ID: 457719
Sample Name: Quotation Request August RFQ8012021.exe
Cookbook: default.jbs
Time: 08:43:06
Date: 02/08/2021
Version: 33.0.0 White Diamond

Table of Contents

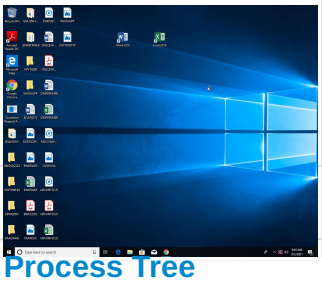
Windows Analysis Report Quotation Request August RF…

Overview

General Information

Sample Name:	Quotation Request August RFQ8012021.exe
Analysis ID:	457719
MD5:	dd69f329393643a.
SHA1:	dbcb022f10c8cfc…
SHA256:	9327c22d332141..
Tags:	exe NanoCore
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

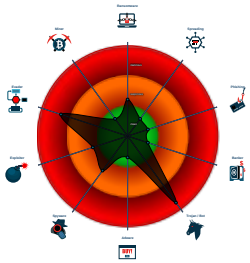
Nanocore

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

Signatures

- Detected Nanocore Rat
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Allocates memory in foreign process…
- Creates an undocumented autostart …
- Drops PE files with benign system n…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …

Classification



Process Tree

- **System is w10x64**
- Quotation Request August RFQ8012021.exe (PID: 6640 cmdline: 'C:\Users\user\Desktop\Quotation Request August RFQ8012021.exe' MD5: DD69F329393643AA570BD3A940323136)
  - cmd.exe (PID: 7156 cmdline: 'cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon' /f /v 'Shell' /t REG_SZ /d 'explorer.exe,C:\Users\user\AppData\Roaming\MainProc.exe,' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 7164 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - reg.exe (PID: 5868 cmdline: REG ADD 'HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon' /f /v 'Shell' /t REG_SZ /d 'explorer.exe,C:\Users\user\AppData\Roaming\MainProc.exe,' MD5: CEE2A7E57DF2A159A065A34913A055C2)
  - MainProc.exe (PID: 6288 cmdline: 'C:\Users\user\AppData\Roaming\MainProc.exe' MD5: DD69F329393643AA570BD3A940323136)
    - InstallUtil.exe (PID: 5880 cmdline: C:\Users\user\AppData\Local\Temp\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
    - smss.exe (PID: 5460 cmdline: 'C:\Users\user\AppData\Local\Temp\smss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
      - smss.exe (PID: 5908 cmdline: 'C:\Users\user\AppData\Local\Temp\smss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - smss.exe (PID: 6752 cmdline: 'C:\Users\user\AppData\Local\Temp\smss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
      - smss.exe (PID: 5772 cmdline: 'C:\Users\user\AppData\Local\Temp\smss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - smss.exe (PID: 5032 cmdline: 'C:\Users\user\AppData\Local\Temp\smss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
      - smss.exe (PID: 6904 cmdline: 'C:\Users\user\AppData\Local\Temp\smss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - smss.exe (PID: 1664 cmdline: 'C:\Users\user\AppData\Local\Temp\smss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
      - smss.exe (PID: 4928 cmdline: 'C:\Users\user\AppData\Local\Temp\smss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - smss.exe (PID: 6196 cmdline: 'C:\Users\user\AppData\Local\Temp\smss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
      - smss.exe (PID: 7084 cmdline: 'C:\Users\user\AppData\Local\Temp\smss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - smss.exe (PID: 6048 cmdline: 'C:\Users\user\AppData\Local\Temp\smss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
      - smss.exe (PID: 7116 cmdline: 'C:\Users\user\AppData\Local\Temp\smss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - smss.exe (PID: 6712 cmdline: 'C:\Users\user\AppData\Local\Temp\smss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
      - smss.exe (PID: 1260 cmdline: 'C:\Users\user\AppData\Local\Temp\smss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
- dhcpmon.exe (PID: 2928 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: EFEC8C379D165E3F33B536739AEE26A3)
  - conhost.exe (PID: 2224 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000012.00000002.933931703.000000000407E000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xb4377:$a: NanoCore • 0xb439c:$a: NanoCore • 0xb43f5:$a: NanoCore • 0xc4594:$a: NanoCore • 0xc45ba:$a: NanoCore • 0xc4616:$a: NanoCore • 0xd146d:$a: NanoCore • 0xd14c6:$a: NanoCore • 0xd14f9:$a: NanoCore • 0xd1725:$a: NanoCore • 0xd17a1:$a: NanoCore • 0xd1dba:$a: NanoCore • 0xd1f03:$a: NanoCore • 0xd23d7:$a: NanoCore • 0xd26be:$a: NanoCore • 0xd26d5:$a: NanoCore • 0xdb579:$a: NanoCore • 0xdb5f5:$a: NanoCore • 0xdded8:$a: NanoCore • 0xe34a1:$a: NanoCore • 0xe351b:$a: NanoCore
00000012.00000002.920030285.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000012.00000002.920030285.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000012.00000002.920030285.000000000402000.00000040.00000001.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:$j: #=q
00000012.00000002.944192934.0000000007E20000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5b99:$x1: NanoCore.ClientPluginHost • 0x5bb3:$x2: IClientNetworkHost
Click to see the 32 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
18.2.InstallUtil.exe.4337c5e.11.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x170b:$x1: NanoCore.ClientPluginHost • 0x1725:$x2: IClientNetworkHost
18.2.InstallUtil.exe.4337c5e.11.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x170b:$x2: NanoCore.ClientPluginHost • 0x34b6:$s4: PipeCreated • 0x16f8:$s5: IClientLoggingHost
18.2.InstallUtil.exe.412d7e1.7.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2dbb:$x1: NanoCore.ClientPluginHost • 0x2de5:$x2: IClientNetworkHost
18.2.InstallUtil.exe.412d7e1.7.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2dbb:$x2: NanoCore.ClientPluginHost • 0x4c6b:$s4: PipeCreated
18.2.InstallUtil.exe.7dc0000.25.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5b0b:$x1: NanoCore.ClientPluginHost • 0x5b44:$x2: IClientNetworkHost
Click to see the 194 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: System File Execution Location Anomaly

Sigma detected: Possible Applocker Bypass

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

Persistence and Installation Behavior:

Drops PE files with benign system names

Boot Survival:

Creates an undocumented autostart registry key

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

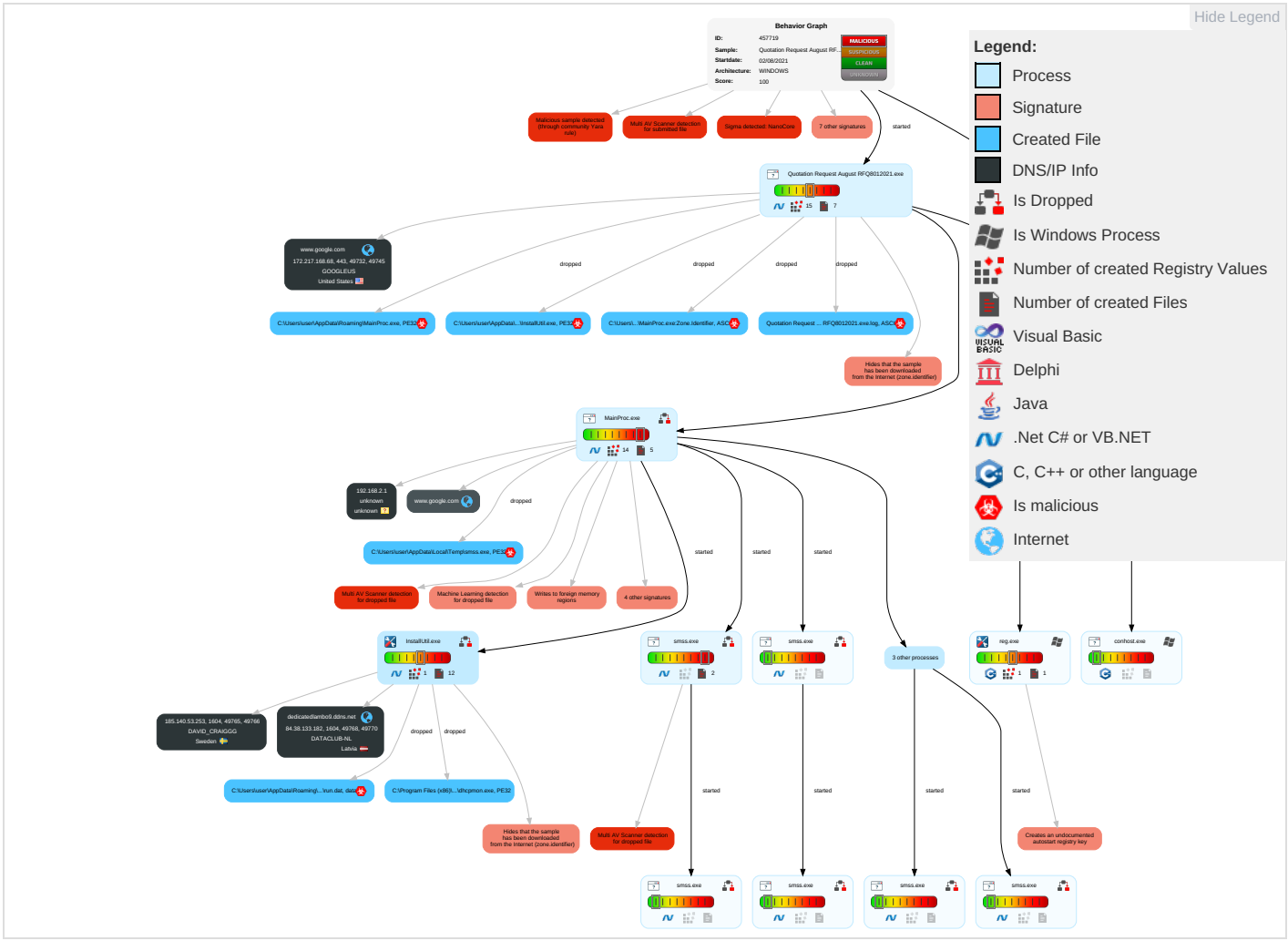
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C a
Valid Accounts 1	Windows Management Instrumentation 1	Valid Accounts 1	Valid Accounts 1	Disable or Modify Tools 1	Input Capture 2 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	E C
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	N P
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 3 1 2	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 1 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	R S
Local Accounts	At (Windows)	Logon Script (Mac)	Registry Run Keys / Startup Folder 1	Software Packing 1 1	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	N A L P
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Security Software Discovery 1 1 1	SSH	Keylogging	Data Transfer Size Limits	A L P
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 2	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	M C
External Remote Services	Scheduled Task	Startup Items	Startup Items	Valid Accounts 1	DCSync	Virtualization/Sandbox Evasion 2 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	C U
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Modify Registry 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	A L
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 1	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	W
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Virtualization/Sandbox Evasion 2 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Fi P
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Process Injection 3 1 2	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	M

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C a
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Hidden Files and Directories 1	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	D

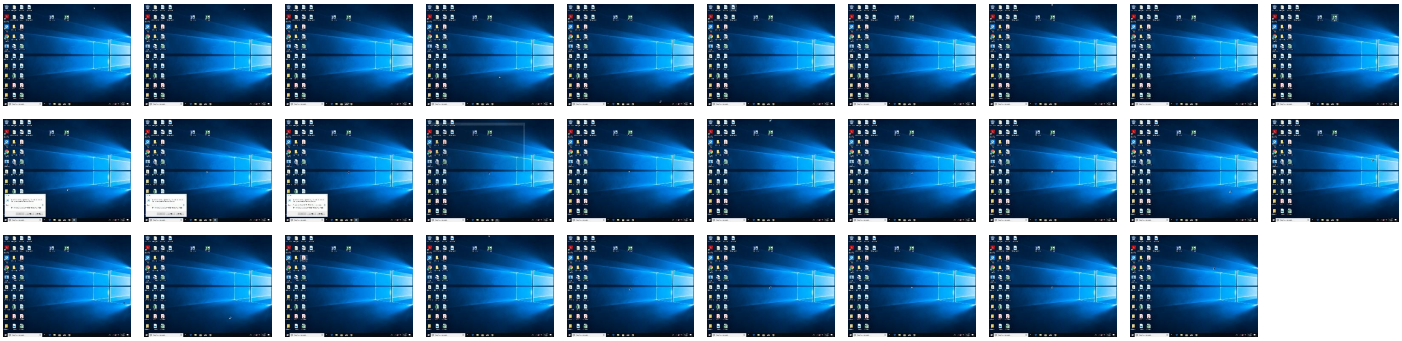
Behavior Graph



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
Quotation Request August RFQ8012021.exe	26%	Virustotal		Browse
Quotation Request August RFQ8012021.exe	15%	ReversingLabs		
Quotation Request August RFQ8012021.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\MainProc.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\smss.exe	14%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\smss.exe	13%	ReversingLabs		
C:\Users\user\AppData\Roaming\MainProc.exe	15%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
18.2.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
18.2.InstallUtil.exe.61a0000.19.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Source	Detection	Scanner	Label	Link	Download
18.2.InstallUtil.exe.3ff8a40.6.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.pki.goog/gsr1/gsr1.crl0;	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj?&	0%	Avira URL Cloud	safe	
http://ns.ado/1?&	0%	Avira URL Cloud	safe	
http://ns.d	0%	URL Reputation	safe	
http://ns.adobe.c/g5	0%	Avira URL Cloud	safe	
http://crl.pki.goog/gtsr1/gtsr1.crl0W	0%	URL Reputation	safe	
http://pki.goog/gsr1/gsr1.crt02	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://ns.adobe.cobj5	0%	Avira URL Cloud	safe	
http://ns.adobe.c/g?&	0%	Avira URL Cloud	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/15	0%	Avira URL Cloud	safe	
http://crls.pki.goog/gts1c3/fVJxbV-Ktmk.crl0	0%	Avira URL Cloud	safe	
http://pki.goog/repo/certs/gts1c3.der0	0%	URL Reputation	safe	
http://pki.goog/repo/certs/gtsr1.der04	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dedicatedlambo9.ddns.net	84.38.133.182	true	false		high
www.google.com	172.217.168.68	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
172.217.168.68	www.google.com	United States		15169	GOOGLEUS	false
84.38.133.182	dedicatedlambo9.ddns.net	Latvia		203557	DATACLUB-NL	false
185.140.53.253	unknown	Sweden		209623	DAVID_CRAIGGG	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	457719
Start date:	02.08.2021

Start time:	08:43:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Quotation Request August RFQ8012021.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:	39
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@38/23@8/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.6% (good quality ratio 1.3%) • Quality average: 66.9% • Quality standard deviation: 33.7%
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
08:44:35	API Interceptor	1x Sleep call for process: Quotation Request August RFQ8012021.exe modified
08:45:07	API Interceptor	461x Sleep call for process: InstallUtil.exe modified
08:45:09	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

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	41064
Entropy (8bit):	6.164873449128079
Encrypted:	false
SSDEEP:	384:FtpFVLK0MsihB9VKS7xdgE7KJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+sPZTd:ZBMs2SqdD86Iq8gZZFyViML3an
MD5:	EFEC8C379D165E3F33B536739AEE26A3
SHA1:	C875908ACBA5CAC1E0B40F06A83F0F156A2640FA
SHA-256:	46DEE184523A584E56DF93389F81992911A1BA6B1F05AD7D803C6AB1450E18CB
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCFF
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....0..T.....r... .....@.. ....`.....4r..O.....b..h>.....p..... ..... ..H.....text....R... ...T..... ..`.rsrc.....V.....@..@.rel oc.....`.....@..B.....hr.....H.....".|J.....lm.....o.....2~.....o....*.r...p(....*VrK..p(....s.....*..0.....(....(....o....o....(....o.... .....T(....o....(....o....o ...o!....4(....o....(....o....o ...o".....(....rm..ps#...o....($.....(%....o&....ry..p.....%.r...p.%.(.....(....('....((.....o)...('.....*.*.....".(*...*..{Q...-...}Q.....(+...(....(,....(+...*"..(- ...*..(....*..(.....r...p.(/...o0...s....}T...*....0.. .....~S...-.s

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Quotation Request August RFQ8012021.exe.log	
Process:	C:\Users\user\Desktop\Quotation Request August RFQ8012021.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1316
Entropy (8bit):	5.343667025898124
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7csXE4D8Q:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHe
MD5:	379135DE3C31F3A766187BD9B6C730C9
SHA1:	BEFFE8BDE231861A3FD901A12F51523399B9A5E7
SHA-256:	BDE88F5C7F95E26FFC5EBE86C38AE61E78E0A5AA932A83DE00F2A46DB24DD22D
SHA-512:	2897AAB0225823AC258D5D5E52B43140F2B47603689C968243F515B516A2712CAC69A0D7317C53575CF725D7EBDC85C93637F57E626778117364D5666C9FB993
Malicious:	**true**
Reputation:	unknown
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,"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.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=b77a

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	950
Entropy (8bit):	5.350971482944737
Encrypted:	false
SSDEEP:	24:MLiKNE4qpE4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7a:MeIH2HKXwYHKhQnoPtHoxHhAHKzva
MD5:	CEE81B7EB08EE82CFE49E47B81B50D1A
SHA1:	4746C7068BD50E3309BFFDBE8983B8F27D834DFD
SHA-256:	B9A90255691E7C9D3CCBD27D00FC514DDD6087446D8DB03335CEF1B5634CC460
SHA-512:	AF5865439412974FCB6B11E22CFFF1ACA0BEBF83CF398D6056CEEF93720AF0FBCB579858C39E6AA0D989680F2180F2CA181D7D12887604B420D0E1976B8AEA7

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Configuration.Install, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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..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\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\smss.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\smss.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1362
Entropy (8bit):	5.343186145897752
Encrypted:	false
SSDEEP:	24:ML9E4Ks2eE4O1lEE4UVwPKDE4KhK3VZ9pKhuE4IWUAE4KI6no84j:MxHKXeHKlEHU0YHKhQnouHIW7HKjovj
MD5:	1249251E90A1C28AB8F7235F30056DEB
SHA1:	166BA6B64E9B0D9BA7B856334F7D7EC027030BA1
SHA-256:	B5D65BF3581136CD5368BC47FA3972E06F526EED407BC6571D11D9CD4B5C4D83
SHA-512:	FD880C5B12B22241F67139ABD09B99ACE7A4DD24635FC6B340A3E7C463E2AEF3FA68EF647352132934BC1F8CA134F46064049449ACB67954BEDDEA9AA967088
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",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,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
Process:	C:\Users\user\Desktop\Quotation Request August RFQ8012021.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	41064
Entropy (8bit):	6.164873449128079
Encrypted:	false
SSDEEP:	384:FtpFVLK0MsihB9VKS7xdgE7KJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+sPZTd:ZBMs2SqdD86lq8gZZFyViML3an
MD5:	EFEC8C379D165E3F33B536739AEE26A3
SHA1:	C875908ACBA5CAC1E0B40F06A83F0F156A2640FA
SHA-256:	46DEE184523A584E56DF93389F81992911A1BA6B1F05AD7D803C6AB1450E18CB
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCFF
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....0..T.....r... .....@.. ....`.....4r..O.....b..h>.....p..... ..... ..H.....text....R... ...T..... ..`.rsrc.....V.....@..@.reloc.....`.....@..B.....hr.....H.....".J.....lm.....o.....2~.....o....*.r...p(....*VrK..p(....s.....*..0.....(....(....o....o....(....o.... .....T(....o....(....o....o ...o!....4(....o....(....o....o ...o".....(....rm..ps#...o....($.....(%....o&....ry..p.....%.r...p.%.(.....(....('....((.....o)...('.....*.*.....".(*...*..{Q...-...}Q.....(+...(....(,....(+...*"..(-...*..(....*..(.....r...p.(/...o0...s....}T...*....0.. .....~S...-.s

C:\Users\user\AppData\Local\Temp\smss.exe	
Process:	C:\Users\user\AppData\Roaming\MainProc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	78336
Entropy (8bit):	4.369296705546591
Encrypted:	false
SSDEEP:	768:jlU4+MS3Fu0thSOV4GM0SuHk9Oh/1TRIWUk7NlfaNV9KQLxXXSv:l6o03IGMLuHk+Ck5lfaNP7xSv
MD5:	0E362E7005823D0BEC3719B902ED6D62
SHA1:	590D860B909804349E0CDC2F1662B37BD62F7463
SHA-256:	2D0DC6216F613AC7551A7E70A798C22AEE8EB9819428B1357E2B8C73BEF905AD
SHA-512:	518991B68496B3F8545E418CF9B345E0791E09CC20D177B8AA47E0ABA447AA55383C64F5BDACA39F2B061A5D08C16F2AD484AF8A9F238CA23AB081618FBA3AD3

C:\Users\user\AppData\Local\Temp\smss.exe	
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 14%, Browse • Antivirus: ReversingLabs, Detection: 13%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Y .....P..&.....D... .....@.. ....`.....D..W....`.....hD..... ....H.....text...$... ...&..... ..`.rsrc.....`.....(.....@..@.rel oc.....0.....@..B.....D.....H.....l....%.....).....0..6.....(8...t....&.(8...t....&.....(8...t.....8;....8%.....(8...t....&.(8...t..... .:.....(8...t....:.....(8...t....:....(8...t.....\:@....(8...t....&.)...&8.....(8...t....&(8...t....&.....:.....8x.....:L...88....(8...t....&(8...t....&(8...t....&(8...t.....:....8!..... (8...t....&.....(8...t....&.....(8...t....:8.....(8...t....&.

C:\Users\user\AppData\Local\Temp\smss.txt	
Process:	C:\Users\user\AppData\Local\Temp\smss.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:DymfNt+kiEaKC5YIcEs:Wm1wknaZ5YPEs
MD5:	6030D395E9112F76A144D1A2D3A5A74A
SHA1:	8F8E1A7E7FC9711730CF084962911106AF1C890A
SHA-256:	991205B28FA86D000ADA3BE09B940CD49598CBA126F4041DA905A4FCFAA541B3
SHA-512:	28A229D642DFABA4F7AE7D972DC1B89FE89D4914E4451CEBCD57C9EBE780D397FCA9953EC8AF51A0F6BD2343A784907485EC051EA2C6B6CA803B731CAD852 04
Malicious:	false
Reputation:	unknown
Preview:	6288..C:\Users\user\AppData\Roaming\MainProc.exe..6196..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
File Type:	data
Category:	dropped
Size (bytes):	1392
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	24:IQnybgCUtvd7xCFhwUuQnybgCUtvd7xCFhwUuQnybgCUtvd7xCFhwUuQnybgCUt4:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/f
MD5:	E78C6686C5A1A9CB0724F84DEA9A75F0
SHA1:	80E61D5BDC7AF293362024781DA66BEA9D370FF9
SHA-256:	FBE0B513511C00AC3B7169E1BCFB675CFD708B249365D724269C23FAC1184967
SHA-512:	FF3835238CAEA26D8800B56901AB962ACD2FA390F955C4A8A15B5817AAB7642D105538CF63938D218567501477FB4B23C2834F22CBC8BA0002C7BCACB2875637
Malicious:	false
Reputation:	unknown
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.....&.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.....&.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.....&.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.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:F+1kw8n:dn
MD5:	015F76206A31860FD0EBF2D06C6E4F1C
SHA1:	0F85C4922624E7B45C9FFED521F18E293988484F
SHA-256:	209B2BD9810266DEA38E4C30B19C6C050C2EE187D5A6FB4C025902F22FD35B45
SHA-512:	173637CB893AE5A42394292CE39132AA1CEE1FA747BB64FB28E26C6AF88A76CAE3E5924333F7B8D1A8BC9846ECCADC383109F7325C9703F581B1C2DE1A07BB 0
Malicious:	**true**
Reputation:	unknown
Preview:	.....U.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	
Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	4.501629167387823
Encrypted:	false
SSDEEP:	3:9bzY6oRDlvYk:RzWDl3
MD5:	ACD3FB4310417DC77FE06F15B0E353E6
SHA1:	80E7002E655EB5765FDEB21114295CB96AD9D5EB
SHA-256:	DC3AE604991C9BB8FF8BC4502AE3D0DB8A3317512C0F432490B103B89C1A4368
SHA-512:	DA46A917DB6276CD4528CFE4AD113292D873CA2EBE53414730F442B83502E5FAF3D1AE87BFA295ADF01E3B44FDBCE239E21A318BFB2CCD1F4753846CB21F6F97
Malicious:	false
Reputation:	unknown
Preview:	9iH...}Z.4..f..J".C;"a

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	5.320159765557392
Encrypted:	false
SSDEEP:	3:9bzY6oRDlvYVsRLY6oRDT6P2bfVn1:RzWDlfRWDT621
MD5:	BB0F9B9992809E733EFFF8B0E562CFD6
SHA1:	F0BAB3CF73A04F5A689E6AFC764FEE9276992742
SHA-256:	C48F04FE7525AA3A3F9540889883F649726233DE021724823720A59B4F37CEAC
SHA-512:	AE4280AA460DC1C0301D458A3A443F6884A0BE37481737B2ADAFD72C33C55F09BED88ED239C91FE6F19CA137AC3CD7C9B8454C21D3F8E759687F701C8B3C7A6
Malicious:	false
Reputation:	unknown
Preview:	9iH...}Z.4..f..J".C;"a9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92
Malicious:	false
Reputation:	unknown
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i...........J.5b7}..fK..HV.,.,...0.... ....n.w6PMl.....v.””.v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*l..v&.jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.Ql..j_..&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.........Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.|i4...i...;O...n.?.,. ....v?.5}.OY@.dG|<.._[.69@.2..m..l..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....l..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\MainProc.exe	
Process:	C:\Users\user\Desktop\Quotation Request August RFQ8012021.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	775168
Entropy (8bit):	6.683069808516563
Encrypted:	false
SSDEEP:	12288:BLLLO6nlb8uYhkOH7aSV7B+AcitG07iLQSWmJhbfvfkt:BPLRlb853uu7Bg0+LQSWP
MD5:	DD69F329393643AA570BD3A940323136
SHA1:	DBCB022F10C8CFCDD93A75253B9E20260F86DAFE
SHA-256:	9327C22D332141A7EE037B2D393E0AD352A2FC4F6DC9B7CF9C78155D70681E6B

C:\Users\user\AppData\Roaming\MainProc.exe	
SHA-512:	836B07E9F14621179B2C5CD4FA7F778F41A51240ED25B5C62A64D7F1B48B233FA972D6CA77A96B780D1F61251BEF9F5B982B694A02A359A55AD3DC2EC23DD0C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 15%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....51....."...P..... .....@.. .....@..... .`.....O.....J..... ..... ..... ..H.....text..... ..... ..`.rsrc...J.....@..@.reloc..... . .....@..B.....H.....P...l.....t.....(...*&..(!....*.s".....s#.....s$.....s%.....s&.....*Z.....o9.....*&..(:....*j..{....(...+}..... {....+.*j..{....(...+}....{....+.*j..{....(...+}....{....+.*j..{....(...+}....{....+.*j..{....(...+}....{....+.*j..{....(...+}....{....+.*j..{....(...+}....{....+.*j..{....(...+}....{....+.*j..{....(...+}..... {....+.*...{.....,.+.....,.rq..ps?...z..|.

C:\Users\user\AppData\Roaming\MainProc.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Quotation Request August RFQ8012021.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:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2017
Entropy (8bit):	4.663189584482275
Encrypted:	false
SSDEEP:	48:zK4Qu4D4ql0+1AcJRy0EJP64gFljVlWo3ggxUnQK2qmBvgw1+5:zKJDEcTytNe3Wo3uQVBIe+5
MD5:	9C305D95E7DA8FCA9651F7F426BB25BC
SHA1:	FDB5C18C26CF5B83EF5DC297C0F9CEBEF6A97FFC
SHA-256:	444F71CF504D22F0EE88024D61501D3B79AE5D1AFD521E72499F325F6B0B82BE
SHA-512:	F2829518AE0F6DD35C1DE1175FC8BE3E52EDCAFAD0B2455AC593F5E5D4BD480B014F52C3AE24E742B914685513BE5DF862373E75C45BB7908C775D7E2E404D3
Malicious:	false
Reputation:	unknown
Preview:	Microsoft (R) .NET Framework Installation utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....Usage: InstallUtil [/u | /uninstall] [option [...]] assembly [[option [...]] assembly] [...]]....InstallUtil executes the installers in each given assembly...If the /u or /uninstall switch is specified, it uninstalls..the assemblies, otherwise it installs them. Unlike other..options, /u applies to all assemblies, regardless of where it..appears on the command line.....Installation is done in a transactioned way: If one of the..assemblies fails to install, the installations of all other..assemblies are rolled back. Uninstall is not transactioned.....Options take the form /switch=[value]. Any option that occurs..before the name of an assembly will apply to that assembly's..installation. Options are cumulative but overridable - options..specified for one assembly will apply to the next as well unless..the option is specified with a new value. The default for

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.683069808516563
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Quotation Request August RFQ8012021.exe

General

File size:	775168
MD5:	dd69f329393643aa570bd3a940323136
SHA1:	dbcb022f10c8cfcdd93a75253b9e20260f86dafe
SHA256:	9327c22d332141a7ee037b2d393e0ad352a2fc4f6dc9b7c f9c78155d70681e6b
SHA512:	836b07e9f14621179b2c5cd4fa7f778f41a51240ed25b5c 62a64d7f1b48b233fa972d6ca77a96b780d1f61251bef9f5 b982b694a02a359a55ad3dc2ec23dd0c8
SSDEEP:	12288:BLLLO6nlb8uYhkOH7aSV7B+AcitG07iLQSWmJ hbfvfkt:BPLRlb853uu7Bg0+LQSWP
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....PE..L..... 51....."...P..... .....@.. .....@..... ....` .....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4be70e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x31359EF3 [Thu Feb 29 12:41:23 1996 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	0xbc714	0xbc800	False	0.601980841761	data	6.69306847965	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc0000	0x64a	0x800	False	0.361328125	data	3.73777316937	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc2000	0xc	0x200	False	0.044921875	data	0.101910425663	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
Aug 2, 2021 08:43:57.933033943 CEST	192.168.2.4	8.8.8.8	0x1966	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Aug 2, 2021 08:44:34.640358925 CEST	192.168.2.4	8.8.8.8	0x11f5	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Aug 2, 2021 08:45:26.005337000 CEST	192.168.2.4	8.8.8.8	0x859c	Standard query (0)	dedicatedl ambo9.ddns.net	A (IP address)	IN (0x0001)
Aug 2, 2021 08:45:33.274184942 CEST	192.168.2.4	8.8.8.8	0xf875	Standard query (0)	dedicatedl ambo9.ddns.net	A (IP address)	IN (0x0001)
Aug 2, 2021 08:45:40.482608080 CEST	192.168.2.4	8.8.8.8	0x7744	Standard query (0)	dedicatedl ambo9.ddns.net	A (IP address)	IN (0x0001)
Aug 2, 2021 08:45:47.813150883 CEST	192.168.2.4	8.8.8.8	0xfa33	Standard query (0)	dedicatedl ambo9.ddns.net	A (IP address)	IN (0x0001)
Aug 2, 2021 08:45:54.743391991 CEST	192.168.2.4	8.8.8.8	0xd6ba	Standard query (0)	dedicatedl ambo9.ddns.net	A (IP address)	IN (0x0001)
Aug 2, 2021 08:46:00.841999054 CEST	192.168.2.4	8.8.8.8	0x9015	Standard query (0)	dedicatedl ambo9.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 2, 2021 08:43:57.960870981 CEST	8.8.8.8	192.168.2.4	0x1966	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)
Aug 2, 2021 08:44:34.666949987 CEST	8.8.8.8	192.168.2.4	0x11f5	No error (0)	www.google.com		172.217.168.68	A (IP address)	IN (0x0001)
Aug 2, 2021 08:45:26.040527105 CEST	8.8.8.8	192.168.2.4	0x859c	No error (0)	dedicatedl ambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)
Aug 2, 2021 08:45:33.311067104 CEST	8.8.8.8	192.168.2.4	0xf875	No error (0)	dedicatedl ambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)
Aug 2, 2021 08:45:40.515060902 CEST	8.8.8.8	192.168.2.4	0x7744	No error (0)	dedicatedl ambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)
Aug 2, 2021 08:45:47.848233938 CEST	8.8.8.8	192.168.2.4	0xfa33	No error (0)	dedicatedl ambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)
Aug 2, 2021 08:45:54.777112961 CEST	8.8.8.8	192.168.2.4	0xd6ba	No error (0)	dedicatedl ambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)
Aug 2, 2021 08:46:00.867130041 CEST	8.8.8.8	192.168.2.4	0x9015	No error (0)	dedicatedl ambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)

HTTPS Packets

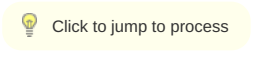
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Aug 2, 2021 08:43:58.095330000 CEST	172.217.168.68	443	192.168.2.4	49732	CN=www.google.com CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon Jun 28 06:12:58 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Sep 20 06:12:57 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		
Aug 2, 2021 08:44:34.812608957 CEST	172.217.168.68	443	192.168.2.4	49745	CN=www.google.com CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GTS CA 1C3, O=Google Trust Services LLC, C=US CN=GTS Root R1, O=Google Trust Services LLC, C=US CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Mon Jun 28 06:12:58 CEST 2021 Thu Aug 13 02:00:42 CEST 2020 Fri Jun 19 02:00:42 CEST 2020	Mon Sep 20 06:12:57 CEST 2021 Thu Sep 30 02:00:42 CEST 2027 Fri Jan 28 01:00:42 CET 2028	769,49162-49161-49172-49171-53-47-10,0-10-11-35-23-65281,29-23-24,0	54328bd36c14bd82ddaa0c04b25ed9ad
					CN=GTS CA 1C3, O=Google Trust Services LLC, C=US	CN=GTS Root R1, O=Google Trust Services LLC, C=US	Thu Aug 13 02:00:42 CEST 2020	Thu Sep 30 02:00:42 CEST 2027		
					CN=GTS Root R1, O=Google Trust Services LLC, C=US	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE	Fri Jun 19 02:00:42 CEST 2020	Fri Jan 28 01:00:42 CET 2028		

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Quotation Request August RFQ8012021.exe PID: 6640 Parent PID: 5776

General

Start time:	08:43:55
Start date:	02/08/2021
Path:	C:\Users\user\Desktop\Quotation Request August RFQ8012021.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Quotation Request August RFQ8012021.exe'
Imagebase:	0x450000
File size:	775168 bytes
MD5 hash:	DD69F329393643AA570BD3A940323136
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: 00000000.00000002.739331027.0000000003B17000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.739331027.0000000003B17000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.739331027.0000000003B17000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.739152820.00000000039B9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.739152820.00000000039B9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.739152820.00000000039B9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 7156 Parent PID: 6640

General

Start time:	08:44:14
Start date:	02/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon' /f /v 'Shell' /t REG_SZ /d 'explorer.exe,C:\Users\user\AppData\Roaming\MainProc.exe,'
Imagebase:	0x11d0000
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

Show Windows behavior

Analysis Process: conhost.exe PID: 7164 Parent PID: 7156

General

General

Start time:	08:44:15
Start date:	02/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: reg.exe PID: 5868 Parent PID: 7156

General

Start time:	08:44:16
Start date:	02/08/2021
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD 'HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon' /f /v 'Shell' /t REG_SZ /d 'explorer.exe,C:\Users\user\AppData\Roaming\MainProc.exe,'
Imagebase:	0x1320000
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

Show Windows behavior

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: MainProc.exe PID: 6288 Parent PID: 6640

General

Start time:	08:44:33
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Roaming\MainProc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\MainProc.exe'
Imagebase:	0x200000
File size:	775168 bytes
MD5 hash:	DD69F329393643AA570BD3A940323136
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.941301528.0000000003797000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.941301528.0000000003797000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.941301528.0000000003797000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 15%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Analysis Process: InstallUtil.exe PID: 5880 Parent PID: 6288

General

Start time:	08:44:59
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Imagebase:	0xc60000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: NanoCore, Description: unknown, Source: 00000012.00000002.933931703.000000000407E000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.920030285.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.920030285.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.920030285.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.944192934.0000000007E20000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.944192934.0000000007E20000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.944407587.0000000007E90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.944407587.0000000007E90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.944029550.0000000007DC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.944029550.0000000007DC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.941935265.00000000061A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.941935265.00000000061A0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.941935265.00000000061A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.944158898.0000000007E10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.944158898.0000000007E10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.944132813.0000000007E00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.944132813.0000000007E00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.943444482.00000000074C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.943444482.00000000074C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.944269292.0000000007E50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.944269292.0000000007E50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.942229491.0000000006570000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.942229491.0000000006570000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.941578983.0000000005870000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.941578983.0000000005870000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.944075779.0000000007DE0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.944075779.0000000007DE0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.944247779.0000000007E40000.00000004.00000001.sdmp, Author: Florian Roth
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: smss.exe PID: 5460 Parent PID: 6288

General

Start time:	08:45:07
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Local\Temp\smss.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\smss.exe'
Imagebase:	0x1e0000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 14%, Metadefender, Browse • Detection: 13%, ReversingLabs
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: smss.exe PID: 5908 Parent PID: 5460

General

Start time:	08:45:11
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Local\Temp\smss.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\smss.exe'
Imagebase:	0x220000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

Analysis Process: smss.exe PID: 6752 Parent PID: 6288

General

Start time:	08:45:15
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Local\Temp\smss.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\smss.exe'
Imagebase:	0x780000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: smss.exe PID: 5772 Parent PID: 6752

General

Start time:	08:45:17
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Local\Temp\smss.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\smss.exe'
Imagebase:	0x270000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: dhcpmon.exe PID: 2928 Parent PID: 3424

General

Start time:	08:45:17
Start date:	02/08/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xb70000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: conhost.exe PID: 2224 Parent PID: 2928

General

Start time:	08:45:18
Start date:	02/08/2021

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: smss.exe PID: 5032 Parent PID: 6288

General

Start time:	08:45:22
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Local\Temp\smss.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\smss.exe'
Imagebase:	0xf30000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: smss.exe PID: 6904 Parent PID: 5032

General

Start time:	08:45:26
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Local\Temp\smss.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\smss.exe'
Imagebase:	0x350000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: smss.exe PID: 1664 Parent PID: 6288

General

Start time:	08:45:32
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Local\Temp\smss.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\smss.exe'
Imagebase:	0x460000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: smss.exe PID: 4928 Parent PID: 1664

General

Start time:	08:45:36
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Local\Temp\smss.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\smss.exe'
Imagebase:	0xf50000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: smss.exe PID: 6196 Parent PID: 6288

General

Start time:	08:45:41
Start date:	02/08/2021
Path:	C:\Users\user\AppData\Local\Temp\smss.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\smss.exe'
Imagebase:	0x500000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Disassembly

Code Analysis