ID: 551433
Sample Name: Payment confirmation .exe
Cookbook: default.jbs
Time: 08:24:50
Date: 12/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

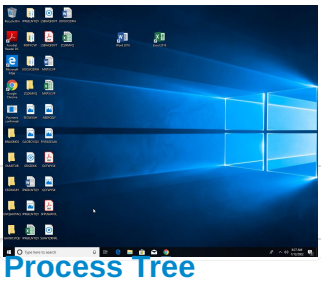
Windows Analysis Report Payment confirmation .exe

Overview

General Information

Sample Name:	Payment confirmation .exe
Analysis ID:	551433
MD5:	aa035026516778..
SHA1:	efae7e259b45818.
SHA256:	39c5635ea42d63..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

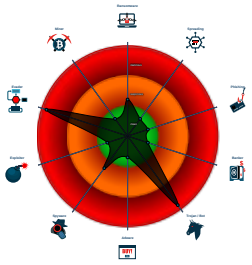
Nanocore

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Antivirus detection for URL or domain
- Yara detected Nanocore RAT
- Initial sample is a PE file and has a …
- Connects to many ports of the same…
- Tries to detect sandboxes and other…
- Sigma detected: Suspicius Add Tas…
- Machine Learning detection for samp…

Classification



Process Tree

- **System is w10x64**
- Payment confirmation .exe (PID: 6996 cmdline: "C:\Users\user\Desktop\Payment confirmation .exe" MD5: AA035026516778019F8B8BD0E224FC03)
  - powershell.exe (PID: 3604 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\QNRaul.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 3600 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 3116 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\QNRaul" /XML "C:\Users\user\AppData\Local\Temp\tmpEEA4.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5036 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Payment confirmation .exe (PID: 5432 cmdline: C:\Users\user\Desktop\Payment confirmation .exe MD5: AA035026516778019F8B8BD0E224FC03)
  - Payment confirmation .exe (PID: 5520 cmdline: C:\Users\user\Desktop\Payment confirmation .exe MD5: AA035026516778019F8B8BD0E224FC03)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "2616a878-9933-42e4-9fe0-3b57e29b",
  "Domain1": "naki.airdns.org",
  "Domain2": "37.120.210.211",
  "Port": 56281,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "faff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.938485517.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000A.00000002.938485517.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000A.00000002.938485517.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
0000000A.00000002.943461917.00000000052E0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
0000000A.00000002.943461917.00000000052E0000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost

Click to see the 32 entries

Unpacked PEs

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
0.2.Payment confirmation .exe.363c208.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x5a9ad:$x1: NanoCore.ClientPluginHost • 0xa4fcd:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x5a9ea:$x2: IClientNetworkHost • 0xa500a:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x5e51d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0xa8b3d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.Payment confirmation .exe.363c208.3.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.Payment confirmation .exe.363c208.3.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0x5a715:$a: NanoCore • 0x5a725:$a: NanoCore • 0x5a959:$a: NanoCore • 0x5a96d:$a: NanoCore • 0x5a9ad:$a: NanoCore • 0xa4d35:$a: NanoCore • 0xa4d45:$a: NanoCore • 0xa4f79:$a: NanoCore • 0xa4f8d:$a: NanoCore • 0xa4fcd:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x5a774:$b: ClientPlugin • 0x5a976:$b: ClientPlugin • 0x5a9b6:$b: ClientPlugin
10.2.Payment confirmation .exe.3a22a86.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0x145e3:$x1: NanoCore.ClientPluginHost • 0x3c845:$x1: NanoCore.ClientPluginHost • 0x556df:$x1: NanoCore.ClientPluginHost • 0x7d92d:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost • 0x14610:$x2: IClientNetworkHost • 0x3c85f:$x2: IClientNetworkHost • 0x5570c:$x2: IClientNetworkHost • 0x7d947:$x2: IClientNetworkHost
10.2.Payment confirmation .exe.3a22a86.5.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x145e3:$x2: NanoCore.ClientPluginHost • 0x3c845:$x2: NanoCore.ClientPluginHost • 0x556df:$x2: NanoCore.ClientPluginHost • 0x7d92d:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0x156be:$s4: PipeCreated • 0x3fb82:$s4: PipeCreated • 0x567ba:$s4: PipeCreated • 0x80c6a:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost • 0x145fd:$s5: IClientLoggingHost • 0x3c832:$s5: IClientLoggingHost • 0x556f9:$s5: IClientLoggingHost • 0x7d91a:$s5: IClientLoggingHost
Click to see the 69 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Antivirus detection for URL or domain

