ID: 358327
Sample Name: RFQ.exe
Cookbook: default.jbs
Time: 12:15:39
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

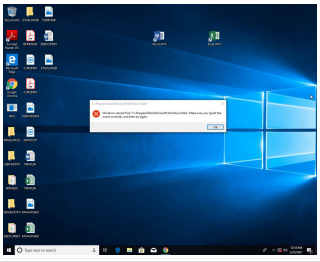
Analysis Report RFQ.exe

Overview

General Information

Sample Name:	RFQ.exe
Analysis ID:	358327
MD5:	6733e06c6be5ca..
SHA1:	9412d3147b30a8..
SHA256:	72f30e8884110e0.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

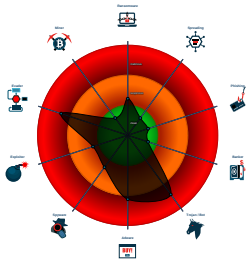
Nanocore

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

Signatures

- Detected Nanocore Rat
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- .NET source code contains very larg…
- Drops PE files to the startup folder
- Hides that the sample has been dow…
- Contains capabilities to detect virtua…
- Contains long sleeps (>= 3 min)
- Creates a DirectInput object (often fo…
- Creates a process in suspended mo…
- Creates a start menu entry (Start Me…

Classification



Startup

- **System is w10x64**
- RFQ.exe (PID: 6876 cmdline: 'C:\Users\user\Desktop\RFQ.exe' MD5: 6733E06C6BE5CA14FFC33763202F53C8)
  - cmd.exe (PID: 6032 cmdline: 'cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'audiomac' /t REG_SZ /d 'C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\july\enrnus.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 1428 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - reg.exe (PID: 6188 cmdline: REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'audiomac' /t REG_SZ /d 'C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\july\enrnus.exe' MD5: CEE2A7E57DF2A159A065A34913A055C2)
  - enrnus.exe (PID: 2288 cmdline: 'C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\july\enrnus.exe' MD5: 6733E06C6BE5CA14FFC33763202F53C8)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.476175749.000000000488C000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x10b97:$x1: NanoCore.ClientPluginHost • 0x43755:$x1: NanoCore.ClientPluginHost • 0x10bd4:$x2: IClientNetworkHost • 0x43792:$x2: IClientNetworkHost • 0x14707:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x472c5:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.476175749.000000000488C000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.476175749.000000000488C000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x108ff:$a: NanoCore • 0x1090f:$a: NanoCore • 0x10b43:$a: NanoCore • 0x10b57:$a: NanoCore • 0x10b97:$a: NanoCore • 0x434bd:$a: NanoCore • 0x434cd:$a: NanoCore • 0x43701:$a: NanoCore • 0x43715:$a: NanoCore • 0x43755:$a: NanoCore • 0x1095e:$b: ClientPlugin • 0x10b60:$b: ClientPlugin • 0x10ba0:$b: ClientPlugin • 0x4351c:$b: ClientPlugin • 0x4371e:$b: ClientPlugin • 0x4375e:$b: ClientPlugin • 0x10a85:$c: ProjectData • 0x43643:$c: ProjectData • 0x1148c:$d: DESCrypto • 0x4404a:$d: DESCrypto • 0x18e58:$e: KeepAlive
00000000.00000002.475624148.000000000478E000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x43ca7:$x1: NanoCore.ClientPluginHost • 0x76877:$x1: NanoCore.ClientPluginHost • 0xa9437:$x1: NanoCore.ClientPluginHost • 0x43ce4:$x2: IClientNetworkHost • 0x768b4:$x2: IClientNetworkHost • 0xa9474:$x2: IClientNetworkHost • 0x47817:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x7a3e7:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0xacfa7:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.475624148.000000000478E000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 14 entries				

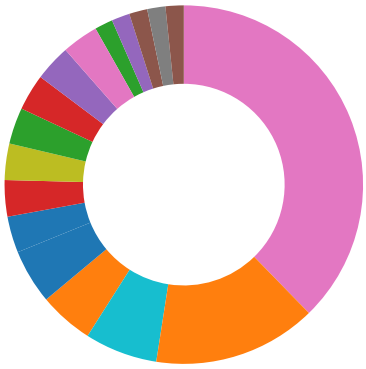
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.RFQ.exe.48272aa.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.RFQ.exe.48272aa.4.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
0.2.RFQ.exe.48272aa.4.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.RFQ.exe.48272aa.4.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xe0f5:$a: NanoCore • 0xe105:$a: NanoCore • 0xe339:$a: NanoCore • 0xe34d:$a: NanoCore • 0xe38d:$a: NanoCore • 0xe154:$b: ClientPlugin • 0xe356:$b: ClientPlugin • 0xe396:$b: ClientPlugin • 0xe27b:$c: ProjectData • 0xec82:$d: DESCrypto • 0x1664e:$e: KeepAlive • 0x1463c:$g: LogClientMessage • 0x10837:$i: get_Connected • 0xefb8:$j: #=q • 0xefe8:$j: #=q • 0xf004:$j: #=q • 0xf034:$j: #=q • 0xf050:$j: #=q • 0xf06c:$j: #=q • 0xf09c:$j: #=q • 0xf0b8:$j: #=q
0.2.RFQ.exe.48bf5c8.7.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 72 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Compliance:

Uses 32bit PE files

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

Binary contains paths to debug symbols

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Boot Survival:

Drops PE files to the startup folder

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

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

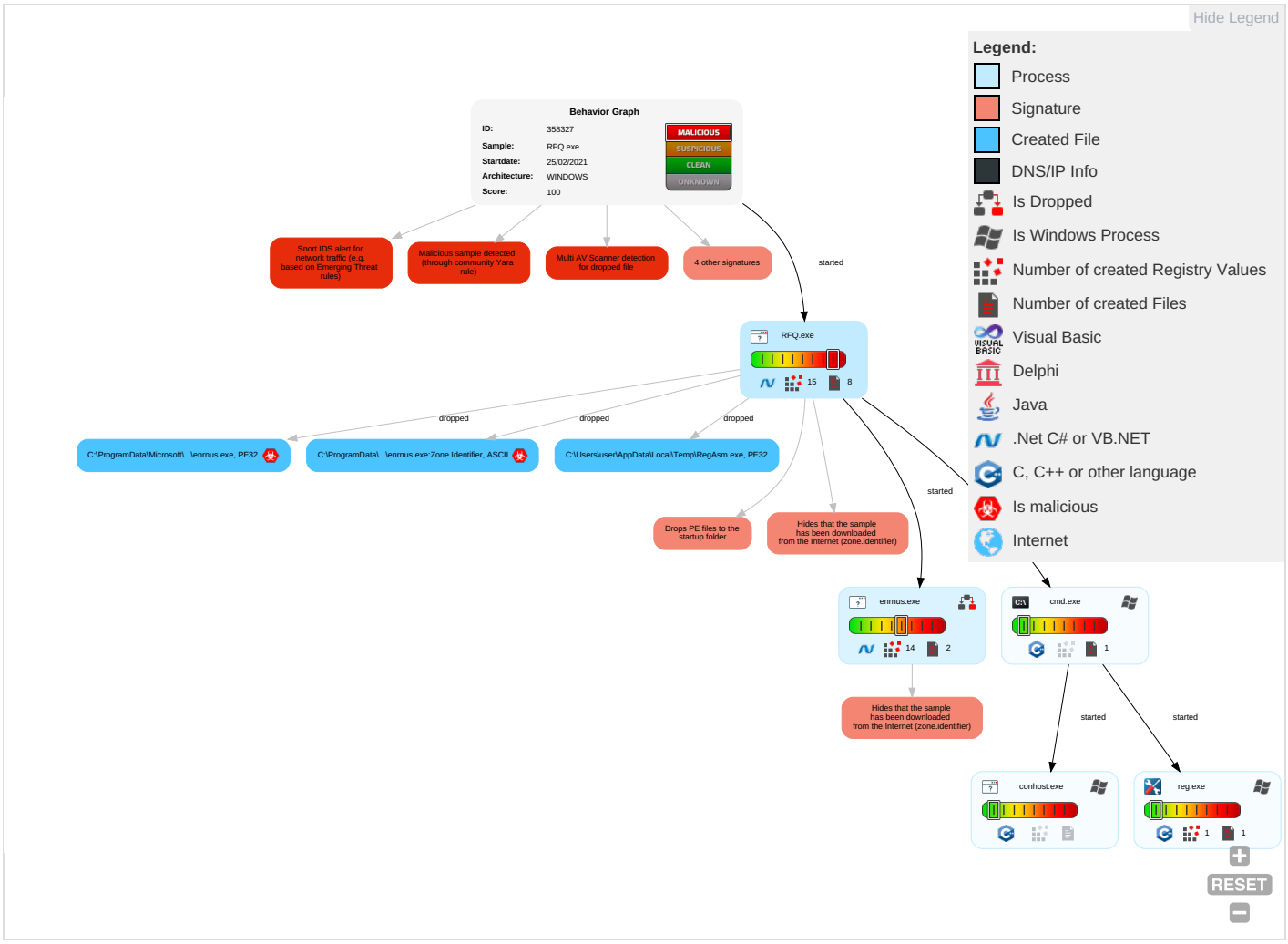
Detected Nanocore Rat

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	Networ Effects
Valid Accounts	Windows Management Instrumentation	Startup Items 1	Startup Items 1	Masquerading 1	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesd Insecur Networl Commu
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 1 2 1	Process Injection 1 2	Modify Registry 1	LSASS Memory	Security Software Discovery 1 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Remote Access Software 1	Exploit Redirec Calls/SI
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1 2 1	Virtualization/Sandbox Evasion 3	Security Account Manager	Virtualization/Sandbox Evasion 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Disable or Modify Tools 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 2	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammir Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecur Protoco

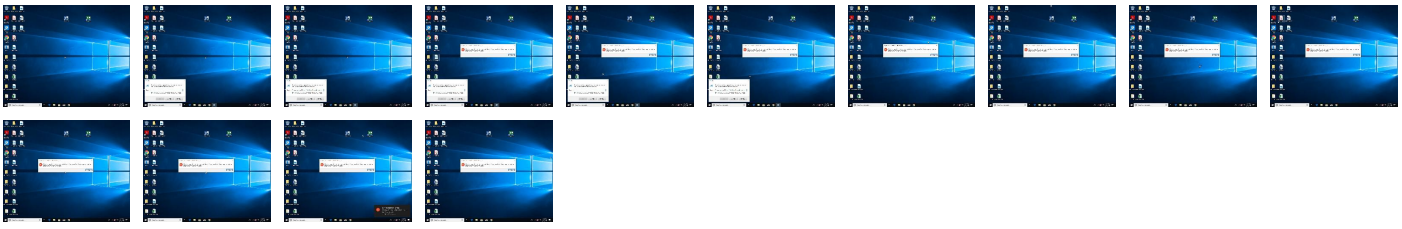
Behavior Graph

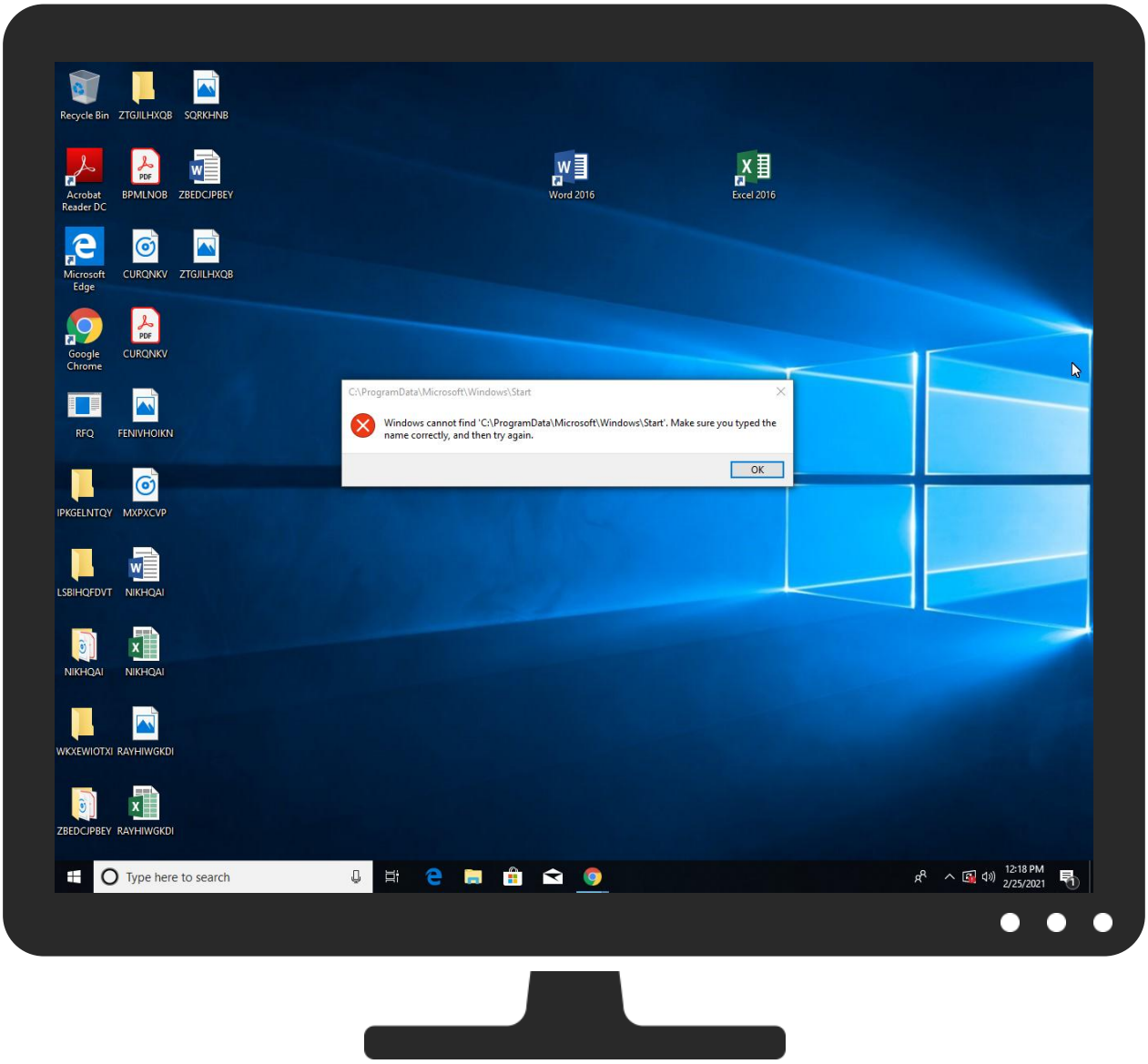


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\july\enrnus.exe	15%	ReversingLabs	Win32.Trojan.Wacatac	
C:\Users\user\AppData\Local\Temp\RegAsm.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\RegAsm.exe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ns.adb	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ns.adb	RFQ.exe, 00000000.00000003.347926461.00000000098E4000.00000004.00000001.sdmp, enrnus.exe, 00000014.00000003.494057230.00000000096F4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pki.goog/gsr2/GTS1O1.crt0	RFQ.exe, 00000000.00000002.474429338.0000000002ED3000.00000004.00000001.sdmp, enrnus.exe, 00000014.00000002.593387777.000000010AC000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.c/g	RFQ.exe, 00000000.00000003.347926461.00000000098E4000.00000004.00000001.sdmp, RFQ.exe, 00000000.00000003.471130439.00000000098E5000.00000004.00000001.sdmp, enrnus.exe, 00000014.00000003.494393505.00000000096F4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.pki.goog/gsr2/gsr2.crl0?	enrnus.exe, 00000014.00000002.593387777.00000000010AC000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.pki.goog/gsr202	enrnus.exe, 00000014.00000002.593387777.00000000010AC000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pki.goog/repository/0	enrnus.exe, 00000014.00000002.593387777.00000000010AC000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.cobj	