ID: 341478
Sample Name: PROOF OF PAYMENT.exe
Cookbook: default.jbs
Time: 12:59:11
Date: 19/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents 2
Analysis Report PROOF OF PAYMENT.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: NanoCore 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Signature Overview 5
AV Detection: 6
Compliance: 6
Networking: 6
E-Banking Fraud: 6
System Summary: 6
Data Obfuscation: 6
Boot Survival: 6
Hooking and other Techniques for Hiding and Protection: 6
Malware Analysis System Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 10
Contacted IPs 13
Public 13
Private 13
General Information 13
Simulations 15
Behavior and APIs 15
Joe Sandbox View / Context 15
IPs 15
Domains 15
ASN 15
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
Static File Info 18
General 18
File Icon 19

Static PE Info 19
General 19
Entrypoint Preview 19
Data Directories 21
Sections 21
Resources 21
Imports 21
Version Infos 22
Network Behavior 22
Network Port Distribution 22
TCP Packets 22
UDP Packets 23
DNS Queries 24
DNS Answers 24
Code Manipulations 25
Statistics 25
Behavior 25
System Behavior 25
Analysis Process: PROOF OF PAYMENT.exe PID: 6396 Parent PID: 5892 25
General 25
File Activities 26
File Created 26
File Deleted 26
File Written 26
File Read 28
Analysis Process: schtasks.exe PID: 4712 Parent PID: 6396 28
General 28
File Activities 29
File Read 29
Analysis Process: conhost.exe PID: 6252 Parent PID: 4712 29
General 29
Analysis Process: PROOF OF PAYMENT.exe PID: 4540 Parent PID: 6396 29
General 29
File Activities 30
File Created 30
File Deleted 31
File Written 31
File Read 31
Registry Activities 32
Key Value Created 32
Analysis Process: dhcpmon.exe PID: 6868 Parent PID: 3440 32
General 32
File Activities 32
File Created 32
File Deleted 33
File Written 33
File Read 34
Analysis Process: schtasks.exe PID: 7048 Parent PID: 6868 34
General 34
File Activities 35
File Read 35
Analysis Process: conhost.exe PID: 6952 Parent PID: 7048 35
General 35
Analysis Process: dhcpmon.exe PID: 6796 Parent PID: 6868 35
General 35
File Activities 36
File Created 36
File Read 36
Disassembly 36
Code Analysis 36

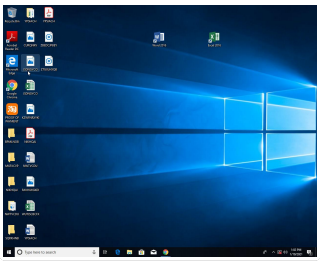
Analysis Report PROOF OF PAYMENT.exe

Overview

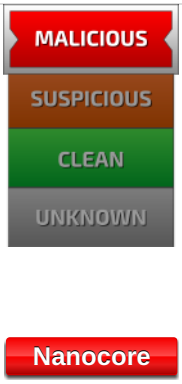
General Information

Sample Name:	PROOF OF PAYMENT.exe
Analysis ID:	341478
MD5:	57090f9293d9a01.
SHA1:	c477a883773dec..
SHA256:	7f7afb406c8f911…
Tags:	exe NanoCore nVpn RAT

Most interesting Screenshot:



Detection



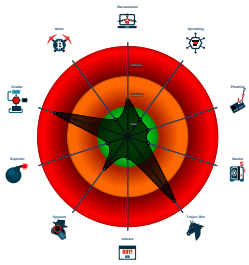
Nanocore

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

Signatures

- Detected Nanocore Rat
- 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…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Startup

- **System is w10x64**
- PROOF OF PAYMENT.exe (PID: 6396 cmdline: 'C:\Users\user\Desktop\PROOF OF PAYMENT.exe' MD5: 57090F9293D9A013C7FF7FB614681A46)
  - schtasks.exe (PID: 4712 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\RbJJtmpPB' /XML 'C:\Users\user\AppData\Local\Temp\tmpC0F9.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6252 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - PROOF OF PAYMENT.exe (PID: 4540 cmdline: {path} MD5: 57090F9293D9A013C7FF7FB614681A46)
- dhcpmon.exe (PID: 6868 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 57090F9293D9A013C7FF7FB614681A46)
  - schtasks.exe (PID: 7048 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\RbJJtmpPB' /XML 'C:\Users\user\AppData\Local\Temp\tmpB41.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6952 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 6796 cmdline: {path} MD5: 57090F9293D9A013C7FF7FB614681A46)
- **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
00000003.00000002.716409354.0000000005F0 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost

Source	Rule	Description	Author	Strings
00000003.00000002.716409354.0000000005F0 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
00000003.00000002.716409354.0000000005F0 0000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.364292242.0000000003FB F000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x157b65:$x1: NanoCore.ClientPluginHost • 0x157ba2:$x2: IClientNetworkHost • 0x15b6d5:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.364292242.0000000003FB F000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 35 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.PROOF OF PAYMENT.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
3.2.PROOF OF PAYMENT.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
3.2.PROOF OF PAYMENT.exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
3.2.PROOF OF PAYMENT.exe.400000.0.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
3.2.PROOF OF PAYMENT.exe.5f00000.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
Click to see the 11 entries				

Sigma Overview

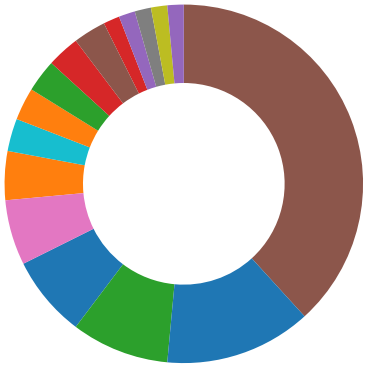
System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview

- AV Detection
- Compliance
- 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
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

- Found malware configuration
- 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

Data Obfuscation:

- .NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM_3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

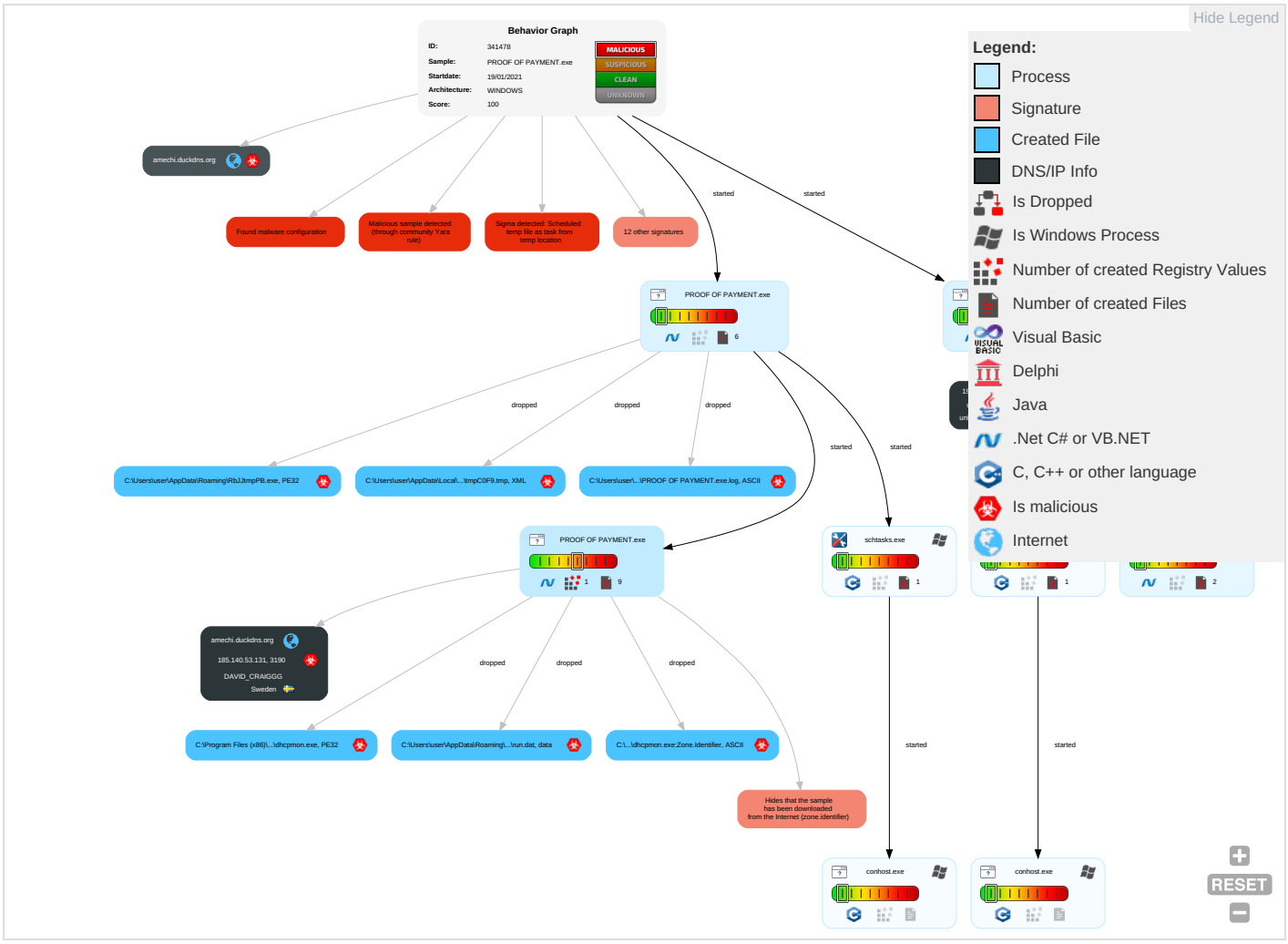
Detected Nanocore Rat

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 1 1	Security Software Discovery 1 1 1	Remote Services	Input Capture 1 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 3	LSASS Memory	Virtualization/Sandbox Evasion 3	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 2	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 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocols

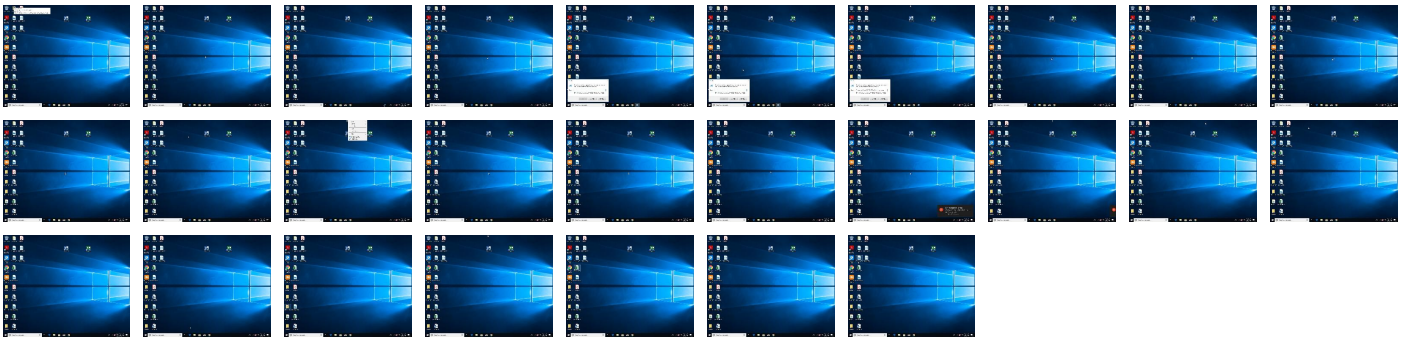
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
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\RbJJtmpPB.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.PROOF OF PAYMENT.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.2.PROOF OF PAYMENT.exe.5f00000.6.unpack	100%	Avira	TR/NanoCore.fadte		Download File
11.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
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.fontbureau.comma	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.comion	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.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.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.como1	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	
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.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	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		unknown

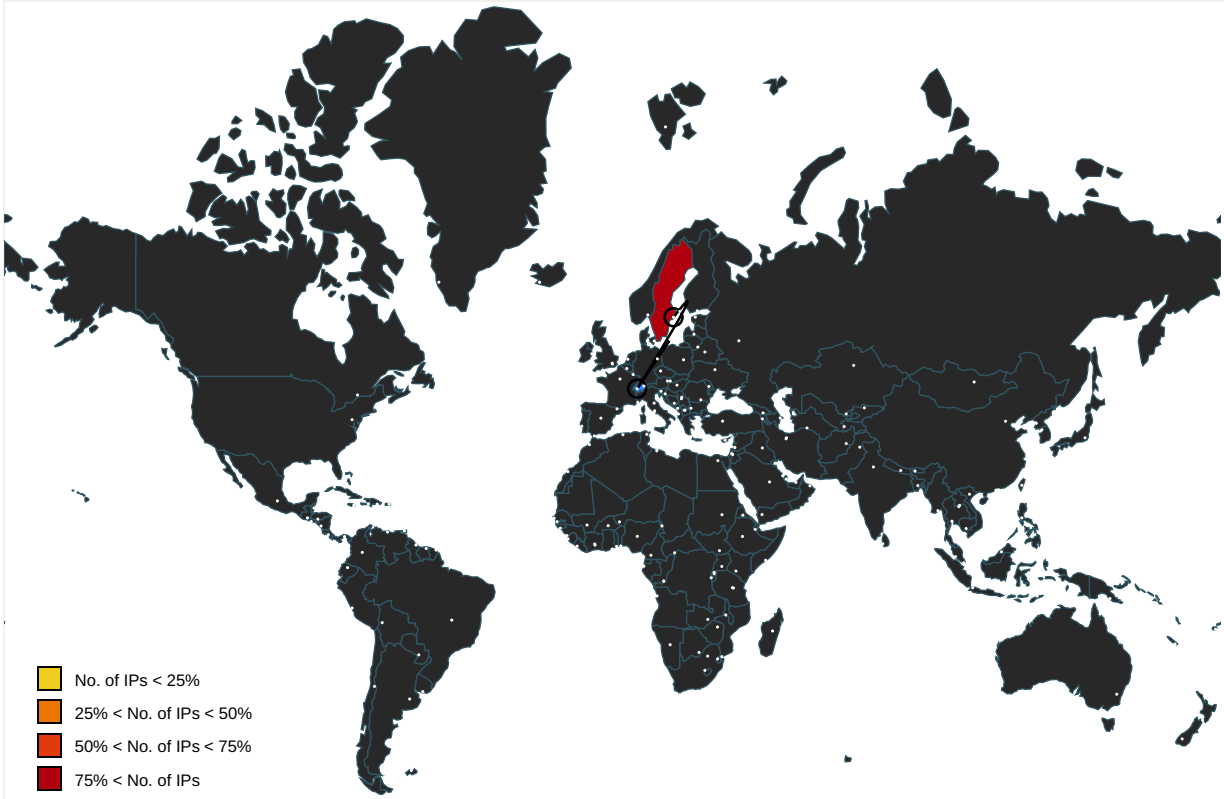
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	PROOF OF PAYMENT.exe, 00000000.00000002.368359287.0000000006E12000.00000004.00000001.sdmp, dhcpmon.exe, 00000007.00000002.408064954.0000000006010000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	PROOF OF PAYMENT.exe, 00000000.00000002.368359287.0000000006E12000.00000004.00000001.sdmp, dhcpmon.exe, 00000007.00000002.408064954.0000000006010000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	PROOF OF PAYMENT.exe, 00000000.00000002.368359287.0000000006E12000.00000004.00000001.sdmp, dhcpmon.exe, 00000007.00000002.408064954.0000000006010000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	PROOF OF PAYMENT.exe, 00000000.00000002.368359287.0000000006E12000.00000004.00000001.sdmp, dhcpmon.exe, 00000007.00000002.408064954.0000000006010000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	PROOF OF PAYMENT.exe, 00000000.00000002.368359287.0000000006E12000.00000004.00000001.sdmp, dhcpmon.exe, 00000007.00000002.408064954.0000000006010000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	PROOF OF PAYMENT.exe, 00000000.00000002.368359287.0000000006E12000.00000004.00000001.sdmp, dhcpmon.exe, 00000007.00000002.408064954.0000000006010000.00000002.00000001.sdmp	false		high
http://www.fontbureau.comma	PROOF OF PAYMENT.exe, 00000000.00000002.355257450.0000000000D97000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	dhcpmon.exe, 00000007.00000002.408064954.0000000006010000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comion	PROOF OF PAYMENT.exe, 00000000.00000002.355257450.0000000000D97000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	dhcpmon.exe, 00000007.00000002.408064954.0000000006010000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	PROOF OF PAYMENT.exe, 00000000.00000002.368359287.0000000006E12000.00000004.00000001.sdmp, dhcpmon.exe, 00000007.00000002.408064954.0000000006010000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	PROOF OF PAYMENT.exe, 00000000.00000002.368359287.0000000006E12000.00000004.00000001.sdmp, dhcpmon.exe, 00000007.00000002.408064954.0000000006010000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	PROOF OF PAYMENT.exe, 00000000.00000002.368359287.0000000006E12000.00000004.00000001.sdmp, dhcpmon.exe, 00000007.00000002.408064954.0000000006010000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	PROOF OF PAYMENT.exe, 00000000.00000002.368359287.0000000006E12000.00000004.00000001.sdmp, dhcpmon.exe, 00000007.00000002.408064954.0000000006010000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	PROOF OF PAYMENT.exe, 00000000.00000002.368359287.0000000006E12000.00000004.00000001.sdmp, dhcpmon.exe, 00000007.00000002.408064954.0000000006010000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/cThe	PROOF OF PAYMENT.exe, 00000000.00000002.368359287.0000000006E12000.00000004.00000001.sdmp, dhcpmon.exe, 00000007.00000002.408064954.0000000006010000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	PROOF OF PAYMENT.exe, 00000000.00000002.368359287.0000000006E12000.00000004.00000001.sdmp, dhcpmon.exe, 00000007.00000002.408064954.0000000006010000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	PROOF OF PAYMENT.exe, 00000000.00000002.368359287.0000000006E12000.00000004.00000001.sdmp, dhcpmon.exe, 00000007.00000002.408064954.0000000006010000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	PROOF OF PAYMENT.exe, 00000000.00000002.368359287.0000000006E12000.00000004.00000001.sdmp, dhcpmon.exe, 00000007.00000002.408064954.0000000006010000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	PROOF OF PAYMENT.exe, 00000000.00000002.368359287.0000000006E12000.00000004.00000001.sdmp, dhcpmon.exe, 00000007.00000002.408064954.0000000006010000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	PROOF OF PAYMENT.exe, 00000000.00000002.368359287.0000000006E12000.00000004.00000001.sdmp, dhcpmon.exe, 00000007.00000002.408064954.0000000006010000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	PROOF OF PAYMENT.exe, 00000000.00000002.368359287.0000000006E12000.00000004.00000001.sdmp, dhcpmon.exe, 00000007.00000002.408064954.0000000006010000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	PROOF OF PAYMENT.exe, 00000000.00000002.368359287.0000000006E12000.00000004.00000001.sdmp, dhcpmon.exe, 00000007.00000002.408064954.0000000006010000.00000002.00000001.sdmp	false		high
http://www.fontbureau.como1	PROOF OF PAYMENT.exe, 00000000.00000002.355257450.0000000000D97000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fonts.com	PROOF OF PAYMENT.exe, 00000000.00000002.368359287.0000000006E12000.00000004.00000001.sdmp, dhcpmon.exe, 00000007.00000002.408064954.0000000006010000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	PROOF OF PAYMENT.exe, 00000000.00000002.368359287.0000000006E12000.00000004.00000001.sdmp, dhcpmon.exe, 00000007.00000002.408064954.0000000006010000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	PROOF OF PAYMENT.exe, 00000000.00000002.368359287.0000000006E12000.00000004.00000001.sdmp, dhcpmon.exe, 00000007.00000002.408064954.0000000006010000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	PROOF OF PAYMENT.exe, 00000000.00000002.368359287.0000000006E12000.00000004.00000001.sdmp, dhcpmon.exe, 00000007.00000002.408064954.0000000006010000.00000002.00000001.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, 00000000.00000002.356878983.0000000002E41000.00000004.00000001.sdmp, dhcpmon.exe, 00000007.00000002.403339864.0000000003021000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	PROOF OF PAYMENT.exe, 00000000.00000002.368359287.0000000006E12000.00000004.00000001.sdmp, dhcpmon.exe, 00000007.00000002.408064954.0000000006010000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

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:	341478
Start date:	19.01.2021
Start time:	12:59:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 23s
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:	27

Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@12/8@10/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 104.43.193.48, 40.88.32.150, 52.147.198.201, 51.11.168.160, 92.122.213.201, 92.122.213.247, 205.185.216.10, 205.185.216.42, 51.103.5.159, 52.254.96.93, 20.54.26.129, 104.84.56.60, 20.190.159.138, 40.126.31.1, 40.126.31.143, 20.190.159.132, 20.190.159.134, 40.126.31.8, 40.126.31.135, 40.126.31.6, 51.104.139.180 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, www.tm.lg.prod.aadmsa.akadns.net, bn2eap.displaycatalog.md.mp.microsoft.com.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, skypedataprdcoleus15.cloudapp.net, emea1.notify.windows.com.akadns.net, login.live.com, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, cds.d2s7q6s2.hwcdn.net, www.tm.a.prd.aadg.akadns.net, login.msa.msidentity.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, par02p.wns.notify.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
13:00:09	API Interceptor	1409x Sleep call for process: PROOF OF PAYMENT.exe modified
13:00:17	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
13:00:28	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	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	• 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	• 79.134.225.73

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	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
	PO AR483-1590436 _ J-3000 PROJT.xlsx	Get hash	malicious	Browse	• 185.140.53.202
	Qotation.exe	Get hash	malicious	Browse	• 185.140.53.154
	PO - 2021-000511.exe	Get hash	malicious	Browse	• 185.244.30.69
	file.exe	Get hash	malicious	Browse	• 91.193.75.155
	Orden n.#U00ba 21115, pdf.exe	Get hash	malicious	Browse	• 185.140.53.129
	Lists.exe	Get hash	malicious	Browse	• 185.140.53.136
	Quotation Request.exe	Get hash	malicious	Browse	• 185.244.30.171
	PO-PDF_PDF.exe	Get hash	malicious	Browse	• 185.244.30.69
	Quiero hacer el pedido de su producto.exe	Get hash	malicious	Browse	• 185.244.30.18
	PO 047428.xlsx	Get hash	malicious	Browse	• 185.140.53.183
	SLIP.exe	Get hash	malicious	Browse	• 185.244.30.171
	2owa3HlP0V.exe	Get hash	malicious	Browse	• 185.140.53.183
	TAtAHTebr6.exe	Get hash	malicious	Browse	• 185.140.53.183
	Quotation.exe	Get hash	malicious	Browse	• 185.244.30.29

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Halkbank_Ekstre_20210118_162356_389771.exe	Get hash	malicious	Browse	• 91.193.75.189
	Urgent order 1812021-672 Q30721,pdf.exe	Get hash	malicious	Browse	• 185.140.53.131

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):	1018880
Entropy (8bit):	6.942682124565148
Encrypted:	false
SSDEEP:	12288:XqV5OpnI6faaeOd6/MTrklNE5b/wKB0dJ:k5OpnImys6/4kjE5bAJ
MD5:	57090F9293D9A013C7FF7FB614681A46
SHA1:	C477A883773DECABC0518173B640045802FAC0E8
SHA-256:	7F7AFB406C8F911F21354B2EA60FD688CE8083ED0AB10156C6F3421D927D2FAB
SHA-512:	398EC37B9927B59D8355D593BAE50289E2AC40529CB34B788D25D0FFA92F443218494C84B91B6A498A3940D78538F6B9A579E26242BF5F4C5CDB7A4A972D3D3A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....0.....:... .....@.. ..... ..@.....O..... ..... ..H.....text...@.... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....$.....k.....H.....".(.....*Vr...p.....r...p.....*..0..L.....}.....(.....(.....(.....s!.....("....o#.....($....o%.....(&... .*.0..K.....}.....('.....((.....,5...(.....s!.....(.....o#.....(.....o%....8.....r...p.d...()...o*...td.....(+.....9.....s.....s,..s-...o.....o/...(0.....o1...(2.....o3...(4.....o5...(6.....o7... (8.....o9...(:.....(;.....(.....+....s,...s-...(

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:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PROOF OF PAYMENT.exe.log	
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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\tmpB41.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):	1654
Entropy (8bit):	5.160770966789842
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB38tn:cbha7JlNQV/rydbz9I3YODOLNdq3Q
MD5:	C6367F6AFBFF748963C28C323A57DBB6
SHA1:	F12A2B73E3FE4048F7C3DDFA88475EA01F72ECB0
SHA-256:	44B4FFF536D6D4D1D8AAFFBBEEBA432505193B5DA48546AD2B8BEA6E91A6313C
SHA-512:	C539355185A6313EB8C1B804F68D11980F96DC70289DAF085A123D7A89D8CCC61A91B1B0E1EB728FE24F5C96B4129E96A7FDCBE4BD372BA99E540B982A98DEI D
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>.. <StartWhenAvail

C:\Users\user\AppData\Local\Temp\tmpC0F9.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):	1654
Entropy (8bit):	5.160770966789842
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB38tn:cbha7JlNQV/rydbz9I3YODOLNdq3Q
MD5:	C6367F6AFBFF748963C28C323A57DBB6
SHA1:	F12A2B73E3FE4048F7C3DDFA88475EA01F72ECB0
SHA-256:	44B4FFF536D6D4D1D8AAFFBBEEBA432505193B5DA48546AD2B8BEA6E91A6313C

C:\Users\user\AppData\Local\Temp\tmpC0F9.tmp	
SHA-512:	C539355185A6313EB8C1B804F68D11980F96DC70289DAF085A123D7A89D8CCC61A91B1B0E1EB728FE24F5C96B4129E96A7FDCBE4BD372BA99E540B982A98DE D
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>.. <StartWhenAvail

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\PROOF OF PAYMENT.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:aaOtn:aaC
MD5:	1A0740DC072472AB674A074D43DCE1AB
SHA1:	D9551A079277B57C5B32A3BD211D79792B5F8E83
SHA-256:	F0E68EE525ACE1BFDA5F6B5DD98529738CE5D40BB51709C7EBB2CA779387FD83
SHA-512:	3E0639D3159013E73D72DB6D65F63B8CCA7F1C3A2A8B2512FAFFFD15E226E3F923213341F4B8D1C26F96711ADFC48BCA7F3E9AE8BF58E8A1D64522459B8BC2E 0
Malicious:	**true**
Preview:	...8...H

C:\Users\user\AppData\Roaming\RbJJtmpPB.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):	1018880
Entropy (8bit):	6.942682124565148
Encrypted:	false
SSDEEP:	12288:XqV5OpnI6faaeOd6/MTrklNE5b/wKB0dJ:k5OpnImys6/4kjE5bAJ
MD5:	57090F9293D9A013C7FF7FB614681A46
SHA1:	C477A883773DECABC0518173B640045802FAC0E8
SHA-256:	7F7AFB406C8F911F21354B2EA60FD688CE8083ED0AB10156C6F3421D927D2FAB
SHA-512:	398EC37B9927B59D8355D593BAE50289E2AC40529CB34B788D25D0FFA92F443218494C84B91B6A498A3940D78538F6B9A579E26242BF5F4C5CDB7A4A972D3D3A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....0.....:.... .....@.. ..... ..@.....O..... ..... ..H.....text...@.... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....$.....k.....H.....".(.....*Vr...p.....r...p.....*..0..L.....}.....(..... (.....(.....s!.....("....o#.....($....o%.....(&... .*.0..K.....}.....('.....((.....,5...(.....s!.....(.....o#.....(.....o%....8.....r...p.d...()...o*...td.....(+.....9.....s.....s,...s-...o.....o/...(0.....o1...(2.....o3...(4.....o5...(6.....o7... (8.....o9...(:.....(;.....(.....+....s,...s-...(

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.942682124565148
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	PROOF OF PAYMENT.exe
File size:	1018880
MD5:	57090f9293d9a013c7ff7fb614681a46

General

SHA1:	c477a883773decabc0518173b640045802fac0e8
SHA256:	7f7afb406c8f911f21354b2ea60fd688ce8083ed0ab10156 c6f3421d927d2fab
SHA512:	398ec37b9927b59d8355d593bae50289e2ac40529cb34b 788d25d0ffa92f443218494c84b91b6a498a3940d78538f 6b9a579e26242bf5f4c5cdb7a4a972d3d3a
SSDEEP:	12288:XqV5OpnI6faaeOd6/MTrklNE5b/wKB0dJ:k5OpnI mys6/4kjE5bAJ
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.......PE..L..... .`..............0.............:.... ....@.. .... @................................

File Icon

	
Icon Hash:	926cd8b0b4d24f92

Static PE Info

General

Entrypoint:	0x4dee3a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60069D86 [Tue Jan 19 08:51:18 2021 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 [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xdede8	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe0000	0x1b788	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xfc000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xdce40	0xdd000	False	0.471612300269	data	7.10175200758	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xe0000	0x1b788	0x1b800	False	0.186869673295	data	3.43661210575	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xfc000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xe01a0	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0xe0618	0x2ad0	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xe30f8	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 3892081920, next used block 3187504384		
RT_ICON	0xe56b0	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4294866176, next used block 4294866176		
RT_ICON	0xe6768	0x10828	dBase III DBT, version number 0, next free block index 40		
RT_ICON	0xf6fa0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 670987520, next used block 0		
RT_GROUP_ICON	0xfb1d8	0x5a	data		
RT_VERSION	0xfb244	0x342	data		
RT_MANIFEST	0xfb598	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

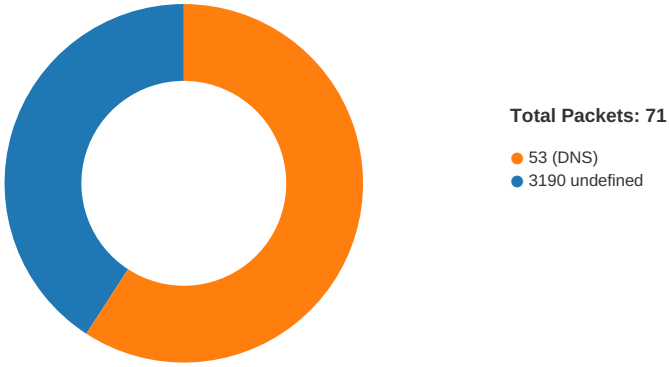
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Hewlett-Packard 2016
Assembly Version	46.3.0.0
InternalName	W.exe
FileVersion	46.3.0.0
CompanyName	Hewlett-Packard
LegalTrademarks	
Comments	
ProductName	
ProductVersion	46.3.0.0
FileDescription	
OriginalFilename	W.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 13:00:20.458858967 CET	49727	3190	192.168.2.6	185.140.53.131
Jan 19, 2021 13:00:23.468259096 CET	49727	3190	192.168.2.6	185.140.53.131
Jan 19, 2021 13:00:29.546869993 CET	49727	3190	192.168.2.6	185.140.53.131
Jan 19, 2021 13:00:37.774944067 CET	49731	3190	192.168.2.6	185.140.53.131
Jan 19, 2021 13:00:40.954102039 CET	49731	3190	192.168.2.6	185.140.53.131
Jan 19, 2021 13:00:46.954551935 CET	49731	3190	192.168.2.6	185.140.53.131
Jan 19, 2021 13:00:55.587681055 CET	49742	3190	192.168.2.6	185.140.53.131
Jan 19, 2021 13:00:58.596179962 CET	49742	3190	192.168.2.6	185.140.53.131
Jan 19, 2021 13:01:04.596689939 CET	49742	3190	192.168.2.6	185.140.53.131
Jan 19, 2021 13:01:13.558219910 CET	49751	3190	192.168.2.6	185.140.53.131
Jan 19, 2021 13:01:16.550934076 CET	49751	3190	192.168.2.6	185.140.53.131
Jan 19, 2021 13:01:22.551265001 CET	49751	3190	192.168.2.6	185.140.53.131
Jan 19, 2021 13:01:30.716780901 CET	49753	3190	192.168.2.6	185.140.53.131
Jan 19, 2021 13:01:33.724112034 CET	49753	3190	192.168.2.6	185.140.53.131
Jan 19, 2021 13:01:39.724651098 CET	49753	3190	192.168.2.6	185.140.53.131
Jan 19, 2021 13:01:48.705497980 CET	49758	3190	192.168.2.6	185.140.53.131
Jan 19, 2021 13:01:51.712265968 CET	49758	3190	192.168.2.6	185.140.53.131
Jan 19, 2021 13:01:57.726008892 CET	49758	3190	192.168.2.6	185.140.53.131

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 13:02:08.073179960 CET	49759	3190	192.168.2.6	185.140.53.131
Jan 19, 2021 13:02:11.086462975 CET	49759	3190	192.168.2.6	185.140.53.131
Jan 19, 2021 13:02:17.086971045 CET	49759	3190	192.168.2.6	185.140.53.131
Jan 19, 2021 13:02:25.276586056 CET	49760	3190	192.168.2.6	185.140.53.131
Jan 19, 2021 13:02:28.291044950 CET	49760	3190	192.168.2.6	185.140.53.131
Jan 19, 2021 13:02:34.291505098 CET	49760	3190	192.168.2.6	185.140.53.131
Jan 19, 2021 13:02:44.401058912 CET	49761	3190	192.168.2.6	185.140.53.131
Jan 19, 2021 13:02:47.432745934 CET	49761	3190	192.168.2.6	185.140.53.131
Jan 19, 2021 13:02:53.433733940 CET	49761	3190	192.168.2.6	185.140.53.131
Jan 19, 2021 13:03:01.088367939 CET	49762	3190	192.168.2.6	185.140.53.131
Jan 19, 2021 13:03:04.090867043 CET	49762	3190	192.168.2.6	185.140.53.131

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 12:59:55.805496931 CET	51774	53	192.168.2.6	8.8.8.8
Jan 19, 2021 12:59:55.853490114 CET	53	51774	8.8.8.8	192.168.2.6
Jan 19, 2021 12:59:56.807934046 CET	56023	53	192.168.2.6	8.8.8.8
Jan 19, 2021 12:59:56.864518881 CET	53	56023	8.8.8.8	192.168.2.6
Jan 19, 2021 12:59:57.750016928 CET	58384	53	192.168.2.6	8.8.8.8
Jan 19, 2021 12:59:57.798019886 CET	53	58384	8.8.8.8	192.168.2.6
Jan 19, 2021 12:59:58.920078039 CET	60261	53	192.168.2.6	8.8.8.8
Jan 19, 2021 12:59:58.967937946 CET	53	60261	8.8.8.8	192.168.2.6
Jan 19, 2021 12:59:59.899736881 CET	56061	53	192.168.2.6	8.8.8.8
Jan 19, 2021 12:59:59.947690010 CET	53	56061	8.8.8.8	192.168.2.6
Jan 19, 2021 13:00:00.908983946 CET	58336	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:00:00.959762096 CET	53	58336	8.8.8.8	192.168.2.6
Jan 19, 2021 13:00:01.726190090 CET	53781	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:00:01.774106979 CET	53	53781	8.8.8.8	192.168.2.6
Jan 19, 2021 13:00:02.676625013 CET	54064	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:00:02.727356911 CET	53	54064	8.8.8.8	192.168.2.6
Jan 19, 2021 13:00:03.732181072 CET	52811	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:00:03.782949924 CET	53	52811	8.8.8.8	192.168.2.6
Jan 19, 2021 13:00:05.037970066 CET	55299	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:00:05.094533920 CET	53	55299	8.8.8.8	192.168.2.6
Jan 19, 2021 13:00:05.990865946 CET	63745	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:00:06.041475058 CET	53	63745	8.8.8.8	192.168.2.6
Jan 19, 2021 13:00:06.870400906 CET	50055	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:00:06.918375015 CET	53	50055	8.8.8.8	192.168.2.6
Jan 19, 2021 13:00:08.621339083 CET	61374	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:00:08.672243118 CET	53	61374	8.8.8.8	192.168.2.6
Jan 19, 2021 13:00:20.191162109 CET	50339	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:00:20.418487072 CET	53	50339	8.8.8.8	192.168.2.6
Jan 19, 2021 13:00:24.397658110 CET	63307	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:00:24.445785046 CET	53	63307	8.8.8.8	192.168.2.6
Jan 19, 2021 13:00:31.901995897 CET	49694	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:00:31.965888023 CET	53	49694	8.8.8.8	192.168.2.6
Jan 19, 2021 13:00:37.717550993 CET	54982	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:00:37.773875952 CET	53	54982	8.8.8.8	192.168.2.6
Jan 19, 2021 13:00:44.926678896 CET	50010	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:00:44.975646019 CET	53	50010	8.8.8.8	192.168.2.6
Jan 19, 2021 13:00:46.890588999 CET	63718	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:00:46.941603899 CET	53	63718	8.8.8.8	192.168.2.6
Jan 19, 2021 13:00:48.181619883 CET	62116	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:00:48.241581917 CET	53	62116	8.8.8.8	192.168.2.6
Jan 19, 2021 13:00:49.147144079 CET	63816	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:00:49.206397057 CET	53	63816	8.8.8.8	192.168.2.6
Jan 19, 2021 13:00:49.908449888 CET	55014	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:00:49.975354910 CET	53	55014	8.8.8.8	192.168.2.6
Jan 19, 2021 13:00:50.204334974 CET	62208	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:00:50.263297081 CET	53	62208	8.8.8.8	192.168.2.6
Jan 19, 2021 13:00:51.036570072 CET	57574	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:00:51.092920065 CET	53	57574	8.8.8.8	192.168.2.6
Jan 19, 2021 13:00:51.918710947 CET	51818	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 19, 2021 13:00:51.977901936 CET	53	51818	8.8.8.8	192.168.2.6
Jan 19, 2021 13:00:52.906135082 CET	56628	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:00:52.967947006 CET	53	56628	8.8.8.8	192.168.2.6
Jan 19, 2021 13:00:54.188534975 CET	60778	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:00:54.237760067 CET	53	60778	8.8.8.8	192.168.2.6
Jan 19, 2021 13:00:55.359288931 CET	53799	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:00:55.585820913 CET	53	53799	8.8.8.8	192.168.2.6
Jan 19, 2021 13:00:56.010690928 CET	54683	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:00:56.067133904 CET	53	54683	8.8.8.8	192.168.2.6
Jan 19, 2021 13:00:56.214086056 CET	59329	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:00:56.271733999 CET	53	59329	8.8.8.8	192.168.2.6
Jan 19, 2021 13:00:57.452632904 CET	64021	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:00:57.509658098 CET	53	64021	8.8.8.8	192.168.2.6
Jan 19, 2021 13:00:58.588377953 CET	56129	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:00:58.644809961 CET	53	56129	8.8.8.8	192.168.2.6
Jan 19, 2021 13:01:13.499985933 CET	58177	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:01:13.556488991 CET	53	58177	8.8.8.8	192.168.2.6
Jan 19, 2021 13:01:30.495064020 CET	50700	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:01:30.714359999 CET	53	50700	8.8.8.8	192.168.2.6
Jan 19, 2021 13:01:32.905016899 CET	54069	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:01:32.965356112 CET	53	54069	8.8.8.8	192.168.2.6
Jan 19, 2021 13:01:41.057282925 CET	61178	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:01:41.116576910 CET	53	61178	8.8.8.8	192.168.2.6
Jan 19, 2021 13:01:41.876019955 CET	57017	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:01:41.924115896 CET	53	57017	8.8.8.8	192.168.2.6
Jan 19, 2021 13:01:48.640922070 CET	56327	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:01:48.701491117 CET	53	56327	8.8.8.8	192.168.2.6
Jan 19, 2021 13:02:08.015522957 CET	50243	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:02:08.071655989 CET	53	50243	8.8.8.8	192.168.2.6
Jan 19, 2021 13:02:25.218017101 CET	62055	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:02:25.274441004 CET	53	62055	8.8.8.8	192.168.2.6
Jan 19, 2021 13:02:44.175540924 CET	61249	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:02:44.397716045 CET	53	61249	8.8.8.8	192.168.2.6
Jan 19, 2021 13:03:01.029556036 CET	65252	53	192.168.2.6	8.8.8.8
Jan 19, 2021 13:03:01.087860107 CET	53	65252	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 19, 2021 13:00:20.191162109 CET	192.168.2.6	8.8.8.8	0x4d7a	Standard query (0)	amechi.duckdns.org	A (IP address)	IN (0x0001)
Jan 19, 2021 13:00:37.717550993 CET	192.168.2.6	8.8.8.8	0xe58b	Standard query (0)	amechi.duckdns.org	A (IP address)	IN (0x0001)
Jan 19, 2021 13:00:55.359288931 CET	192.168.2.6	8.8.8.8	0x8393	Standard query (0)	amechi.duckdns.org	A (IP address)	IN (0x0001)
Jan 19, 2021 13:01:13.499985933 CET	192.168.2.6	8.8.8.8	0x366a	Standard query (0)	amechi.duckdns.org	A (IP address)	IN (0x0001)
Jan 19, 2021 13:01:30.495064020 CET	192.168.2.6	8.8.8.8	0xb8e3	Standard query (0)	amechi.duckdns.org	A (IP address)	IN (0x0001)
Jan 19, 2021 13:01:48.640922070 CET	192.168.2.6	8.8.8.8	0x639d	Standard query (0)	amechi.duckdns.org	A (IP address)	IN (0x0001)
Jan 19, 2021 13:02:08.015522957 CET	192.168.2.6	8.8.8.8	0x3216	Standard query (0)	amechi.duckdns.org	A (IP address)	IN (0x0001)
Jan 19, 2021 13:02:25.218017101 CET	192.168.2.6	8.8.8.8	0xb61	Standard query (0)	amechi.duckdns.org	A (IP address)	IN (0x0001)
Jan 19, 2021 13:02:44.175540924 CET	192.168.2.6	8.8.8.8	0x3636	Standard query (0)	amechi.duckdns.org	A (IP address)	IN (0x0001)
Jan 19, 2021 13:03:01.029556036 CET	192.168.2.6	8.8.8.8	0x70b8	Standard query (0)	amechi.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

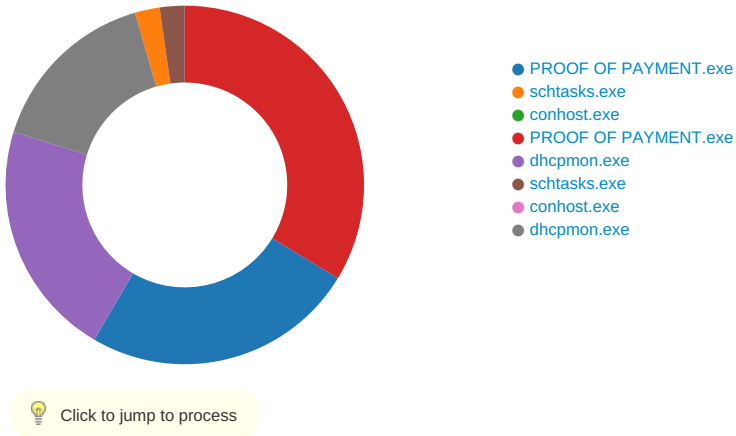
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 19, 2021 13:00:20.418487072 CET	8.8.8.8	192.168.2.6	0x4d7a	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 19, 2021 13:00:37.773875952 CET	8.8.8.8	192.168.2.6	0xe58b	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 19, 2021 13:00:55.585820913 CET	8.8.8.8	192.168.2.6	0x8393	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 19, 2021 13:01:13.556488991 CET	8.8.8.8	192.168.2.6	0x366a	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 19, 2021 13:01:30.714359999 CET	8.8.8.8	192.168.2.6	0xb8e3	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 19, 2021 13:01:41.116576910 CET	8.8.8.8	192.168.2.6	0xe7f9	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.akadns.net		CNAME (Canonical name)	IN (0x0001)
Jan 19, 2021 13:01:48.701491117 CET	8.8.8.8	192.168.2.6	0x639d	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 19, 2021 13:02:08.071655989 CET	8.8.8.8	192.168.2.6	0x3216	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 19, 2021 13:02:25.274441004 CET	8.8.8.8	192.168.2.6	0xb61	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 19, 2021 13:02:44.397716045 CET	8.8.8.8	192.168.2.6	0x3636	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)
Jan 19, 2021 13:03:01.087860107 CET	8.8.8.8	192.168.2.6	0x70b8	No error (0)	amechi.duckdns.org		185.140.53.131	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: PROOF OF PAYMENT.exe PID: 6396 Parent PID: 5892

General

Start time:	13:00:00
Start date:	19/01/2021
Path:	C:\Users\user\Desktop\PROOF OF PAYMENT.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PROOF OF PAYMENT.exe'
Imagebase:	0x880000
File size:	1018880 bytes
MD5 hash:	57090F9293D9A013C7FF7FB614681A46
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.364292242.0000000003FBF000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.364292242.0000000003FBF000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.364292242.0000000003FBF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.364005154.0000000003E49000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.364005154.0000000003E49000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.364005154.0000000003E49000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.357322278.0000000002EC6000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	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	6E0ACF06	unknown
C:\Users\user\AppData\Roaming\RbJJtmpPB.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CEF1E60	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpC0F9.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CEF7038	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	6E3BC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpC0F9.tmp	success or wait	1	6CEF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\RbJJtmpPB.exe	unknown	1018880	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 86 9d 06 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 d0 0d 00 00 ba 01 00 00 00 00 00 3a ee 0d 00 00 20 00 00 00 00 0e 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 e0 0f 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......`.......... ....0.............:.... ....@.. ....@.................	success or wait	1	6CEF1B4F	WriteFile
C:\Users\user\AppData\Local\Temp\tmpC0F9.tmp	unknown	1654	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 65 6e 67 69 6e 65 65 72 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	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </Registratio	success or wait	1	6CEF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E3BC907	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	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Users\user\Desktop\PROOF OF PAYMENT.exe	unknown	1018880	success or wait	1	6CEF1B4F	ReadFile

Analysis Process: schtasks.exe PID: 4712 Parent PID: 6396

General

Start time:	13:00:12
Start date:	19/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\RbJJtmpPB' /XML 'C:\Users\user\AppData\Local\Temp\tmpC0F9.tmp'
Imagebase:	0x930000
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\tmpC0F9.tmp	unknown	2	success or wait	1	93AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpC0F9.tmp	unknown	1655	success or wait	1	93ABD9	ReadFile

Analysis Process: conhost.exe PID: 6252 Parent PID: 4712

General

Start time:	13:00:12
Start date:	19/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: PROOF OF PAYMENT.exe PID: 4540 Parent PID: 6396

General

Start time:	13:00:13
Start date:	19/01/2021
Path:	C:\Users\user\Desktop\PROOF OF PAYMENT.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x920000
File size:	1018880 bytes
MD5 hash:	57090F9293D9A013C7FF7FB614681A46
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.716409354.0000000005F00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.716409354.0000000005F00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.716409354.0000000005F00000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.716279193.0000000005830000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.716279193.0000000005830000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.710137249.0000000002E11000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.706369637.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.706369637.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.706369637.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.713378603.0000000003E4A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.713378603.0000000003E4A000.00000004.00000001.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	6E0ACF06	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	6E0ACF06	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	6CEFBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CEF1E60	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	6CEFBEFF	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	6CEFDD66	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	6CEFDD66	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6CEFBEFF	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	6CEFBEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PROOF OF PAYMENT.exe:Zone.Identifier	success or wait	1	6CE72935	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	01 b6 ff 38 bd bc d8 48	...8...H	success or wait	1	6CEF1B4F	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 86 9d 06 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 d0 0d 00 00 ba 01 00 00 00 00 00 3a ee 0d 00 00 20 00 00 00 00 0e 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 e0 0f 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......`.......... ....0.............:..... ....@.. ....@................	success or wait	4	6CEFDD66	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CEFDD66	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	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6E06D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6E06D72F	unknown
C:\Users\user\Desktop\PROOF OF PAYMENT.exe	unknown	4096	success or wait	1	6E06D72F	unknown
C:\Users\user\Desktop\PROOF OF PAYMENT.exe	unknown	512	success or wait	1	6E06D72F	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	6CEF646A	RegSetValueExW

Analysis Process: dhcpmon.exe PID: 6868 Parent PID: 3440

General

Start time:	13:00:26
Start date:	19/01/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xc10000
File size:	1018880 bytes
MD5 hash:	57090F9293D9A013C7FF7FB614681A46
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: 00000007.00000002.404349364.000000000419F000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.404349364.000000000419F000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.404349364.000000000419F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000007.00000002.403470150.00000000030A6000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6E0ACF06	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	6E0ACF06	unknown
C:\Users\user\AppData\Local\Temp\tmpB41.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CEF7038	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	6E3BC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpB41.tmp	success or wait	1	6CEF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpB41.tmp	unknown	1654	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 65 6e 67 69 6e 65 65 72 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	<?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>.. </Registratio	success or wait	1	6CEF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	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 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E3BC907	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	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile

Analysis Process: schtasks.exe PID: 7048 Parent PID: 6868

General

Start time:	13:00:31
Start date:	19/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\RbJJtmpPB' /XML 'C:\Users\user\AppData\Local\Temp\tmpB41.tmp'
Imagebase:	0x930000
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\tmpB41.tmp	unknown	2	success or wait	1	93AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpB41.tmp	unknown	1655	success or wait	1	93ABD9	ReadFile

Analysis Process: conhost.exe PID: 6952 Parent PID: 7048

General

Start time:	13:00:32
Start date:	19/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 6796 Parent PID: 6868

General

Start time:	13:00:33
Start date:	19/01/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xb40000
File size:	1018880 bytes
MD5 hash:	57090F9293D9A013C7FF7FB614681A46
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: 0000000B.00000002.416463226.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.416463226.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.416463226.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.418085053.0000000002F41000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.418085053.0000000002F41000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.418172375.0000000003F49000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.418172375.0000000003F49000.00000004.00000001.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	6E0ACF06	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	6E0ACF06	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	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile

Disassembly

Code Analysis