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:

Connects to many ports of the same IP (likely port scanning)

C2 URLs / IPs found in malware configuration

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

.NET source code contains method to dynamically call methods (often used by packers)

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 AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

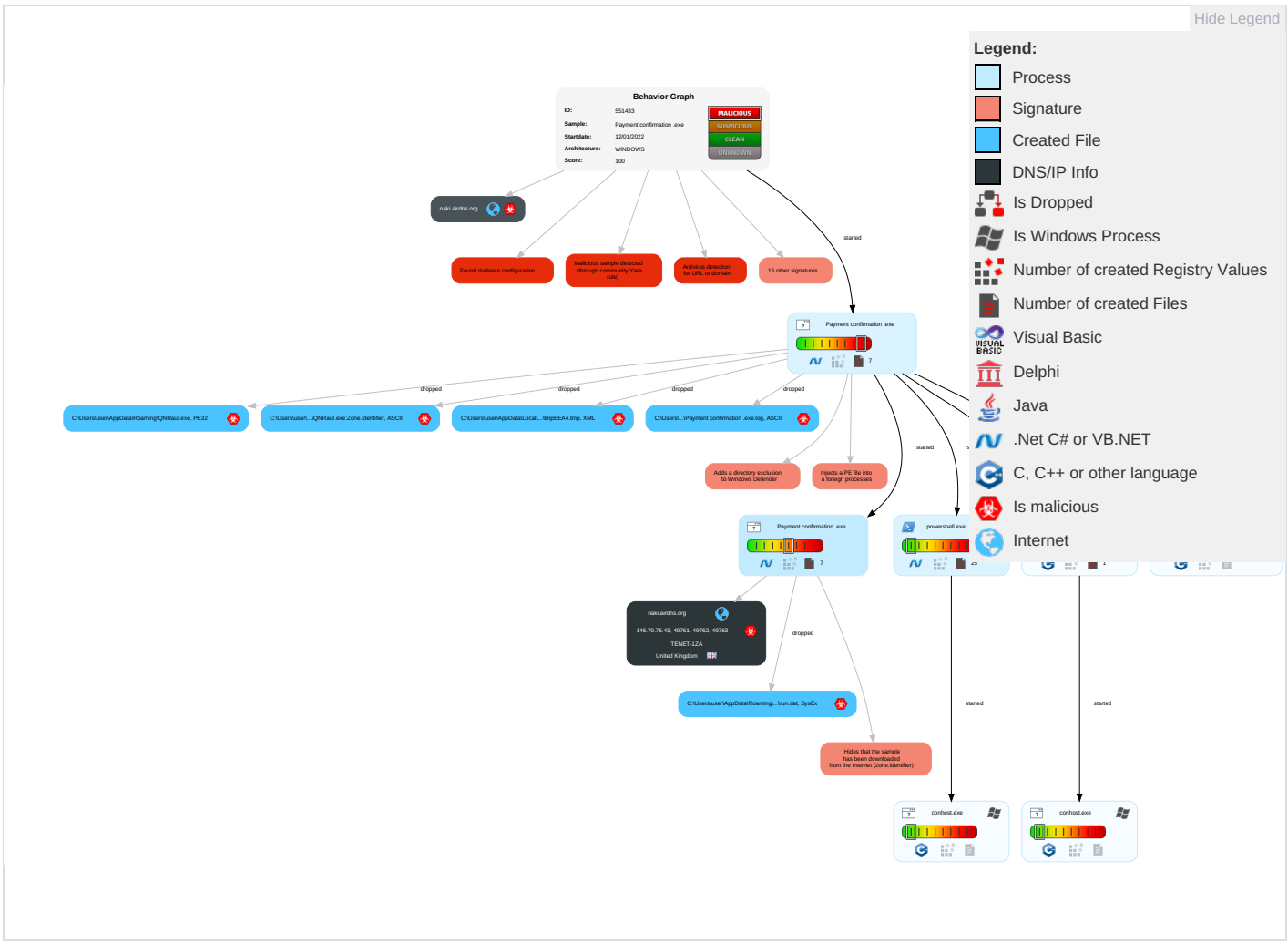
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1	Input Capture 1 1	Security Software Discovery 1 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM C 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 1 1	Manip Device Comm
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	Jamm Denial Servic
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 Acces
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	Down Insecu Protoc

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
Payment confirmation .exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\QNRaul.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.Payment confirmation .exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.2.Payment confirmation .exe.52e0000.7.unpack	100%	Avira	TR/NanoCore.fadte		Download File
10.0.Payment confirmation .exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.0.Payment confirmation .exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.0.Payment confirmation .exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.0.Payment confirmation .exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
10.0.Payment confirmation .exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/jp/C	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
37.120.210.211	100%	Avira URL Cloud	malware	
naki.airdns.org	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/;	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/pt-b	0%	Avira URL Cloud	safe	
http://www.monotype.p	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/)	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.carterandcone.comM	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.commfet	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/O	0%	URL Reputation	safe	
http://www.tiro.como	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/L	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/C	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/;	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/y	0%	URL Reputation	safe	
http://www.sakkal.com.	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/z	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/t	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0/	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/)	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/p	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.carterandcone.comwit	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/~Rm	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
naki.airdns.org	146.70.76.43	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
37.120.210.211	true	• Avira URL Cloud: malware	unknown
naki.airdns.org	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
146.70.76.43	naki.airdns.org	United Kingdom		2018	TENET-1ZA	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	551433
Start date:	12.01.2022
Start time:	08:24:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Payment confirmation .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:	22
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@11/10@14/1
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 34.8% (good quality ratio 17.4%) • Quality average: 37.2% • Quality standard deviation: 38%
HCA Information:	• Successful, ratio: 99% • 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

Simulations

Behavior and APIs

Time	Type	Description
08:26:02	API Interceptor	831x Sleep call for process: Payment confirmation .exe modified
08:26:12	API Interceptor	44x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Payment confirmation .exe.log	
Process:	C:\Users\user\Desktop\Payment confirmation .exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x847mE4P:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzQ
MD5:	A9EFF9253CAF99EC8665E41D736DDAED
SHA1:	D95BB4ABC856D774DA4602A59DE252B4BF560530
SHA-256:	DBC637B33F1F3CD1AB40AFED23F94C4571CA43621EBB52C5DC267DBDC52D4783
SHA-512:	96B67A84B750589BDB758224641065919F34BBF02BB286B9F5D566B48965A0E38FB88308B61351A6E11C46B76BFEC370FBC8B978A9F0F07A847567172D5CA5F3
Malicious:	**true**
Reputation:	moderate, 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\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22280
Entropy (8bit):	5.603448558149079
Encrypted:	false
SSDEEP:	384:GtCDm0k8v6v30rXSJScSBKnYjultIab7Y9gtbSJ3xyT1MaDZlbAV7O4l6ZBDI+ip:eQ23MXE4KYClt17hcwC6fwoVg
MD5:	438CEF22F7B9AB115F27C9E03ED52A92
SHA1:	3E50A0EF10FB3EE05A1772B685114078755E461C
SHA-256:	4DDC221F1F2DA6CD48D3117C60008429D9F2631F0BF7C5DF8927989ECBB05CCC
SHA-512:	BB186A39B67EA9D43ED556451FCE481451C5A8F995867FC84CD7D1815D1D5A6BB1323710979FF0CF0378E2C5439318E3ED42CEBEA7212213AA293BC2763DFA0
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Preview:	@...e.....y.....h.....y...l.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_2qnk0ivh.iyj.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mevy52tz.tt5.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmpEEA4.tmp	
Process:	C:\Users\user\Desktop\Payment confirmation .exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1593
Entropy (8bit):	5.1360806454884385
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtadxvn:cgeKwYrFdOFzOzN33ODOiDdKrsuT+v
MD5:	B0A91C23E82AA9831131A946DC8882B2
SHA1:	6ACB72396925F2655F17259CB41980C1E77B5BBB
SHA-256:	830508EBB4A30C675781AA7A61A4A3B41379B090CC472B86368AA906849E39B8
SHA-512:	3B0104905227E5357708DE138902E7FD99DD89145A829B1EFC5878097A3DC49CCF0E0162629D019E30B39DA89D5E1050553A7F749A9B29AC47D899B9DAC44158
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserI d>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>. <Sto pIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\Payment confirmation .exe
File Type:	data
Category:	dropped
Size (bytes):	232

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C356A5
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\Payment confirmation .exe
File Type:	SysEx File - Twister
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:p2Bn:e
MD5:	6D4C80C6B89E030207C12FF4661B6118
SHA1:	7401D0D745A13BD2905E25C23E65421C382391A9
SHA-256:	EBABE9E7478812E1D324E5F7D94EFA80B73BAB3E1A3CFC9E155047BC3858344F
SHA-512:	812A64696E0931C6B19AA555B24F21003D58758276ACE42F45F9A58BFEFD67FD3AA2089B2F17285D6D498507E8B2411BEB11D9B93490F849ABC8225A911A6741
Malicious:	**true**
Preview:	.%7...H

C:\Users\user\AppData\Roaming\QNRaul.exe	
Process:	C:\Users\user\Desktop\Payment confirmation .exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	542720
Entropy (8bit):	7.954488841460159
Encrypted:	false
SSDEEP:	12288:bXGyj7pcvY2GblmQ1S3IAHQ7RBw/73iErP:fTc3bwNBwuEr
MD5:	AA035026516778019F8B8BD0E224FC03
SHA1:	EFAE7E259B4581830C7E6BFEB94ED6DD25A54229
SHA-256:	39C5635EA42D63FE84500B9760FBE56E0FD32430077007496 09BCA1CD8D9E5D4
SHA-512:	A2CBCE6A6597479167089339504B7BC39BAE9845F2295397062F2FFE1B79037A5640208663A5E208D87856CEEADD1EFE061B933ED69A79D572BD597F3FF75899
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....v.a.....0..<.....NZ... ...`....@.. .....@..Y..O...`..... ....H.....text...T:... ...<..... ..`.rsrc.....`.....>.....@..@.rel oc.....F.....@..B.....0Z.....H.....L...\.....6...|.....&.(.....**..(.....*....0.....r...pr...p.QsF....+..*..0.....r;..prA..p.EsF....+..*..0 .....rw..pr...p.VsF....+..*..0.....r...pr...p.JsF....+..*..0.....r...pr...p.ZsF....+..*..0.....r+..pr1..p.Z.MsG....+..*....0.....rg..pro..p.Z.MsG....+..*....0.....r...pr...p. Z.MsG....+..*....0.....r...pr...ps=....+..*....0.....r...pr#..ps=....+..*....0.....

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

C:\Users\user\Documents\20220112\PowerShell_transcript.830021.GhMaXGHf.20220112082610.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5773
Entropy (8bit):	5.39117162081354
Encrypted:	false
SSDEEP:	96:BZIjKNxqDo1ZSZNjKNxqDo1ZxrpzjZ/jKNxqDo1Zbajj5Zh:x
MD5:	322C10DE7FC412A3E88EABCEB5DD0130
SHA1:	51593CE60CD26DD9EF22B0784C44CB381CE5D4A8
SHA-256:	43AD0D4351316231CFCB26AC59E6F01839779EEFF38D961A10D251ACE4172D9B
SHA-512:	5BECB37FE14E9735811D84CD391891E276FE903A0CCD0D42D3782AEE792A06F01B9A37A72FDC207F331CADB7894CF933CE35F579AED2A73B55AFB78B0A052B3
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220112082611..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 830021 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\QNRaul.exe..Process ID: 3604..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220112082611..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\QNRaul.exe..**********..Windows PowerShell transcript start..Start time: 20220112083015..Username: computer\user..RunAs User: computer\user..Confi

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.954488841460159
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:	Payment confirmation .exe
File size:	542720
MD5:	aa035026516778019f8b8bd0e224fc03
SHA1:	efae7e259b4581830c7e6bfeb94ed6dd25a54229
SHA256:	39c5635ea42d63fe84500b9760fbe56e0fd3243007700749609bca1cd8d9e5d4
SHA512:	a2cbce6a659747916708933950 4b7bc39bae9845f2295397062f2ffe1b79037a5640208663a5e208d87856ceeadd1efe061b933ed69a79d572bd597f3ff75899
SSDEEP:	12288:bXGyj7pcvY2GblmQ1S3IAHQ7RBw/73iErP:fTc3bwNBwuEr
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....v.a.....0..<.....NZ... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x485a4e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui

General

Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61DE7680 [Wed Jan 12 06:34:40 2022 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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x83a54	0x83c00	False	0.961252520161	data	7.96359768292	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x86000	0x6d4	0x800	False	0.37109375	data	3.68471441086	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x88000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 12, 2022 08:26:21.358510017 CET	192.168.2.4	8.8.8.8	0xa905	Standard query (0)	naki.airdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 08:26:28.396239996 CET	192.168.2.4	8.8.8.8	0x5745	Standard query (0)	naki.airdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 08:26:36.512564898 CET	192.168.2.4	8.8.8.8	0xf50	Standard query (0)	naki.airdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 08:26:44.168963909 CET	192.168.2.4	8.8.8.8	0x6bab	Standard query (0)	naki.airdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 08:26:51.997921944 CET	192.168.2.4	8.8.8.8	0xf097	Standard query (0)	naki.airdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 08:26:59.029360056 CET	192.168.2.4	8.8.8.8	0x5e15	Standard query (0)	naki.airdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 08:27:05.947813034 CET	192.168.2.4	8.8.8.8	0x7c75	Standard query (0)	naki.airdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 08:27:13.125575066 CET	192.168.2.4	8.8.8.8	0xb2df	Standard query (0)	naki.airdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 12, 2022 08:27:20.194072008 CET	192.168.2.4	8.8.8.8	0x37d	Standard query (0)	naki.airdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 08:27:27.167675972 CET	192.168.2.4	8.8.8.8	0x4dd2	Standard query (0)	naki.airdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 08:27:35.424280882 CET	192.168.2.4	8.8.8.8	0x70e1	Standard query (0)	naki.airdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 08:27:43.627265930 CET	192.168.2.4	8.8.8.8	0x150b	Standard query (0)	naki.airdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 08:27:50.791979074 CET	192.168.2.4	8.8.8.8	0xa18a	Standard query (0)	naki.airdns.org	A (IP address)	IN (0x0001)
Jan 12, 2022 08:27:58.324325085 CET	192.168.2.4	8.8.8.8	0xf965	Standard query (0)	naki.airdns.org	A (IP address)	IN (0x0001)

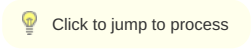
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 12, 2022 08:26:21.463951111 CET	8.8.8.8	192.168.2.4	0xa905	No error (0)	naki.airdns.org		146.70.76.43	A (IP address)	IN (0x0001)
Jan 12, 2022 08:26:28.600332975 CET	8.8.8.8	192.168.2.4	0x5745	No error (0)	naki.airdns.org		146.70.76.43	A (IP address)	IN (0x0001)
Jan 12, 2022 08:26:36.701642990 CET	8.8.8.8	192.168.2.4	0xf50	No error (0)	naki.airdns.org		146.70.76.43	A (IP address)	IN (0x0001)
Jan 12, 2022 08:26:44.187479019 CET	8.8.8.8	192.168.2.4	0x6bab	No error (0)	naki.airdns.org		146.70.76.43	A (IP address)	IN (0x0001)
Jan 12, 2022 08:26:52.014723063 CET	8.8.8.8	192.168.2.4	0xf097	No error (0)	naki.airdns.org		146.70.76.43	A (IP address)	IN (0x0001)
Jan 12, 2022 08:26:59.048402071 CET	8.8.8.8	192.168.2.4	0x5e15	No error (0)	naki.airdns.org		146.70.76.43	A (IP address)	IN (0x0001)
Jan 12, 2022 08:27:05.964391947 CET	8.8.8.8	192.168.2.4	0x7c75	No error (0)	naki.airdns.org		146.70.76.43	A (IP address)	IN (0x0001)
Jan 12, 2022 08:27:13.144364119 CET	8.8.8.8	192.168.2.4	0xb2df	No error (0)	naki.airdns.org		146.70.76.43	A (IP address)	IN (0x0001)
Jan 12, 2022 08:27:20.212605953 CET	8.8.8.8	192.168.2.4	0x37d	No error (0)	naki.airdns.org		146.70.76.43	A (IP address)	IN (0x0001)
Jan 12, 2022 08:27:27.183885098 CET	8.8.8.8	192.168.2.4	0x4dd2	No error (0)	naki.airdns.org		146.70.76.43	A (IP address)	IN (0x0001)
Jan 12, 2022 08:27:35.440875053 CET	8.8.8.8	192.168.2.4	0x70e1	No error (0)	naki.airdns.org		146.70.76.43	A (IP address)	IN (0x0001)
Jan 12, 2022 08:27:43.646083117 CET	8.8.8.8	192.168.2.4	0x150b	No error (0)	naki.airdns.org		146.70.76.43	A (IP address)	IN (0x0001)
Jan 12, 2022 08:27:50.810436010 CET	8.8.8.8	192.168.2.4	0xa18a	No error (0)	naki.airdns.org		146.70.76.43	A (IP address)	IN (0x0001)
Jan 12, 2022 08:27:58.343009949 CET	8.8.8.8	192.168.2.4	0xf965	No error (0)	naki.airdns.org		146.70.76.43	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Payment confirmation .exe PID: 6996 Parent PID: 1088

General

Start time:	08:25:51
Start date:	12/01/2022
Path:	C:\Users\user\Desktop\Payment confirmation .exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Payment confirmation .exe"
Imagebase:	0x80000
File size:	542720 bytes
MD5 hash:	AA035026516778019F8B8BD0E224FC03
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.730307873.0000000002611000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.730520964.00000000034AE000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.730520964.00000000034AE000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.730520964.00000000034AE000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.729736514.0000000002401000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 3604 Parent PID: 6996

General

Start time:	08:26:09
Start date:	12/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\QNRaul.exe
Imagebase:	0x1210000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities — Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 3600 Parent PID: 3604

General

Start time:	08:26:09
Start date:	12/01/2022
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: schtasks.exe PID: 3116 Parent PID: 6996

General

Start time:	08:26:10
Start date:	12/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\QNRaul" /XML "C:\Users\user\AppData\Local\Temp\tmpEEA4.tmp
Imagebase:	0x1060000
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 — Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 5036 Parent PID: 3116

General

Start time:	08:26:12
Start date:	12/01/2022
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: Payment confirmation .exe PID: 5432 Parent PID: 6996

General

Start time:	08:26:13
Start date:	12/01/2022
Path:	C:\Users\user\Desktop\Payment confirmation .exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Payment confirmation .exe
Imagebase:	0xc0000
File size:	542720 bytes
MD5 hash:	AA035026516778019F8B8BD0E224FC03
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Payment confirmation .exe PID: 5520 Parent PID: 6996

General

Start time:	08:26:14
Start date:	12/01/2022
Path:	C:\Users\user\Desktop\Payment confirmation .exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Payment confirmation .exe
Imagebase:	0x6a0000
File size:	542720 bytes
MD5 hash:	AA035026516778019F8B8BD0E224FC03
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.938485517.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.938485517.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.938485517.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.943461917.00000000052E0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.943461917.00000000052E0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.943461917.00000000052E0000.00000004.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.726108630.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.726108630.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.726108630.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.939719570.0000000002991000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.725697344.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.725697344.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.725697344.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.726654593.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.726654593.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.726654593.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.944294212.00000000062B0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.944294212.00000000062B0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.941482368.0000000003A19000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.941482368.0000000003A19000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000000.724292610.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000000.724292610.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000000.724292610.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.943393198.00000000052D0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.943393198.00000000052D0000.00000004.00020000.sdmp, Author: Florian Roth
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis