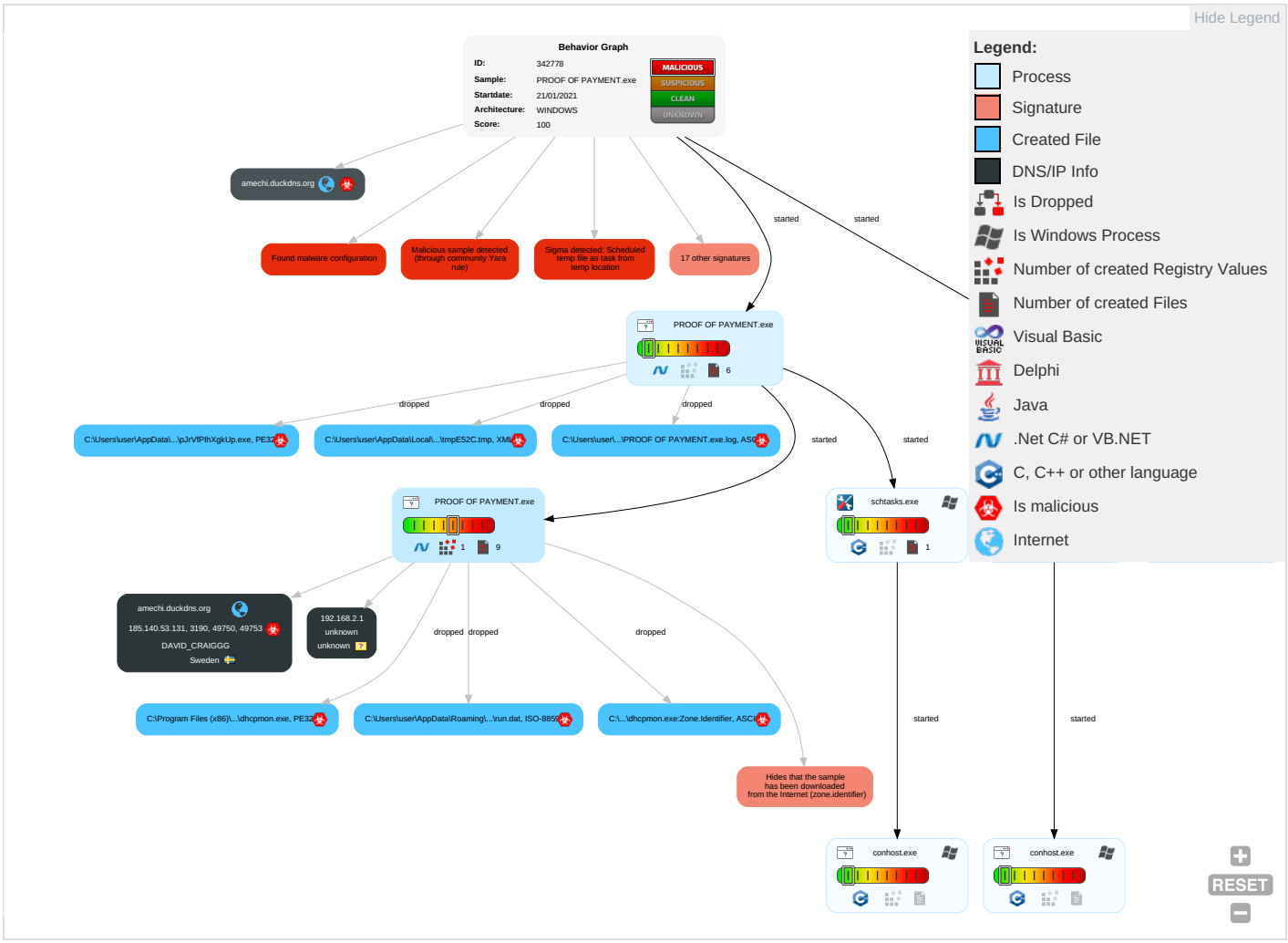
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 2	Masquerading 2	Input Capture 2 1	Security Software Discovery 2 2 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdro Insecure Network Commun
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 4	LSASS Memory	Virtualization/Sandbox Evasion 4	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Manipula Device Commun
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Timestomp 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue C Base Sta

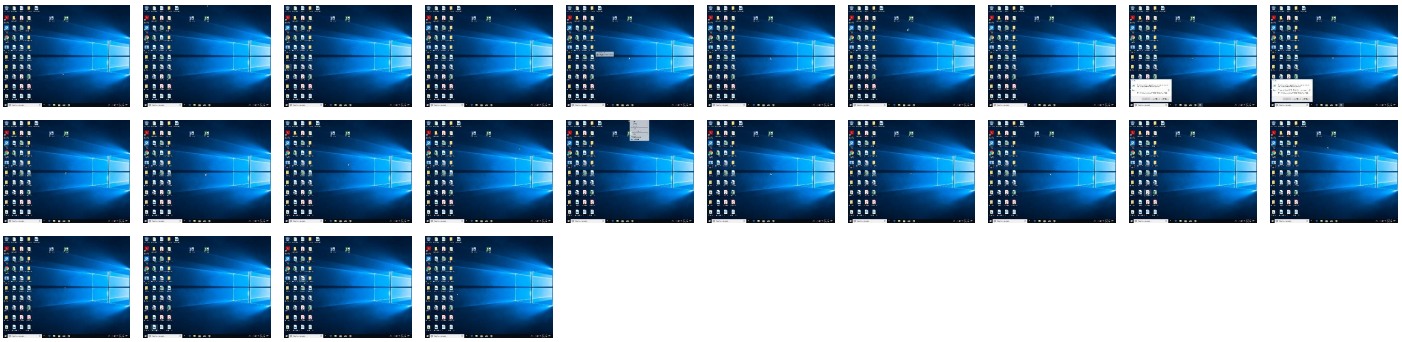
Behavior Graph



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
PROOF OF PAYMENT.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\pJrVfPIhXgkUp.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.2.dhcpmon.exe.e60000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.PROOF OF PAYMENT.exe.5f70000.5.unpack	100%	Avira	TR/NanoCore.fadte		Download File
1.2.PROOF OF PAYMENT.exe.640000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
7.2.PROOF OF PAYMENT.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
amechi.duckdns.org	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comionF	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.carterandcone.comueX	0%	Avira URL Cloud	safe	
http://www.carterandcone.comva	0%	Avira URL Cloud	safe	
http://www.fontbureau.comdiaF	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.fontbureau.comtuedm	0%	Avira URL Cloud	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.fontbureau.comued	0%	Avira URL Cloud	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%	Avira URL Cloud	safe	
http://www.fontbureau.comcomd_	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.jiyu-kobo.co.jp/roso	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htmY	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/5	0%	Avira URL Cloud	safe	
http://www.carterandcone.comD	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/typedesigners.html:	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnl	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.carterandcone.comR	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.como.	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.fontbureau.commm	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cnf	0%	Avira URL Cloud	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.como5	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.fontbureau.comnc.	0%	Avira URL Cloud	safe	
http://www.carterandcone.comf	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.fontbureau.comcomd	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/P	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/P	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/P	0%	URL Reputation	safe	
http://www.founder.com.cn/cnz	0%	Avira URL Cloud	safe	
http://www.carterandcone.comt	0%	URL Reputation	safe	
http://www.carterandcone.comt	0%	URL Reputation	safe	
http://www.carterandcone.comt	0%	URL Reputation	safe	
http://www.fontbureau.comd_	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.jiyu-kobo.co.jp/on	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://www.jiyu-kobo.co.jp//Mo_	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Sue	0%	Avira URL Cloud	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
amechi.duckdns.org	185.140.53.131	true	true	• 4%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comionF	PROOF OF PAYMENT.exe, 00000001.00000003.675123633.000000000B39D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	PROOF OF PAYMENT.exe, 00000001.00000002.707113887.000000000B480000.00000002.00000001.sdmp, dhcpmon.exe, 0000000C.00000002.767911748.000000000BD80000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	PROOF OF PAYMENT.exe, 00000001.00000002.707113887.000000000B480000.00000002.00000001.sdmp, dhcpmon.exe, 0000000C.00000002.767911748.000000000BD80000.00000002.00000001.sdmp	false		high

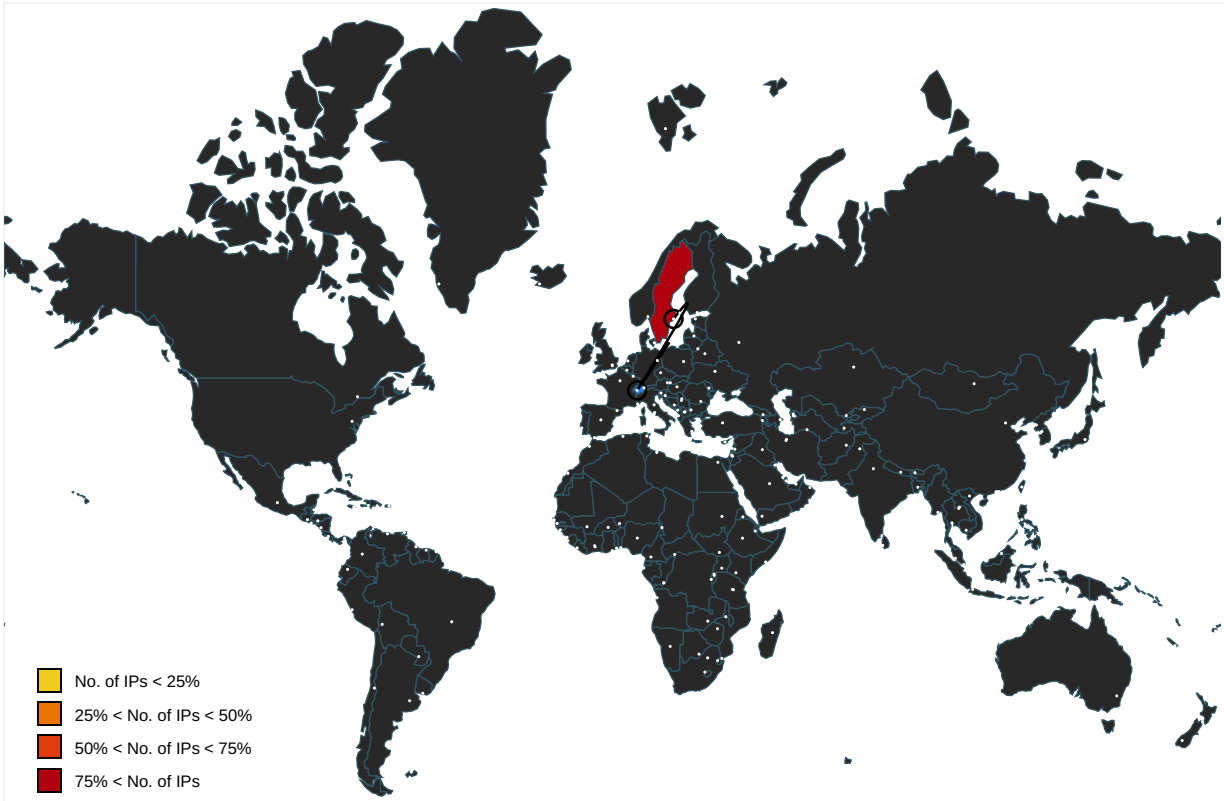
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	PROOF OF PAYMENT.exe, 00000001.00000002.707113887.000000000B480000.00000002.00000001.sdmp, dhcpmon.exe, 0000000C.00000002.767911748.000000000BD80000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comueX	PROOF OF PAYMENT.exe, 00000001.00000003.666802005.000000000B3A4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	PROOF OF PAYMENT.exe, 00000001.00000002.707113887.000000000B480000.00000002.00000001.sdmp, dhcpmon.exe, 0000000C.00000002.767911748.000000000BD80000.00000002.00000001.sdmp	false		high
http://www.carterandcone.comva	PROOF OF PAYMENT.exe, 00000001.00000003.666802005.000000000B3A4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-user.html.	PROOF OF PAYMENT.exe, 00000001.00000003.670107984.000000000B39D000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comdiaF	PROOF OF PAYMENT.exe, 00000001.00000003.669540752.000000000B39D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	dhcpmon.exe, 0000000C.00000002.767911748.000000000BD80000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	dhcpmon.exe, 0000000C.00000002.767911748.000000000BD80000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comtuedm	PROOF OF PAYMENT.exe, 00000001.00000003.671353872.000000000B39D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comessed	PROOF OF PAYMENT.exe, 00000001.00000003.669540752.000000000B39D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersZ	PROOF OF PAYMENT.exe, 00000001.00000003.668897969.000000000B3A5000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comued	PROOF OF PAYMENT.exe, 00000001.00000003.671353872.000000000B39D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	PROOF OF PAYMENT.exe, 00000001.00000002.707113887.000000000B480000.00000002.00000001.sdmp, dhcpmon.exe, 0000000C.00000002.767911748.000000000BD80000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	PROOF OF PAYMENT.exe, 00000001.00000003.666802005.000000000B3A4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com(	PROOF OF PAYMENT.exe, 00000001.00000003.667062493.000000000B3A5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.comcomd_	PROOF OF PAYMENT.exe, 00000001.00000003.670107984.000000000B39D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.sajatypeworks.com	PROOF OF PAYMENT.exe, 00000001.00000003.665018666.0000000010DC000.00000004.00000001.sdmp, dhcpmon.exe, 0000000C.00000002.767911748.000000000BD80000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/roso	PROOF OF PAYMENT.exe, 00000001.00000003.667077696.000000000B399000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.typography.netD	PROOF OF PAYMENT.exe, 00000001.00000002.707113887.000000000B480000.00000002.00000001.sdmp, dhcpmon.exe, 0000000C.00000002.767911748.000000000BD80000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	PROOF OF PAYMENT.exe, 00000001.00000002.707113887.000000000B480000.00000002.00000001.sdmp, dhcpmon.exe, 0000000C.00000002.767911748.000000000BD80000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htmY	PROOF OF PAYMENT.exe, 00000001.00000003.674156675.000000000B3C3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm	PROOF OF PAYMENT.exe, 00000001.00000002.707113887.000000000B480000.00000002.00000001.sdmp, dhcpmon.exe, 0000000C.00000002.767911748.000000000BD80000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	PROOF OF PAYMENT.exe, 00000001.00000002.707113887.000000000B480000.00000002.00000001.sdmp, dhcpmon.exe, 0000000C.00000002.767911748.000000000BD80000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/5	PROOF OF PAYMENT.exe, 00000001.00000003.667540587.000000000B39D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comD	PROOF OF PAYMENT.exe, 00000001.00000003.666742269.000000000B3A6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ascendercorp.com/typedesigners.html:	PROOF OF PAYMENT.exe, 00000001.00000003.667540587.000000000B39D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersj	PROOF OF PAYMENT.exe, 00000001.00000003.668897969.000000000B3A5000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnl	PROOF OF PAYMENT.exe, 00000001.00000003.666474096.000000000B3A5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/0	PROOF OF PAYMENT.exe, 00000001.00000003.667540587.000000000B39D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlormal	PROOF OF PAYMENT.exe, 00000001.00000003.670715362.000000000B3C3000.00000004.00000001.sdmp	false		high
http://www.carterandcone.comR	PROOF OF PAYMENT.exe, 00000001.00000003.666742269.000000000B3A6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	PROOF OF PAYMENT.exe, 00000001.00000002.707113887.000000000B480000.00000002.00000001.sdmp, dhcpmon.exe, 0000000C.00000002.767911748.000000000BD80000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.como.	PROOF OF PAYMENT.exe, 00000001.00000003.671106569.000000000B39D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.ascendercorp.com/typedesigners.html	PROOF OF PAYMENT.exe, 00000001.00000003.667540587.000000000B39D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.commm	PROOF OF PAYMENT.exe, 00000001.00000003.675123633.000000000B39D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	PROOF OF PAYMENT.exe, 00000001.00000002.707113887.000000000B480000.00000002.00000001.sdmp, dhcpmon.exe, 0000000C.00000002.767911748.000000000BD80000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	PROOF OF PAYMENT.exe, 00000001.00000002.707113887.000000000B480000.00000002.00000001.sdmp, dhcpmon.exe, 0000000C.00000002.767911748.000000000BD80000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	PROOF OF PAYMENT.exe, 00000001.00000002.707113887.000000000B480000.00000002.00000001.sdmp, dhcpmon.exe, 0000000C.00000002.767911748.000000000BD80000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	PROOF OF PAYMENT.exe, 00000001.00000003.666742269.000000000B3A6000.00000004.00000001.sdmp, dhcpmon.exe, 0000000C.00000002.767911748.000000000BD80000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	PROOF OF PAYMENT.exe, 00000001.00000002.698087475.0000000002BA6000.00000004.00000001.sdmp, dhcpmon.exe, 0000000C.00000002.755447551.0000000003486000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cnf	PROOF OF PAYMENT.exe, 00000001.00000003.666474096.000000000B3A5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	PROOF OF PAYMENT.exe, 00000001.00000002.707113887.000000000B480000.00000002.00000001.sdmp, dhcpmon.exe, 0000000C.00000002.767911748.000000000BD80000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.como5	PROOF OF PAYMENT.exe, 00000001.00000003.696672589.000000000B390000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	PROOF OF PAYMENT.exe, 00000001.00000002.707113887.000000000B480000.00000002.00000001.sdmp, dhcpmon.exe, 0000000C.00000002.767911748.000000000BD80000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	PROOF OF PAYMENT.exe, 00000001.00000003.671353872.000000000B39D000.00000004.00000001.sdmp, dhcpmon.exe, 0000000C.00000002.767911748.000000000BD80000.00000002.00000001.sdmp	false		high
http://www.galapagosdesign.com/	PROOF OF PAYMENT.exe, 00000001.00000003.672895387.000000000B39D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comnc.	PROOF OF PAYMENT.exe, 00000001.00000003.668748768.000000000B39D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comf	PROOF OF PAYMENT.exe, 00000001.00000003.666802005.000000000B3A4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.come	PROOF OF PAYMENT.exe, 00000001.00000003.666802005.000000000B3A4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comcomd	PROOF OF PAYMENT.exe, 00000001.00000003.671353872.000000000B39D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/P	PROOF OF PAYMENT.exe, 00000001.00000003.667540587.000000000B39D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnz	PROOF OF PAYMENT.exe, 00000001.00000003.666474096.000000000B3A5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comt	PROOF OF PAYMENT.exe, 00000001.00000003.667062493.000000000B3A5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comd_	PROOF OF PAYMENT.exe, 00000001.00000003.669540752.000000000B39D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/jp/	PROOF OF PAYMENT.exe, 00000001.00000003.667540587.000000000B39D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/on	PROOF OF PAYMENT.exe, 00000001.00000003.667077696.000000000B399000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comd	PROOF OF PAYMENT.exe, 00000001.00000003.669540752.000000000B39D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp//Mo_	PROOF OF PAYMENT.exe, 00000001.00000003.667263984.000000000B39C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Sue	PROOF OF PAYMENT.exe, 00000001.00000003.666912527.000000000B395000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	PROOF OF PAYMENT.exe, 00000001.00000002.707113887.000000000B480000.00000002.00000001.sdmp, dhcpmon.exe, 0000000C.00000002.767911748.000000000BD80000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	PROOF OF PAYMENT.exe, 00000001.00000003.666474096.000000000B3A5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers(	PROOF OF PAYMENT.exe, 00000001.00000003.675123633.000000000B39D000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.htmlN	PROOF OF PAYMENT.exe, 00000001.00000002.707113887.000000000B480000.00000002.00000001.sdmp, dhcpmon.exe, 0000000C.00000002.767911748.000000000BD80000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	PROOF OF PAYMENT.exe, 00000001.00000003.666742269.000000000B3A6000.00000004.00000001.sdmp, PROOF OF PAYMENT.exe, 00000001.00000003.666474096.000000000B3A5000.00000004.00000001.sdmp, dhcpmon.exe, 0000000C.00000002.767911748.000000000BD80000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/.	PROOF OF PAYMENT.exe, 00000001.00000003.672733617.000000000B39D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	PROOF OF PAYMENT.exe, 00000001.00000003.669981678.000000000B39D000.00000004.00000001.sdmp, PROOF OF PAYMENT.exe, 00000001.00000002.707113887.000000000B480000.00000002.00000001.sdmp, dhcpmon.exe, 0000000C.00000002.767911748.000000000BD80000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/t	PROOF OF PAYMENT.exe, 00000001.00000003.667540587.000000000B39D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comz	PROOF OF PAYMENT.exe, 00000001.00000003.666802005.000000000B3A4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	PROOF OF PAYMENT.exe, 00000001.00000003.670641038.000000000B3C3000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/anie	PROOF OF PAYMENT.exe, 00000001.00000003.667263984.000000000B39C000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	PROOF OF PAYMENT.exe, 00000001.00000003.667540587.000000000B39D000.00000004.00000001.sdmp, PROOF OF PAYMENT.exe, 00000001.00000003.667385656.000000000B39C000.00000004.00000001.sdmp, dhcpmon.exe, 0000000C.00000002.767911748.000000000BD80000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.como	PROOF OF PAYMENT.exe, 00000001.00000003.669066568.000000000B39D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cno.	PROOF OF PAYMENT.exe, 00000001.00000003.666742269.000000000B3A6000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	PROOF OF PAYMENT.exe, 00000001.00000002.707113887.000000000B480000.00000002.00000001.sdmp, dhcpmon.exe, 0000000C.00000002.767911748.000000000BD80000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comFf	PROOF OF PAYMENT.exe, 00000001.00000003.669540752.000000000B39D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comals	PROOF OF PAYMENT.exe, 00000001.00000003.671353872.000000000B39D000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/e	PROOF OF PAYMENT.exe, 00000001.00000003.666912527.000000000B395000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/f	PROOF OF PAYMENT.exe, 00000001.00000003.667540587.000000000B39D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comcommm	PROOF OF PAYMENT.exe, 00000001.00000003.696672589.000000000B390000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comalic_	PROOF OF PAYMENT.exe, 00000001.00000003.670674990.000000000B39D000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designers/	PROOF OF PAYMENT.exe, 00000001.00000003.668834638.000000000B3C9000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.131	unknown	Sweden		209623	DAVID_CRAIGGG	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	342778
Start date:	21.01.2021
Start time:	18:19:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PROOF OF PAYMENT.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:	26
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@12/8@27/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.9% (good quality ratio 0.7%) • Quality average: 22.7% • Quality standard deviation: 33.2%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 23.211.6.115, 40.88.32.150, 51.11.168.160, 92.122.213.247, 92.122.213.194, 2.20.142.209, 2.20.142.210, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:20:12	API Interceptor	1323x Sleep call for process: PROOF OF PAYMENT.exe modified
18:20:26	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
18:20:42	API Interceptor	1x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.140.53.131	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	
	Urgent order 1812021-672 Q30721,pdf.exe	Get hash	malicious	Browse	
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	
	R#U00d6SLER Puchase_tcs 10-28-2020,pdf.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
amechi.duckdns.org	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 185.140.53.131
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 185.140.53.131
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 79.134.225.82
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 79.134.225.69
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 79.134.225.69
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 79.134.225.69
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 79.134.225.69
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 79.134.225.69
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 79.134.225.71
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 79.134.225.71
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 79.134.225.71
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 79.134.225.71
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 79.134.225.71
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 79.134.225.71
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 79.134.225.71
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 79.134.225.73

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	SecuriteInfo.com.Artemis1A5E2411DEA6.exe	Get hash	malicious	Browse	• 91.193.75.204
	Payment Invoice PDF.exe	Get hash	malicious	Browse	• 185.244.30.18
	New Doc 20211401#_our new price.exe	Get hash	malicious	Browse	• 91.193.75.243
	company profile.exe	Get hash	malicious	Browse	• 185.140.53.227
	NEWORDERrefno0992883jpg.exe	Get hash	malicious	Browse	• 185.140.53.253
	richiealvin.exe	Get hash	malicious	Browse	• 91.193.75.185
	Quotation.exe	Get hash	malicious	Browse	• 185.140.53.154
	DHL Delivery Shipping Cargo. Pdf.exe	Get hash	malicious	Browse	• 185.244.30.18
	CompanyLicense.exe	Get hash	malicious	Browse	• 185.140.53.253
	Purchase Order 2094742424.exe	Get hash	malicious	Browse	• 185.244.30.132
	PURCHASE OREDER. PRINT. pdf.exe	Get hash	malicious	Browse	• 91.193.75.45
	PO.exe	Get hash	malicious	Browse	• 185.140.53.234
	SWIFT.exe	Get hash	malicious	Browse	• 185.140.53.154
	SecuriteInfo.com.BScope.Trojan-Dropper.Injector.exe	Get hash	malicious	Browse	• 185.140.53.234
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 185.140.53.131
	Orden n.#U00ba STL21119, pdf.exe	Get hash	malicious	Browse	• 185.140.53.129
	Proof of Payment.exe	Get hash	malicious	Browse	• 185.244.30.51
	DxCHoDnNLn.exe	Get hash	malicious	Browse	• 185.140.53.202
	T7gzTHDZ7g.rtf	Get hash	malicious	Browse	• 185.140.53.202
	PO - 2021-000511.exe	Get hash	malicious	Browse	• 185.244.30.69

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\PROOF OF PAYMENT.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1168384
Entropy (8bit):	7.897636731334413
Encrypted:	false
SSDEEP:	24576:E2cXDkZfhBL97dNqehj/5L3xqpljbfrRUoq7Ohn:E2MiBBRNb5LBepfrhqyN
MD5:	DCF168394EF0A6D6774B099DD8493B75
SHA1:	565C77FA9F7F22229FF5AABAD52F6F9E0C5FBCE0
SHA-256:	373E294FCCF1CBC447469AEB6FC86678EFBFD072B5035A295D1FC74CE6E9FD79
SHA-512:	6F19BD8C1CE255848FC9E60B92B758AC960C81E3CB4C3C7BC5E520DE5B03CFC0A2244891150B50ECC179FC35A9D7F9477E567BDD275B32B4873FE640DAFE7A C9
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0.....@..... ....@.. .....`..... @.....O..... .....@.....H.....\.D|.aH..... .....@....text..... ..`.rsrc..... .....@..@.reloc..... .....@..B.....@..... ..`..... ....

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\PROOF OF PAYMENT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
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
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PROOF OF PAYMENT.exe.log	
Process:	C:\Users\user\Desktop\PROOF OF PAYMENT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:ML9E4Ks29E4Kx1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MxHKX9HKx1qHiYHKhQnoPtHoxHhAHKzr
MD5:	B666A4404B132B2BF6C04FBF848EB948
SHA1:	D2EFB3D43F8B8806544D3A47F7DAEE8534981739
SHA-256:	7870616D981C8C0DE9A54E7383CD035470DB20CBF75ACDF729C32889D4B6ED96
SHA-512:	00E955EE9F14CEAE07E571A8EF2E103200CF421BAE83A66ED9F9E1AA6A9F449B653EDF1BFDB662A364D58ECF9B5FE4BB69D590DB2653F2F46A09F4D47719A862
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:ML9E4Ks29E4Kx1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MxHKX9HKx1qHiYHKhQnoPtHoxHhAHKzr
MD5:	B666A4404B132B2BF6C04FBF848EB948
SHA1:	D2EFB3D43F8B8806544D3A47F7DAEE8534981739
SHA-256:	7870616D981C8C0DE9A54E7383CD035470DB20CBF75ACDF729C32889D4B6ED96
SHA-512:	00E955EE9F14CEAE07E571A8EF2E103200CF421BAE83A66ED9F9E1AA6A9F449B653EDF1BFDB662A364D58ECF9B5FE4BB69D590DB2653F2F46A09F4D47719A862
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp5106.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):	5.189454496599504
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGwTtn:cbhK79lNQR/rydbz9I3YODOLNdq3Z
MD5:	C6FAB75DB50999549C6154EF264BE80C
SHA1:	EB84E6A1F6F4CDA87BC0BFA0C33FB853876123E5
SHA-256:	BE05BA07F3B94AE7D7C76A5FEF997D900D5DFA9A9E6A190EA2DD5A8736AE5391
SHA-512:	8E1054F87068027847AFDF2F60CB2B6BBE2FB674C31E1A1B8C93DEF4438591709A2E705E4AD7898C236028A3A3D3972BE62FF57AF5965139C9ECF2FD2D43720D
Malicious:	false
Reputation:	low
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>true

C:\Users\user\AppData\Local\Temp\tmpE52C.tmp	
Process:	C:\Users\user\Desktop\PROOF OF PAYMENT.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1646
Entropy (8bit):	5.189454496599504
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGwTtn:cbhK79lNQR/rydbz9I3YODOLNdq3Z
MD5:	C6FAB75DB50999549C6154EF264BE80C
SHA1:	EB84E6A1F6F4CDA87BC0BFA0C33FB853876123E5
SHA-256:	BE05BA07F3B94AE7D7C76A5FEF997D900D5DFA9A9E6A190EA2DD5A8736AE5391
SHA-512:	8E1054F87068027847AFDF2F60CB2B6BBE2FB674C31E1A1B8C93DEF4438591709A2E705E4AD7898C236028A3A3D3972BE62FF57AF5965139C9ECF2FD2D43720D
Malicious:	**true**
Reputation:	low
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>true

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\PROOF OF PAYMENT.exe
File Type:	ISO-8859 text, with no line terminators

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:mVbP:mxP
MD5:	9CC98A9DC31882B52047540E4E0B3CD1
SHA1:	3C4DEE67488C1716C349FD7977DAEFCCEDE7064B
SHA-256:	022A875D410DE3708A424EC637D04CF866BD83D95FE141EB0B20C3072924646A
SHA-512:	CA91BA3B6DD9E4929D4F7C0CEAA0CD248D3833C04CA2E0C32BD5A203183DCBB8EC837D4ED00661979E31D310682FAD1DA675DF05DC742EE7D9E057366EB0 A54
Malicious:	**true**
Preview:	..}.0..H

C:\Users\user\AppData\Roaming\pJrVfPlhXgkUp.exe	
Process:	C:\Users\user\Desktop\PROOF OF PAYMENT.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1168384
Entropy (8bit):	7.897636731334413
Encrypted:	false
SSDEEP:	24576:E2cXDkZfhBL97dNqehj/5L3xqpljbfrRUoq7Ohn:E2MiBBRNb5LBepfrhqyN
MD5:	DCF168394EF0A6D6774B099DD8493B75
SHA1:	565C77FA9F7F22229FF5AABAD52F6F9E0C5FBCE0
SHA-256:	373E294FCCF1CBC447469AEB6FC86678EFBFD072B5035A295D1FC74CE6E9FD79
SHA-512:	6F19BD8C1CE255848FC9E60B92B758AC960C81E3CB4C3C7BC5E520DE5B03CFC0A2244891150B50ECC179FC35A9D7F9477E567BDD275B32B4873FE640DAFE7A C9
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...................0..............@....... ....@.. ....`............ @.....................................O........................... .........................................................@..................H............\.D|.aH..... ......................@....text............................... ..`.rsrc........... ....@..@.reloc....... ....@..B.............@...................... ..`... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.897636731334413
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:	PROOF OF PAYMENT.exe
File size:	1168384
MD5:	dcf168394ef0a6d6774b099dd8493b75
SHA1:	565c77fa9f7f22229ff5aabad52f6f9e0c5fbce0
SHA256:	373e294fccf1cbc447469aeb6fc86678efbfd072b5035a295d1fc74ce6e9fd79
SHA512:	6f19bd8c1ce255848fc9e60b92b758ac960c81e3cb4c3c7bc5e520de5b03cfc0a2244891150b50ecc179fc35a9d7f9477e567bdd275b32b4873fe640dafe7ac9
SSDEEP:	24576:E2cXDkZfhBL97dNqehj/5L3xqpljbfrRUoq7Ohn:E2MiBBRNb5LBepfrhqyN
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L.....................0..............@....... ....@.. ....`.......... .@...............................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x52400a
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:	0x83ABA3EF [Sun Jan 1 20:51:59 2040 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00524000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1008ac	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x120000	0x608	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x122000	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	0x124000	0x8	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x100000	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
\D|.aH	0x2000	0xfcf8c	0xfd000	False	1.00031458436	data	7.99982924254	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.text	0x100000	0x1f3b8	0x1f400	False	0.35140625	data	4.85294552494	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x120000	0x608	0x800	False	0.33154296875	data	3.4379516301	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x122000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
	0x124000	0x10	0x200	False	0.044921875	Applesoft BASIC program data, first line number 16	0.142635768149	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x1200a0	0x376	data		
RT_MANIFEST	0x120418	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

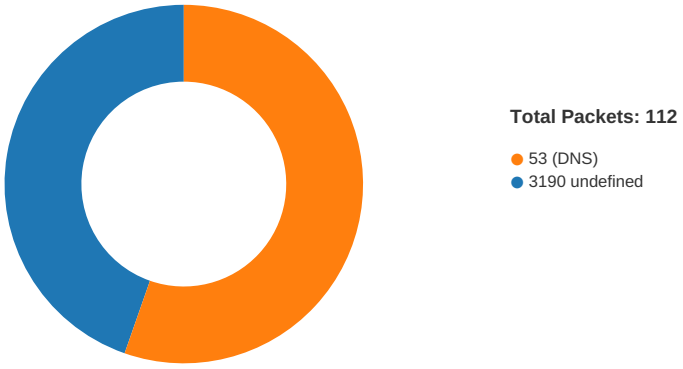
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Made Solutions International 2016
Assembly Version	36.5.0.8
InternalName	W4.exe
FileVersion	36.5.0.8
CompanyName	Made Solutions International
LegalTrademarks	
Comments	Easynote
ProductName	Admin App
ProductVersion	36.5.0.8
FileDescription	Admin App
OriginalFilename	W4.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 18:20:26.636646986 CET	49750	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:20:26.686963081 CET	3190	49750	185.140.53.131	192.168.2.4
Jan 21, 2021 18:20:27.198801041 CET	49750	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:20:27.247421980 CET	3190	49750	185.140.53.131	192.168.2.4
Jan 21, 2021 18:20:27.750178099 CET	49750	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:20:27.801548958 CET	3190	49750	185.140.53.131	192.168.2.4
Jan 21, 2021 18:20:32.339077950 CET	49753	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:20:32.387886047 CET	3190	49753	185.140.53.131	192.168.2.4
Jan 21, 2021 18:20:32.899369001 CET	49753	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:20:32.948204041 CET	3190	49753	185.140.53.131	192.168.2.4
Jan 21, 2021 18:20:33.467303991 CET	49753	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:20:33.516005993 CET	3190	49753	185.140.53.131	192.168.2.4
Jan 21, 2021 18:20:38.044141054 CET	49755	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:20:38.093015909 CET	3190	49755	185.140.53.131	192.168.2.4
Jan 21, 2021 18:20:38.665368080 CET	49755	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:20:38.714430094 CET	3190	49755	185.140.53.131	192.168.2.4
Jan 21, 2021 18:20:39.368534088 CET	49755	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:20:39.417536974 CET	3190	49755	185.140.53.131	192.168.2.4
Jan 21, 2021 18:20:43.754842997 CET	49756	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:20:43.803443909 CET	3190	49756	185.140.53.131	192.168.2.4
Jan 21, 2021 18:20:44.368943930 CET	49756	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:20:44.417614937 CET	3190	49756	185.140.53.131	192.168.2.4
Jan 21, 2021 18:20:45.056510925 CET	49756	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:20:45.105313063 CET	3190	49756	185.140.53.131	192.168.2.4
Jan 21, 2021 18:20:49.941091061 CET	49759	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:20:49.989852905 CET	3190	49759	185.140.53.131	192.168.2.4
Jan 21, 2021 18:20:50.599390984 CET	49759	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:20:50.647996902 CET	3190	49759	185.140.53.131	192.168.2.4
Jan 21, 2021 18:20:51.338809967 CET	49759	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:20:51.387382030 CET	3190	49759	185.140.53.131	192.168.2.4
Jan 21, 2021 18:20:55.870851040 CET	49768	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:20:55.919444084 CET	3190	49768	185.140.53.131	192.168.2.4
Jan 21, 2021 18:20:56.432501078 CET	49768	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:20:56.481225014 CET	3190	49768	185.140.53.131	192.168.2.4
Jan 21, 2021 18:20:56.995039940 CET	49768	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:20:57.043771029 CET	3190	49768	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:01.385477066 CET	49771	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:01.434214115 CET	3190	49771	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:01.948607922 CET	49771	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:01.998749971 CET	3190	49771	185.140.53.131	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 18:21:02.511146069 CET	49771	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:02.560031891 CET	3190	49771	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:06.981112003 CET	49777	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:07.030205011 CET	3190	49777	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:07.620959997 CET	49777	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:07.669727087 CET	3190	49777	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:08.184009075 CET	49777	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:08.232570887 CET	3190	49777	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:14.020345926 CET	49778	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:14.069040060 CET	3190	49778	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:14.574636936 CET	49778	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:14.623289108 CET	3190	49778	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:15.137156010 CET	49778	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:15.185831070 CET	3190	49778	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:19.581602097 CET	49779	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:19.632669926 CET	3190	49779	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:20.137590885 CET	49779	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:20.186188936 CET	3190	49779	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:20.700217962 CET	49779	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:20.748981953 CET	3190	49779	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:25.395379066 CET	49780	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:25.444143057 CET	3190	49780	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:25.950561047 CET	49780	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:25.999279976 CET	3190	49780	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:26.513206005 CET	49780	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:26.561887980 CET	3190	49780	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:30.962618113 CET	49781	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:31.011766911 CET	3190	49781	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:31.529175043 CET	49781	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:31.579611063 CET	3190	49781	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:32.107358932 CET	49781	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:32.156056881 CET	3190	49781	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:36.731923103 CET	49783	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:36.780670881 CET	3190	49783	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:37.295358896 CET	49783	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:37.344342947 CET	3190	49783	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:37.857836962 CET	49783	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:37.906586885 CET	3190	49783	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:42.471095085 CET	49785	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:42.519733906 CET	3190	49785	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:43.030142069 CET	49785	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:43.078917980 CET	3190	49785	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:43.592746019 CET	49785	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:43.641819000 CET	3190	49785	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:48.097086906 CET	49786	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:48.145708084 CET	3190	49786	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:48.655638933 CET	49786	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:48.704374075 CET	3190	49786	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:49.218244076 CET	49786	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:49.267738104 CET	3190	49786	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:53.814023972 CET	49787	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:53.862994909 CET	3190	49787	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:54.374924898 CET	49787	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:54.423679113 CET	3190	49787	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:54.937490940 CET	49787	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:54.986247063 CET	3190	49787	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:59.346096992 CET	49788	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:59.394851923 CET	3190	49788	185.140.53.131	192.168.2.4
Jan 21, 2021 18:21:59.906557083 CET	49788	3190	192.168.2.4	185.140.53.131
Jan 21, 2021 18:21:59.955153942 CET	3190	49788	185.140.53.131	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 18:19:55.067909002 CET	58028	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:19:55.124077082 CET	53	58028	8.8.8.8	192.168.2.4
Jan 21, 2021 18:19:55.292099953 CET	53097	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:19:55.360272884 CET	53	53097	8.8.8.8	192.168.2.4
Jan 21, 2021 18:19:56.059154987 CET	49257	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:19:56.111537933 CET	53	49257	8.8.8.8	192.168.2.4
Jan 21, 2021 18:19:57.197954893 CET	62389	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:19:57.248848915 CET	53	62389	8.8.8.8	192.168.2.4
Jan 21, 2021 18:19:58.334696054 CET	49910	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:19:58.382865906 CET	53	49910	8.8.8.8	192.168.2.4
Jan 21, 2021 18:19:59.385020971 CET	55854	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:19:59.432925940 CET	53	55854	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:00.752772093 CET	64549	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:00.800936937 CET	53	64549	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:01.719530106 CET	63153	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:01.767502069 CET	53	63153	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:03.152363062 CET	52991	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:03.200278997 CET	53	52991	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:04.301790953 CET	53700	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:04.349843979 CET	53	53700	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:05.165674925 CET	51726	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:05.213634014 CET	53	51726	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:06.164575100 CET	56794	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:06.212635040 CET	53	56794	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:07.111299038 CET	56534	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:07.159250975 CET	53	56534	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:08.289347887 CET	56627	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:08.340187073 CET	53	56627	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:09.239306927 CET	56621	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:09.290049076 CET	53	56621	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:10.020481110 CET	63116	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:10.068592072 CET	53	63116	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:11.006031990 CET	64078	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:11.065057039 CET	53	64078	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:11.964874983 CET	64801	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:12.021156073 CET	53	64801	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:26.377454042 CET	61721	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:26.597150087 CET	53	61721	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:26.736705065 CET	51255	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:26.788639069 CET	53	51255	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:32.287314892 CET	61522	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:32.338031054 CET	53	61522	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:32.374512911 CET	52337	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:32.432138920 CET	53	52337	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:37.819787979 CET	55046	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:38.041517019 CET	53	55046	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:43.690567970 CET	49612	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:43.753215075 CET	53	49612	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:45.001816034 CET	49285	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:45.061233044 CET	53	49285	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:49.048403025 CET	50601	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:49.099143982 CET	53	50601	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:49.716054916 CET	60875	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:49.896989107 CET	56448	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:49.939874887 CET	53	60875	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:49.953588963 CET	53	56448	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:50.628110886 CET	59172	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:50.689544916 CET	53	59172	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:51.162794113 CET	62420	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:51.219170094 CET	53	62420	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:51.649856091 CET	60579	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:51.713937044 CET	53	60579	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:51.780478001 CET	50183	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:51.829261065 CET	53	50183	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 21, 2021 18:20:52.846740961 CET	61531	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:52.897475004 CET	53	61531	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:53.946583033 CET	49228	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:53.997590065 CET	53	49228	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:55.800205946 CET	59794	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:55.812844992 CET	55916	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:55.848177910 CET	53	59794	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:55.869412899 CET	53	55916	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:56.771868944 CET	52752	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:56.822704077 CET	53	52752	8.8.8.8	192.168.2.4
Jan 21, 2021 18:20:57.481784105 CET	60542	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:20:57.532876015 CET	53	60542	8.8.8.8	192.168.2.4
Jan 21, 2021 18:21:01.327616930 CET	60689	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:21:01.384275913 CET	53	60689	8.8.8.8	192.168.2.4
Jan 21, 2021 18:21:05.048038960 CET	64206	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:21:05.106128931 CET	53	64206	8.8.8.8	192.168.2.4
Jan 21, 2021 18:21:06.923330069 CET	50904	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:21:06.979444981 CET	53	50904	8.8.8.8	192.168.2.4
Jan 21, 2021 18:21:13.962409019 CET	57525	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:21:14.018889904 CET	53	57525	8.8.8.8	192.168.2.4
Jan 21, 2021 18:21:19.522490978 CET	53814	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:21:19.579447985 CET	53	53814	8.8.8.8	192.168.2.4
Jan 21, 2021 18:21:25.142821074 CET	53418	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:21:25.363347054 CET	53	53418	8.8.8.8	192.168.2.4
Jan 21, 2021 18:21:30.839421988 CET	62833	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:21:30.887420893 CET	53	62833	8.8.8.8	192.168.2.4
Jan 21, 2021 18:21:35.675800085 CET	59260	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:21:35.726835966 CET	53	59260	8.8.8.8	192.168.2.4
Jan 21, 2021 18:21:36.682862997 CET	49944	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:21:36.730860949 CET	53	49944	8.8.8.8	192.168.2.4
Jan 21, 2021 18:21:37.322103024 CET	63300	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:21:37.378932953 CET	53	63300	8.8.8.8	192.168.2.4
Jan 21, 2021 18:21:42.412513018 CET	61449	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:21:42.468755960 CET	53	61449	8.8.8.8	192.168.2.4
Jan 21, 2021 18:21:48.038727045 CET	51275	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:21:48.094996929 CET	53	51275	8.8.8.8	192.168.2.4
Jan 21, 2021 18:21:53.752360106 CET	63492	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:21:53.811616898 CET	53	63492	8.8.8.8	192.168.2.4
Jan 21, 2021 18:21:59.287313938 CET	58945	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:21:59.344736099 CET	53	58945	8.8.8.8	192.168.2.4
Jan 21, 2021 18:22:06.958884001 CET	60779	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:22:07.179647923 CET	53	60779	8.8.8.8	192.168.2.4
Jan 21, 2021 18:22:13.336189985 CET	64014	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:22:13.397027969 CET	53	64014	8.8.8.8	192.168.2.4
Jan 21, 2021 18:22:19.120923996 CET	57091	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:22:19.180563927 CET	53	57091	8.8.8.8	192.168.2.4
Jan 21, 2021 18:22:24.973064899 CET	55904	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:22:25.033624887 CET	53	55904	8.8.8.8	192.168.2.4
Jan 21, 2021 18:22:30.705987930 CET	52109	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:22:30.762120962 CET	53	52109	8.8.8.8	192.168.2.4
Jan 21, 2021 18:22:36.456420898 CET	54450	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:22:36.686892986 CET	53	54450	8.8.8.8	192.168.2.4
Jan 21, 2021 18:22:42.330946922 CET	49374	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:22:42.389832020 CET	53	49374	8.8.8.8	192.168.2.4
Jan 21, 2021 18:22:48.195000887 CET	50436	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:22:48.251329899 CET	53	50436	8.8.8.8	192.168.2.4
Jan 21, 2021 18:22:54.368314981 CET	62605	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:22:54.424686909 CET	53	62605	8.8.8.8	192.168.2.4
Jan 21, 2021 18:22:59.616128922 CET	54256	53	192.168.2.4	8.8.8.8
Jan 21, 2021 18:22:59.672491074 CET	53	54256	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 21, 2021 18:20:26.377454042 CET	192.168.2.4	8.8.8.8	0x25e9	Standard query (0)	amechi.duc kdns.org	A (IP address)	IN (0x0001)
Jan 21, 2021 18:20:32.287314892 CET	192.168.2.4	8.8.8.8	0xe11e	Standard query (0)	amechi.duc kdns.org	A (IP address)	IN (0x0001)
Jan 21, 2021 18:20:37.819787979 CET	192.168.2.4	8.8.8.8	0x7842	Standard query (0)	amechi.duc kdns.org	A (IP address)	IN (0x0001)
Jan 21, 2021 18:20:43.690567970 CET	192.168.2.4	8.8.8.8	0xd26f	Standard query (0)	amechi.duc kdns.org	A (IP address)	IN (0x0001)
Jan 21, 2021 18:20:49.716054916 CET	192.168.2.4	8.8.8.8	0xe4b8	Standard query (0)	amechi.duc kdns.org	A (IP address)	IN (0x0001)
Jan 21, 2021 18:20:55.812844992 CET	192.168.2.4	8.8.8.8	0xf037	Standard query (0)	amechi.duc kdns.org	A (IP address)	IN (0x0001)
Jan 21, 2021 18:21:01.327616930 CET	192.168.2.4	8.8.8.8	0x619f	Standard query (0)	amechi.duc kdns.org	A (IP address)	IN (0x0001)
Jan 21, 2021 18:21:06.923330069 CET	192.168.2.4	8.8.8.8	0x7af2	Standard query (0)	amechi.duc kdns.org	A (IP address)	IN (0x0001)
Jan 21, 2021 18:21:13.962409019 CET	192.168.2.4	8.8.8.8	0xa328	Standard query (0)	amechi.duc kdns.org	A (IP address)	IN (0x0001)
Jan 21, 2021 18:21:19.522490978 CET	192.168.2.4	8.8.8.8	0x75b9	Standard query (0)	amechi.duc kdns.org	A (IP address)	IN (0x0001)
Jan 21, 2021 18:21:25.142821074 CET	192.168.2.4	8.8.8.8	0xca7e	Standard query (0)	amechi.duc kdns.org	A (IP address)	IN (0x0001)
Jan 21, 2021 18:21:30.839421988 CET	192.168.2.4	8.8.8.8	0xa158	Standard query (0)	amechi.duc kdns.org	A (IP address)	IN (0x0001)
Jan 21, 2021 18:21:36.682862997 CET	192.168.2.4	8.8.8.8	0x7ced	Standard query (0)	amechi.duc kdns.org	A (IP address)	IN (0x0001)
Jan 21, 2021 18:21:42.412513018 CET	192.168.2.4	8.8.8.8	0xdd3a	Standard query (0)	amechi.duc kdns.org	A (IP address)	IN (0x0001)
Jan 21, 2021 18:21:48.038727045 CET	192.168.2.4	8.8.8.8	0x7241	Standard query (0)	amechi.duc kdns.org	A (IP address)	IN (0x0001)
Jan 21, 2021 18:21:53.752360106 CET	192.168.2.4	8.8.8.8	0xff5c	Standard query (0)	amechi.duc kdns.org	A (IP address)	IN (0x0001)
Jan 21, 2021 18:21:59.287313938 CET	192.168.2.4	8.8.8.8	0xf33b	Standard query (0)	amechi.duc kdns.org	A (IP address)	IN (0x0001)
Jan 21, 2021 18:22:06.958884001 CET	192.168.2.4	8.8.8.8	0x4d84	Standard query (0)	amechi.duc kdns.org	A (IP address)	IN (0x0001)
Jan 21, 2021 18:22:13.336189985 CET	192.168.2.4	8.8.8.8	0x3e3b	Standard query (0)	amechi.duc kdns.org	A (IP address)	IN (0x0001)
Jan 21, 2021 18:22:19.120923996 CET	192.168.2.4	8.8.8.8	0xbcb1	Standard query (0)	amechi.duc kdns.org	A (IP address)	IN (0x0001)
Jan 21, 2021 18:22:24.973064899 CET	192.168.2.4	8.8.8.8	0x3699	Standard query (0)	amechi.duc kdns.org	A (IP address)	IN (0x0001)
Jan 21, 2021 18:22:30.705987930 CET	192.168.2.4	8.8.8.8	0xf2cf	Standard query (0)	amechi.duc kdns.org	A (IP address)	IN (0x0001)
Jan 21, 2021 18:22:36.456420898 CET	192.168.2.4	8.8.8.8	0x9a64	Standard query (0)	amechi.duc kdns.org	A (IP address)	IN (0x0001)
Jan 21, 2021 18:22:42.330946922 CET	192.168.2.4	8.8.8.8	0x4f70	Standard query (0)	amechi.duc kdns.org	A (IP address)	IN (0x0001)
Jan 21, 2021 18:22:48.195000887 CET	192.168.2.4	8.8.8.8	0xde87	Standard query (0)	amechi.duc kdns.org	A (IP address)	IN (0x0001)
Jan 21, 2021 18:22:54.368314981 CET	192.168.2.4	8.8.8.8	0xc231	Standard query (0)	amechi.duc kdns.org	A (IP address)	IN (0x0001)
Jan 21, 2021 18:22:59.616128922 CET	192.168.2.4	8.8.8.8	0x2a6b	Standard query (0)	amechi.duc kdns.org	A (IP address)	IN (0x0001)

DNS Answers

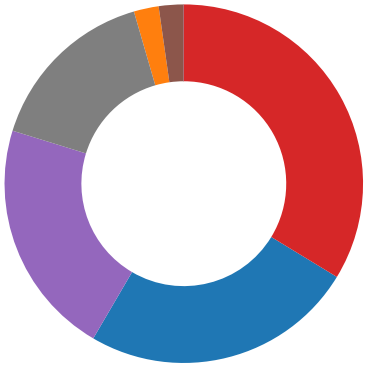
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 21, 2021 18:20:26.597150087 CET	8.8.8.8	192.168.2.4	0x25e9	No error (0)	amechi.duc kdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 21, 2021 18:20:32.338031054 CET	8.8.8.8	192.168.2.4	0xe11e	No error (0)	amechi.duc kdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 21, 2021 18:20:38.041517019 CET	8.8.8.8	192.168.2.4	0x7842	No error (0)	amechi.duc kdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 21, 2021 18:20:43.753215075 CET	8.8.8.8	192.168.2.4	0xd26f	No error (0)	amechi.duc kdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 21, 2021 18:20:49.939874887 CET	8.8.8.8	192.168.2.4	0xe4b8	No error (0)	amechi.duc kdns.org		185.140.53.131	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 21, 2021 18:20:55.869412899 CET	8.8.8.8	192.168.2.4	0xf037	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 21, 2021 18:21:01.384275913 CET	8.8.8.8	192.168.2.4	0x619f	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 21, 2021 18:21:06.979444981 CET	8.8.8.8	192.168.2.4	0x7af2	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 21, 2021 18:21:14.018889904 CET	8.8.8.8	192.168.2.4	0xa328	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 21, 2021 18:21:19.579447985 CET	8.8.8.8	192.168.2.4	0x75b9	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 21, 2021 18:21:25.363347054 CET	8.8.8.8	192.168.2.4	0xca7e	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 21, 2021 18:21:30.887420893 CET	8.8.8.8	192.168.2.4	0xa158	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 21, 2021 18:21:36.730860949 CET	8.8.8.8	192.168.2.4	0x7ced	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 21, 2021 18:21:42.468755960 CET	8.8.8.8	192.168.2.4	0xdd3a	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 21, 2021 18:21:48.094996929 CET	8.8.8.8	192.168.2.4	0x7241	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 21, 2021 18:21:53.811616898 CET	8.8.8.8	192.168.2.4	0xff5c	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 21, 2021 18:21:59.344736099 CET	8.8.8.8	192.168.2.4	0xf33b	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 21, 2021 18:22:07.179647923 CET	8.8.8.8	192.168.2.4	0x4d84	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 21, 2021 18:22:13.397027969 CET	8.8.8.8	192.168.2.4	0x3e3b	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 21, 2021 18:22:19.180563927 CET	8.8.8.8	192.168.2.4	0xbcb1	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 21, 2021 18:22:25.033624887 CET	8.8.8.8	192.168.2.4	0x3699	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 21, 2021 18:22:30.762120962 CET	8.8.8.8	192.168.2.4	0xf2cf	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 21, 2021 18:22:36.686892986 CET	8.8.8.8	192.168.2.4	0x9a64	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 21, 2021 18:22:42.389832020 CET	8.8.8.8	192.168.2.4	0x4f70	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 21, 2021 18:22:48.251329899 CET	8.8.8.8	192.168.2.4	0xde87	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 21, 2021 18:22:54.424686909 CET	8.8.8.8	192.168.2.4	0xc231	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 21, 2021 18:22:59.672491074 CET	8.8.8.8	192.168.2.4	0x2a6b	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: PROOF OF PAYMENT.exe PID: 7064 Parent PID: 5900

General

Start time:	18:19:59
Start date:	21/01/2021
Path:	C:\Users\user\Desktop\PROOF OF PAYMENT.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PROOF OF PAYMENT.exe'
Imagebase:	0x640000
File size:	1168384 bytes
MD5 hash:	DCF168394EF0A6D6774B099DD8493B75
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: 00000001.00000002.701087056.0000000003B39000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.701087056.0000000003B39000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.701087056.0000000003B39000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.697967874.0000000002B2B000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.701602201.0000000003D39000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.701602201.0000000003D39000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.701602201.0000000003D39000.00000004.00000001.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	6D1CCF06	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	6D1CCF06	unknown
C:\Users\user\AppData\Roaming\pJrVfPIhXgkUp.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C011E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpE52C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C017038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PROOF OF PAYMENT.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D4DC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE52C.tmp	success or wait	1	6C016A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pJrVfPIhXgkUp.exe	unknown	1168384	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 ef a3 ab 83 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 f6 01 00 00 da 0f 00 00 00 00 00 0a 40 12 00 00 00 10 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 60 12 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................. ....0.............@....... ....@.. ....` ....@.................	success or wait	1	6C011B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpE52C.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 6a 6f 6e 65 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 6e	<?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>.. </RegistrationIn	success or wait	1	6C011B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PROOF OF PAYMENT.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Windows.Forms, Vers	success or wait	1	6D4DC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Users\user\Desktop\PROOF OF PAYMENT.exe	unknown	1168384	success or wait	1	6C011B4F	ReadFile

Analysis Process: schtasks.exe PID: 6012 Parent PID: 7064

General

Start time:	18:20:20
Start date:	21/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\pJrVfPIhXgkUp' /XML 'C:\ Users\user\AppData\Local\Temp\tmpE52C.tmp'
Imagebase:	0x1390000
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\tmpE52C.tmp	unknown	2	success or wait	1	139AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpE52C.tmp	unknown	1647	success or wait	1	139ABD9	ReadFile

Analysis Process: conhost.exe PID: 5700 Parent PID: 6012

General

Start time:	18:20:21
Start date:	21/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: PROOF OF PAYMENT.exe PID: 6816 Parent PID: 7064

General

Start time:	18:20:21
Start date:	21/01/2021
Path:	C:\Users\user\Desktop\PROOF OF PAYMENT.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x920000
File size:	1168384 bytes
MD5 hash:	DCF168394EF0A6D6774B099DD8493B75
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: 00000007.00000002.1026361866.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.1026361866.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.1026361866.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.1028093890.0000000002D01000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.1029421863.0000000003D49000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.1029421863.0000000003D49000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.1031888458.0000000005F70000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.1031888458.0000000005F70000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.1031888458.0000000005F70000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.1031725645.0000000005EE0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.1031725645.0000000005EE0000.00000004.00000001.sdmp, Author: Florian Roth
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	6D1CCF06	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	6D1CCF06	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	6C01BEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6C011E60	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	6C01BEFF	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	6C01DD66	CopyFileW
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	6C01DD66	CopyFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C01BEFF	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	6C01BEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PROOF OF PAYMENT.exe:Zone.Identifier	success or wait	1	6BF92935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	ae ee 7d d6 30 be d8 48	..}.0..H	success or wait	1	6C011B4F	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 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 ef a3 ab 83 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 f6 01 00 00 da 0f 00 00 00 00 00 0a 40 12 00 00 00 10 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 60 12 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................ ....0.............@....... ....@.. ....` ....@................	success or wait	5	6C01DD66	CopyFileW
C:\Program Files (x86)\DHCP Mo nitor\dhcpmon.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6C01DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0 .0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D18D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0 .0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D18D72F	unknown
C:\Users\user\Desktop\PROOF OF PAYMENT.exe	unknown	4096	success or wait	1	6D18D72F	unknown
C:\Users\user\Desktop\PROOF OF PAYMENT.exe	unknown	512	success or wait	1	6D18D72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	6C01646A	RegSetValueExW

Analysis Process: dhcpmon.exe PID: 5820 Parent PID: 3424

General

Start time:	18:20:36
Start date:	21/01/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xe60000
File size:	1168384 bytes
MD5 hash:	DCF168394EF0A6D6774B099DD8493B75
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: 0000000C.00000002.758221792.0000000004617000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.758221792.0000000004617000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.758221792.0000000004617000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.757375675.000000000441B000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.757375675.000000000441B000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.757375675.000000000441B000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D1CCF06	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	6D1CCF06	unknown
C:\Users\user\AppData\Local\Temp\tmp5106.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C017038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D4DC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp5106.tmp	success or wait	1	6C016A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp5106.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 6a 6f 6e 65 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 6e	<?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>.. </RegistrationIn	success or wait	1	6C011B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Windows.Forms, Vers	success or wait	1	6D4DC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile

Analysis Process: schtasks.exe PID: 2208 Parent PID: 5820

General

Start time:	18:20:45
Start date:	21/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\pJrVfPIhXgkUp' /XML 'C:\Users\user\AppData\Local\Temp\tmp5106.tmp'
Imagebase:	0x1390000
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\tmp5106.tmp	unknown	2	success or wait	1	139AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp5106.tmp	unknown	1647	success or wait	1	139ABD9	ReadFile

Analysis Process: conhost.exe PID: 2044 Parent PID: 2208

General

Start time:	18:20:46
Start date:	21/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: 6780 Parent PID: 5820

General

Start time:	18:20:46
Start date:	21/01/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xa70000
File size:	1168384 bytes
MD5 hash:	DCF168394EF0A6D6774B099DD8493B75
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: 00000011.00000002.770483355.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.770483355.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.770483355.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.772863265.0000000003EA9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.772863265.0000000003EA9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.772748001.0000000002EA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.772748001.0000000002EA1000.00000004.00000001.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	6D1CCF06	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	6D1CCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D1A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D1003DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D1003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D1003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D1A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C011B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C011B4F	ReadFile

Disassembly

Code Analysis