RFQ.exe, 00000000.00000003.347926461.00000000098E4000.00000004.00000001.sdmp, RFQ.exe, 00000000.00000003.471130439.00000000098E5000.00000004.00000001.sdmp, enrnus.exe, 00000014.00000003.494393505.00000000096F4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.pki.goog/gts1o1core0	RFQ.exe, 00000000.00000002.474429338.0000000002ED3000.00000004.00000001.sdmp, enrnus.exe, 00000014.00000002.593387777.00000000010AC000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	RFQ.exe, 00000000.00000002.474404366.0000000002EA1000.00000004.00000001.sdmp, enrnus.exe, 00000014.00000002.594984683.00000000002CF1000.00000004.00000001.sdmp	false		high
http://schema.org/WebPage	RFQ.exe, 00000000.00000002.474462948.0000000002EEB000.00000004.00000001.sdmp, enrnus.exe, 00000014.00000002.595053339.00000000002D3A000.00000004.00000001.sdmp	false		high
http://crl.pki.goog/GTS1O1core.crl0	RFQ.exe, 00000000.00000002.474429338.0000000002ED3000.00000004.00000001.sdmp, enrnus.exe, 00000014.00000002.593387777.00000000010AC000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.ado/1	RFQ.exe, 00000000.00000003.347926461.00000000098E4000.00000004.00000001.sdmp, RFQ.exe, 00000000.00000003.471130439.00000000098E5000.00000004.00000001.sdmp, enrnus.exe, 00000014.00000003.494393505.00000000096F4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358327
Start date:	25.02.2021
Start time:	12:15:39
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RFQ.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211

Number of analysed new started processes analysed:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.adwa.evad.winEXE@8/4@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 3.1% (good quality ratio 1.5%) • Quality average: 26.8% • Quality standard deviation: 33.7%
HCA Information:	• Successful, ratio: 85% • 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 • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.64.90.137, 23.211.6.115, 168.61.161.212, 13.88.21.125, 142.250.185.164, 131.253.33.200, 13.107.22.200, 104.43.193.48, 51.11.168.160, 205.185.216.10, 205.185.216.42, 51.103.5.186, 52.155.217.156, 20.54.26.129, 92.122.213.247, 92.122.213.194, 184.30.20.56, 51.104.139.180 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, www.google.com, 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, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, cds.d2s7q6s2.hwcdn.net, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • 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. • Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:16:42	API Interceptor	306x Sleep call for process: RFQ.exe modified
12:16:45	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run audiomac C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\july\enrnus.exe
12:16:54	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run audiomac C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\july\enrnus.exe
12:17:49	API Interceptor	318x Sleep call for process: enrnus.exe modified
12:18:37	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\RegAsm.exe	CI & PL 2021 shipment for correction,pdf.exe	Get hash	malicious	Browse	
	BL COPY.exe	Get hash	malicious	Browse	
	IDS_ScanCopy6754588899.exe	Get hash	malicious	Browse	
	Order 01001O02.exe	Get hash	malicious	Browse	
	PAYMENT DETAILS.exe	Get hash	malicious	Browse	
	PAYMENT ADVICE 09680820210111091448.exe	Get hash	malicious	Browse	
	CN-Invoice-XXXXX9808-19011143287989.exe	Get hash	malicious	Browse	
	qsiEm04k63.exe	Get hash	malicious	Browse	
	Payment slip.exe	Get hash	malicious	Browse	
	2Dd20YdQDR.exe	Get hash	malicious	Browse	
	atikmdag-patcher 1.4.7.exe	Get hash	malicious	Browse	
	Scan_00059010189_ ref. 004118379411_ pdf.exe	Get hash	malicious	Browse	
	hfix.exe	Get hash	malicious	Browse	
	atikmdag-patcher 1.4.8.exe	Get hash	malicious	Browse	
	Client1.exe	Get hash	malicious	Browse	
	miner.exe	Get hash	malicious	Browse	
	PhoenixMiner_5.4c_Windows.exe	Get hash	malicious	Browse	
	74725794.exe	Get hash	malicious	Browse	
	PO-498475-ORDER.vbs	Get hash	malicious	Browse	
	Payment Advice Note from 19.11.2020.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\july\enrnus.exe	
Process:	C:\Users\user\Desktop\RFQ.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1045504
Entropy (8bit):	6.571163294446179
Encrypted:	false
SSDEEP:	24576:fMjaXzO4jx8swe2M14J8bLMN86APmFsnIBaOhYvO4LPjlDy4XBc+:fMjaXzO4l8swe2k4J8bLMN86APmFNBWO
MD5:	6733E06C6BE5CA14FFC33763202F53C8
SHA1:	9412D3147B30A873B94E2D0F495EAFDEA1479EE1
SHA-256:	72F30E8884110E06B133ECABFDBF523AEF8CC5533273AA3E12AFEE785A5A45BC
SHA-512:	95E4B792853D583ACB7C2BCC1AF974CCBD20EAD31A917208F7BF070E71C15D226EF1A0D61C7E18D8679C33E07A9E9739EDD858F450B00B13C2433758AAAAB13
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 15%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....H.X..... ... .@.. .....`..... ..`.....W.... .....@..... ....H.....text..... ....`.rsrc..... .....@..@.reloc.....@ .....@..B.....H.....\.....(....I.....E.<y...y&..Y..~W.[..2....,Z..C .+..J..GD..k...da...y....d.@..[...b.....(...y>...\|f.U...S..L...v..C} _.....M..`S#`..k.....p.>.Gn8...RO.X.i.mz.f.....M...#.x..!9...{.....c.....^..*..o.....W.7..s...-[..s.s..oi.X....n6.....Z.....Q.y./.r....c^."N..'y*p...]...0..W*...BQ..0..."{y*..R.d..E.-...-....)... <...6.M..8.b.^.*".....E.rR...p5..IaDF.O)4h&P...>A...S.<.u...=.n.o.$..7..C.....X

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\july\enrnus.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\RFQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RFQ.exe.log	
Process:	C:\Users\user\Desktop\RFQ.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1318
Entropy (8bit):	5.35748495629225
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4bE4K5AE4Kzr7K84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoyE4P:MIHK5HKXE1qHbHK5AHKzvKviYHKhQnov
MD5:	C752BC4289E47E13AECB02FB0A525249
SHA1:	FA76430425B22B6D1BB8F737DE9F36DA996FFD9C
SHA-256:	19F546CEC9D3F9217584617117869E36A742D78D070D78212C64518317C0E45F
SHA-512:	98F2B88340F01B00FDB2EDAEFFB4AE9454B7F87E542CD827538D91A70B3EF59CD6B8E6FB63CA94D7750829D12415599C3B6D0C932CBDDCB33F10D887ACF5917
Malicious:	false
Reputation:	low
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..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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.Co

C:\Users\user\AppData\Local\Temp\RegAsm.exe	
Process:	C:\Users\user\Desktop\RFQ.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows

C:\Users\user\AppData\Local\Temp\RegAsm.exe	
Category:	dropped
Size (bytes):	64616
Entropy (8bit):	6.037264560032456
Encrypted:	false
SSDEEP:	768:J8XcJiMjm2ieHlPyCsSuJbn8dBhFVBSMQ6Iq8TSYDKpgLaDViRLNdr:9YMaNylPYSAb8dBnTHv8DKKaDVkX
MD5:	6FD7592411112729BF6B1F2F6C34899F
SHA1:	5E5C839726D6A43C478AB0B95DBF52136679F5EA
SHA-256:	FFE4480CCC81B061F725C54587E9D1BA96547D27FE28083305D75796F2EB3E74
SHA-512:	21EFCC9DEE3960F1A64C6D8A44871742558666BB792D77ACE91236C7DBF42A6CA77086918F363C4391D9C00904C55A952E2C18BE5FA1A67A509827BFC630070I
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: CI & PL 2021 shipment for correction,pdf.exe, Detection: malicious, Browse • Filename: BL COPY.exe, Detection: malicious, Browse • Filename: IDS_ScanCopy6754588899.exe, Detection: malicious, Browse • Filename: Order 01001O02.exe, Detection: malicious, Browse • Filename: PAYMENT DETAILS.exe, Detection: malicious, Browse • Filename: PAYMENT ADVICE 09680820210111091448.exe, Detection: malicious, Browse • Filename: CN-Invoice-XXXXX9808-19011143287989.exe, Detection: malicious, Browse • Filename: qsiEm04k63.exe, Detection: malicious, Browse • Filename: Payment slip.exe, Detection: malicious, Browse • Filename: 2Dd20YdQDR.exe, Detection: malicious, Browse • Filename: atikmdag-patcher 1.4.7.exe, Detection: malicious, Browse • Filename: Scan_00059010189_ ref. 004118379411_ pdf.exe, Detection: malicious, Browse • Filename: hfix.exe, Detection: malicious, Browse • Filename: atikmdag-patcher 1.4.8.exe, Detection: malicious, Browse • Filename: Client1.exe, Detection: malicious, Browse • Filename: miner.exe, Detection: malicious, Browse • Filename: PhoenixMiner_5.4c_Windows.exe, Detection: malicious, Browse • Filename: 74725794.exe, Detection: malicious, Browse • Filename: PO-498475-ORDER.vbs, Detection: malicious, Browse • Filename: Payment Advice Note from 19.11.2020.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...xX.Z.....0.....^.... .....@.. ....`.....O.....8.....h>..... ..... ..H.....text...d.... ..... ..`.rsrc...8.....@..@.reloc..... .....@..B.....@.....H.....A...p.....T.....~P...-.r...p.....(....(....s.....P...*..0..".....(.....-.r...p.rl..p(....s....z.*...0.....(....~P.....o..... .*..(....*n(.....(.....%...(....*~(.....(.....%...%...(....*.(.....(.....%...%...%...(....*V.(.....}Q.....}R...*..{Q...*..{R...*...0.....(.....i.=...}S.....i.@...}T.....i.@...}U.....+m...(....o .....r]..p.o!....,..{T.....{U.....o"....+(.ra..p.o!....,..{T.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.571163294446179
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:	RFQ.exe
File size:	1045504
MD5:	6733e06c6be5ca14ffc33763202f53c8
SHA1:	9412d3147b30a873b94e2d0f495eafdea1479ee1
SHA256:	72f30e8884110e06b133ecabfdbf523aef8cc5533273aa3e12afee785a5a45bc
SHA512:	95e4b792853d583acb7c2bcc1af974ccbd20ead31a917208f7bf070e71c15d226ef1a0d61c7e18d8679c33e07a9e9739edd858f450b00b13c2433758aaaab143
SSDEEP:	24576:fMjaXzO4jx8swe2M14J8bLMN86APmFsnIBaOhYvO4LPjlDy4XBc+:fMjaXzO4l8swe2k4J8bLMN86APmFNBWO
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....H.X..... ... .@.. .....`.....`.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x5001de
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, HIGH_ENTROPY_VA
Time Stamp:	0x588848B6 [Wed Jan 25 06:41:58 2017 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
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add 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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x100184	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x102000	0xcdf	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x104000	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	0xfe1e4	0xfe200	False	0.608103018938	data	6.57523758898	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x102000	0xcdf	0xe00	False	0.378348214286	data	4.77533741669	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x104000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x1020a0	0x39c	data		
RT_MANIFEST	0x10243c	0x8a3	XML 1.0 document, UTF-8 Unicode (with BOM) text		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2005 3H<7C?IA<6FJJE:;5HGJ
Assembly Version	1.0.0.0
InternalName	again.exe
FileVersion	5.8.10.13
CompanyName	3H<7C?IA<6FJJE:;5HGJ
Comments	@EA=>IGI=9H:3@A2AA3
ProductName	EH@8<G955B73@B88=;GA@@2D
ProductVersion	5.8.10.13
FileDescription	EH@8<G955B73@B88=;GA@@2D
OriginalFilename	again.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/25/21-12:18:37.423575	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49756	1985	192.168.2.6	185.244.30.161

UDP Packets

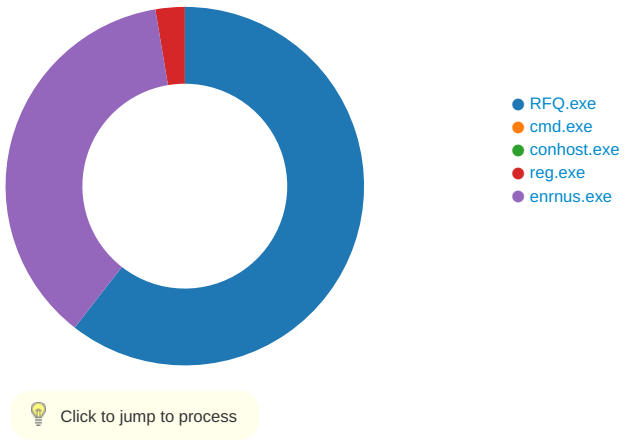
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 12:16:22.727293015 CET	62044	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:16:22.787478924 CET	53	62044	8.8.8.8	192.168.2.6
Feb 25, 2021 12:16:24.581695080 CET	63791	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:16:25.595849991 CET	63791	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:16:25.658751965 CET	53	63791	8.8.8.8	192.168.2.6
Feb 25, 2021 12:16:26.008734941 CET	64267	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:16:26.069957972 CET	53	64267	8.8.8.8	192.168.2.6
Feb 25, 2021 12:16:27.122786999 CET	49448	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:16:27.174323082 CET	53	49448	8.8.8.8	192.168.2.6
Feb 25, 2021 12:16:28.655915976 CET	60342	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:16:28.706482887 CET	53	60342	8.8.8.8	192.168.2.6
Feb 25, 2021 12:16:29.786921978 CET	61346	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:16:29.835741997 CET	53	61346	8.8.8.8	192.168.2.6
Feb 25, 2021 12:16:31.028070927 CET	51774	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:16:31.089288950 CET	53	51774	8.8.8.8	192.168.2.6
Feb 25, 2021 12:16:31.176573038 CET	56023	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:16:31.234807968 CET	53	56023	8.8.8.8	192.168.2.6
Feb 25, 2021 12:16:31.465831041 CET	58384	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:16:31.514385939 CET	53	58384	8.8.8.8	192.168.2.6
Feb 25, 2021 12:16:31.522681952 CET	60261	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:16:31.571381092 CET	53	60261	8.8.8.8	192.168.2.6
Feb 25, 2021 12:16:32.461899996 CET	56061	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:16:32.513628960 CET	53	56061	8.8.8.8	192.168.2.6
Feb 25, 2021 12:16:33.671749115 CET	58336	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:16:33.720500946 CET	53	58336	8.8.8.8	192.168.2.6
Feb 25, 2021 12:16:34.625479937 CET	53781	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:16:34.675333023 CET	53	53781	8.8.8.8	192.168.2.6
Feb 25, 2021 12:16:35.717607021 CET	54064	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:16:35.766388893 CET	53	54064	8.8.8.8	192.168.2.6
Feb 25, 2021 12:16:36.702701092 CET	52811	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:16:36.752760887 CET	53	52811	8.8.8.8	192.168.2.6
Feb 25, 2021 12:16:37.699152946 CET	55299	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:16:37.750910044 CET	53	55299	8.8.8.8	192.168.2.6
Feb 25, 2021 12:16:38.874150038 CET	63745	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:16:38.924274921 CET	53	63745	8.8.8.8	192.168.2.6
Feb 25, 2021 12:16:39.996886969 CET	50055	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:16:40.054152012 CET	53	50055	8.8.8.8	192.168.2.6
Feb 25, 2021 12:16:43.821738958 CET	61374	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:16:43.920892000 CET	53	61374	8.8.8.8	192.168.2.6
Feb 25, 2021 12:16:45.225033045 CET	50339	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:16:45.275497913 CET	53	50339	8.8.8.8	192.168.2.6
Feb 25, 2021 12:16:46.519507885 CET	63307	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:16:46.568161011 CET	53	63307	8.8.8.8	192.168.2.6
Feb 25, 2021 12:16:58.320008993 CET	49694	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:16:58.368999958 CET	53	49694	8.8.8.8	192.168.2.6
Feb 25, 2021 12:17:17.857564926 CET	54982	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:17:17.909198046 CET	53	54982	8.8.8.8	192.168.2.6
Feb 25, 2021 12:17:19.028069973 CET	50010	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:17:19.076870918 CET	53	50010	8.8.8.8	192.168.2.6
Feb 25, 2021 12:17:21.776122093 CET	63718	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:17:21.836282969 CET	53	63718	8.8.8.8	192.168.2.6
Feb 25, 2021 12:17:22.491647959 CET	62116	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:17:22.548764944 CET	53	62116	8.8.8.8	192.168.2.6
Feb 25, 2021 12:17:23.113923073 CET	63816	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:17:23.170830965 CET	53	63816	8.8.8.8	192.168.2.6
Feb 25, 2021 12:17:23.596215963 CET	55014	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:17:23.648888111 CET	53	55014	8.8.8.8	192.168.2.6
Feb 25, 2021 12:17:24.043178082 CET	62208	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:17:24.115250111 CET	57574	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:17:24.121511936 CET	53	62208	8.8.8.8	192.168.2.6
Feb 25, 2021 12:17:24.179927111 CET	53	57574	8.8.8.8	192.168.2.6
Feb 25, 2021 12:17:24.800698042 CET	51818	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 12:17:24.857887983 CET	53	51818	8.8.8.8	192.168.2.6
Feb 25, 2021 12:17:25.413422108 CET	56628	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:17:25.465018034 CET	53	56628	8.8.8.8	192.168.2.6
Feb 25, 2021 12:17:26.684542894 CET	60778	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:17:26.737323999 CET	53	60778	8.8.8.8	192.168.2.6
Feb 25, 2021 12:17:28.095009089 CET	53799	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:17:28.152288914 CET	53	53799	8.8.8.8	192.168.2.6
Feb 25, 2021 12:17:28.723160982 CET	54683	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:17:28.784219027 CET	53	54683	8.8.8.8	192.168.2.6
Feb 25, 2021 12:17:29.805085897 CET	59329	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:17:29.863773108 CET	53	59329	8.8.8.8	192.168.2.6
Feb 25, 2021 12:17:38.610966921 CET	64021	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:17:38.661577940 CET	53	64021	8.8.8.8	192.168.2.6
Feb 25, 2021 12:17:39.065171957 CET	56129	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:17:39.116597891 CET	53	56129	8.8.8.8	192.168.2.6
Feb 25, 2021 12:17:39.137428045 CET	58177	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:17:39.186067104 CET	53	58177	8.8.8.8	192.168.2.6
Feb 25, 2021 12:17:58.726459026 CET	50700	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:17:58.779820919 CET	53	50700	8.8.8.8	192.168.2.6
Feb 25, 2021 12:18:00.975207090 CET	54069	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:18:01.036456108 CET	53	54069	8.8.8.8	192.168.2.6
Feb 25, 2021 12:18:01.730922937 CET	61178	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:18:01.782592058 CET	53	61178	8.8.8.8	192.168.2.6
Feb 25, 2021 12:18:19.645900011 CET	57017	53	192.168.2.6	8.8.8.8
Feb 25, 2021 12:18:19.695908070 CET	53	57017	8.8.8.8	192.168.2.6

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: RFQ.exe PID: 6876 Parent PID: 5912

General

Start time:	12:16:30
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\RFQ.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RFQ.exe'
Imagebase:	0x9f0000
File size:	1045504 bytes
MD5 hash:	6733E06C6BE5CA14FFC33763202F53C8
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: 00000000.00000002.476175749.000000000488C000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.476175749.000000000488C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.476175749.000000000488C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.475624148.000000000478E000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.475624148.000000000478E000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.475624148.000000000478E000.00000004.00000001.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	6DEBCF06	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	6DEBCF06	unknown
C:\Users\user\AppData\Local\Temp\RegAsm.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	9A05B73	CopyFileExW
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\july	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CD0BEFF	CreateDirectoryW
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\july\enrnus.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	9A05B73	CopyFileExW
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\july\enrnus.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	9A05B73	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RFQ.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1CC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\RegAsm.exe	0	64616	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 78 58 8e 5a 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 b0 00 00 00 0c 00 00 00 00 00 00 5e ce 00 00 00 20 00 00 00 e0 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 20 01 00 00 02 00 00 df c9 01 00 03 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...xX.Z.......... ....0............^.... ....@.. ....`................	success or wait	1	9A05B73	CopyFileExW
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\july\enrnus.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 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 b6 48 88 58 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 e2 0f 00 00 10 00 00 00 00 00 00 de 01 10 00 00 20 00 00 00 20 10 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 60 10 00 00 02 00 00 00 00 00 00 02 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....H.X.......... ....@.. ....` ............`................	success or wait	4	9A05B73	CopyFileExW
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\july\enrnus.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	9A05B73	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RFQ.exe.log	unknown	1318	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	6E1CC907	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	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD01B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6032 Parent PID: 6876

General

Start time:	12:16:40

Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'audiomac' /t REG_SZ /d 'C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\july\enrnus.exe'
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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

Analysis Process: conhost.exe PID: 1428 Parent PID: 6032

General

Start time:	12:16:41
Start date:	25/02/2021
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: reg.exe PID: 6188 Parent PID: 6032

General

Start time:	12:16:41
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'audiomac' /t REG_SZ /d 'C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\july\enrnus.exe'
Imagebase:	0xaf0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
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

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	audiomac	unicode	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\july\enrnus.exe	success or wait	1	AF5A1D	RegSetValueExW

Analysis Process: enrnus.exe PID: 2288 Parent PID: 6876

General

Start time:	12:17:36
Start date:	25/02/2021
Path:	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\july\enrnus.exe
Wow64 process (32bit):	true
Commandline:	'C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\july\enrnus.exe'
Imagebase:	0x7c0000
File size:	1045504 bytes
MD5 hash:	6733E06C6BE5CA14FFC33763202F53C8
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: 00000014.00000002.601490451.00000000045D9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.601490451.00000000045D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.601490451.00000000045D9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.601634040.00000000046D7000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.601634040.00000000046D7000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.601634040.00000000046D7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 15%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEBCF06	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	6DEBCF06	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	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD01B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis