ID: 451100
Sample Name: RFQ 10 UNIT.exe
Cookbook: default.jbs
Time: 08:30:30
Date: 20/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report RFQ 10 UNIT.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: NanoCore 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 6
Sigma Overview 6
AV Detection: 7
E-Banking Fraud: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Jbx Signature Overview 7
AV Detection: 7
Networking: 7
E-Banking Fraud: 7
System Summary: 7
Data Obfuscation: 7
Hooking and other Techniques for Hiding and Protection: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 8
Remote Access Functionality: 8
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
Contacted IPs 11
Public 11
General Information 11
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASN 12
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
Static File Info 15
General 16
File Icon 16
Static PE Info 16
General 16
Entrypoint Preview 16
Data Directories 16
Sections 16
Resources 17
Imports 17
Version Infos 17
Network Behavior 17
Network Port Distribution 17
TCP Packets 17
UDP Packets 17
DNS Queries 17
DNS Answers 17
Code Manipulations 18
Statistics 18
Behavior 18

System Behavior 18
Analysis Process: RFQ 10 UNIT.exe PID: 3096 Parent PID: 5556 18
General 18
File Activities 18
File Created 18
File Written 18
File Read 18
Analysis Process: RFQ 10 UNIT.exe PID: 4572 Parent PID: 3096 18
General 19
Analysis Process: RFQ 10 UNIT.exe PID: 1540 Parent PID: 3096 19
General 19
File Activities 19
File Created 19
File Deleted 19
File Written 19
File Read 19
Registry Activities 19
Key Value Created 19
Analysis Process: dhcpmon.exe PID: 4076 Parent PID: 3388 19
General 20
File Activities 20
File Created 20
File Written 20
File Read 20
Analysis Process: dhcpmon.exe PID: 1396 Parent PID: 4076 20
General 20
File Activities 20
File Created 20
File Read 20
Disassembly 20
Code Analysis 20

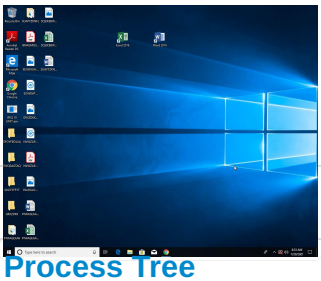
Windows Analysis Report RFQ 10 UNIT.exe

Overview

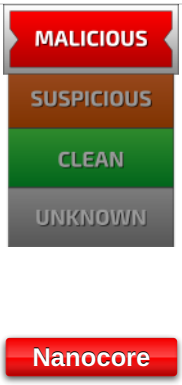
General Information

Sample Name:	RFQ 10 UNIT.exe
Analysis ID:	451100
MD5:	97904d814bcda6..
SHA1:	6ce40705c8de4e..
SHA256:	d4a810dc5c1bf6c..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



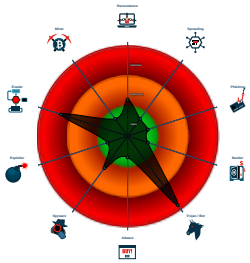
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…

Classification



Process Tree

- **System is w10x64**
- RFQ 10 UNIT.exe (PID: 3096 cmdline: 'C:\Users\user\Desktop\RFQ 10 UNIT.exe' MD5: 97904D814BCDA66EFE2D278EF92DA65F)
  - RFQ 10 UNIT.exe (PID: 4572 cmdline: C:\Users\user\Desktop\RFQ 10 UNIT.exe MD5: 97904D814BCDA66EFE2D278EF92DA65F)
  - RFQ 10 UNIT.exe (PID: 1540 cmdline: C:\Users\user\Desktop\RFQ 10 UNIT.exe MD5: 97904D814BCDA66EFE2D278EF92DA65F)
- dhcpmon.exe (PID: 4076 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 97904D814BCDA66EFE2D278EF92DA65F)
  - dhcpmon.exe (PID: 1396 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 97904D814BCDA66EFE2D278EF92DA65F)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "c9622013-90b3-4810-9b2a-2fbba172",
  "Domain1": "185.140.53.253",
  "Domain2": "dedicatedlambo9.ddns.net",
  "Port": 1604,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000018.00000002.401016722.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000018.00000002.401016722.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000018.00000002.401016722.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
00000008.00000002.485058731.000000000449000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000002.485186935.00000000044C0000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	0xb4357:$a: NanoCore 0xb437c:$a: NanoCore 0xb43d5:$a: NanoCore 0xc4574:$a: NanoCore 0xc459a:$a: NanoCore 0xc45f6:$a: NanoCore 0xd144d:$a: NanoCore 0xd14a6:$a: NanoCore 0xd14d9:$a: NanoCore 0xd1705:$a: NanoCore 0xd1781:$a: NanoCore 0xd1d9a:$a: NanoCore 0xd1ee3:$a: NanoCore 0xd23b7:$a: NanoCore 0xd269e:$a: NanoCore 0xd26b5:$a: NanoCore 0xdb559:$a: NanoCore 0xdb5d5:$a: NanoCore 0xddeb8:$a: NanoCore 0xe3481:$a: NanoCore 0xe34fb:$a: NanoCore
Click to see the 3 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.RFQ 10 UNIT.exe.476b80e.12.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	0x3d99:$x1: NanoCore.ClientPluginHost 0xcd3b:$x1: NanoCore.ClientPluginHost 0x3db3:$x2: IClientNetworkHost 0xcd55:$x2: IClientNetworkHost
8.2.RFQ 10 UNIT.exe.476b80e.12.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	0x3d99:$x2: NanoCore.ClientPluginHost 0xcd3b:$x2: NanoCore.ClientPluginHost 0x4dce:$s4: PipeCreated 0x3d86:$s5: IClientLoggingHost 0xcd28:$s5: IClientLoggingHost
8.2.RFQ 10 UNIT.exe.3466204.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	0x8ba5:$x1: NanoCore.ClientPluginHost 0x15d1f:$x1: NanoCore.ClientPluginHost 0x1fb7f:$x1: NanoCore.ClientPluginHost 0x27ab5:$x1: NanoCore.ClientPluginHost 0x2da98:$x1: NanoCore.ClientPluginHost 0x37513:$x1: NanoCore.ClientPluginHost 0x4194f:$x1: NanoCore.ClientPluginHost 0x4c941:$x1: NanoCore.ClientPluginHost 0x586f7:$x1: NanoCore.ClientPluginHost 0x6444e:$x1: NanoCore.ClientPluginHost 0x8bd2:$x2: IClientNetworkHost 0x15d58:$x2: IClientNetworkHost 0x1fbb8:$x2: IClientNetworkHost 0x27aee:$x2: IClientNetworkHost 0x37670:$x2: IClientNetworkHost 0x41988:$x2: IClientNetworkHost 0x4c95b:$x2: IClientNetworkHost 0x58711:$x2: IClientNetworkHost 0x6448b:$x2: IClientNetworkHost
8.2.RFQ 10 UNIT.exe.3466204.4.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	0x8b7f:$a: NanoCore 0x8ba5:$a: NanoCore 0x8c01:$a: NanoCore 0x15a67:$a: NanoCore 0x15ac0:$a: NanoCore 0x15af3:$a: NanoCore 0x15d1f:$a: NanoCore 0x15d9b:$a: NanoCore 0x163b4:$a: NanoCore 0x164fd:$a: NanoCore 0x169d1:$a: NanoCore 0x16cb8:$a: NanoCore 0x16ccf:$a: NanoCore 0x1fb7f:$a: NanoCore 0x1fbfb:$a: NanoCore 0x224de:$a: NanoCore 0x27ab5:$a: NanoCore 0x27b2f:$a: NanoCore 0x2da98:$a: NanoCore 0x2dae2:$a: NanoCore 0x2e73c:$a: NanoCore
8.2.RFQ 10 UNIT.exe.456f7c1.8.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	0x2dbb:$x1: NanoCore.ClientPluginHost 0x2de5:$x2: IClientNetworkHost
Click to see the 69 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

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:

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

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:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

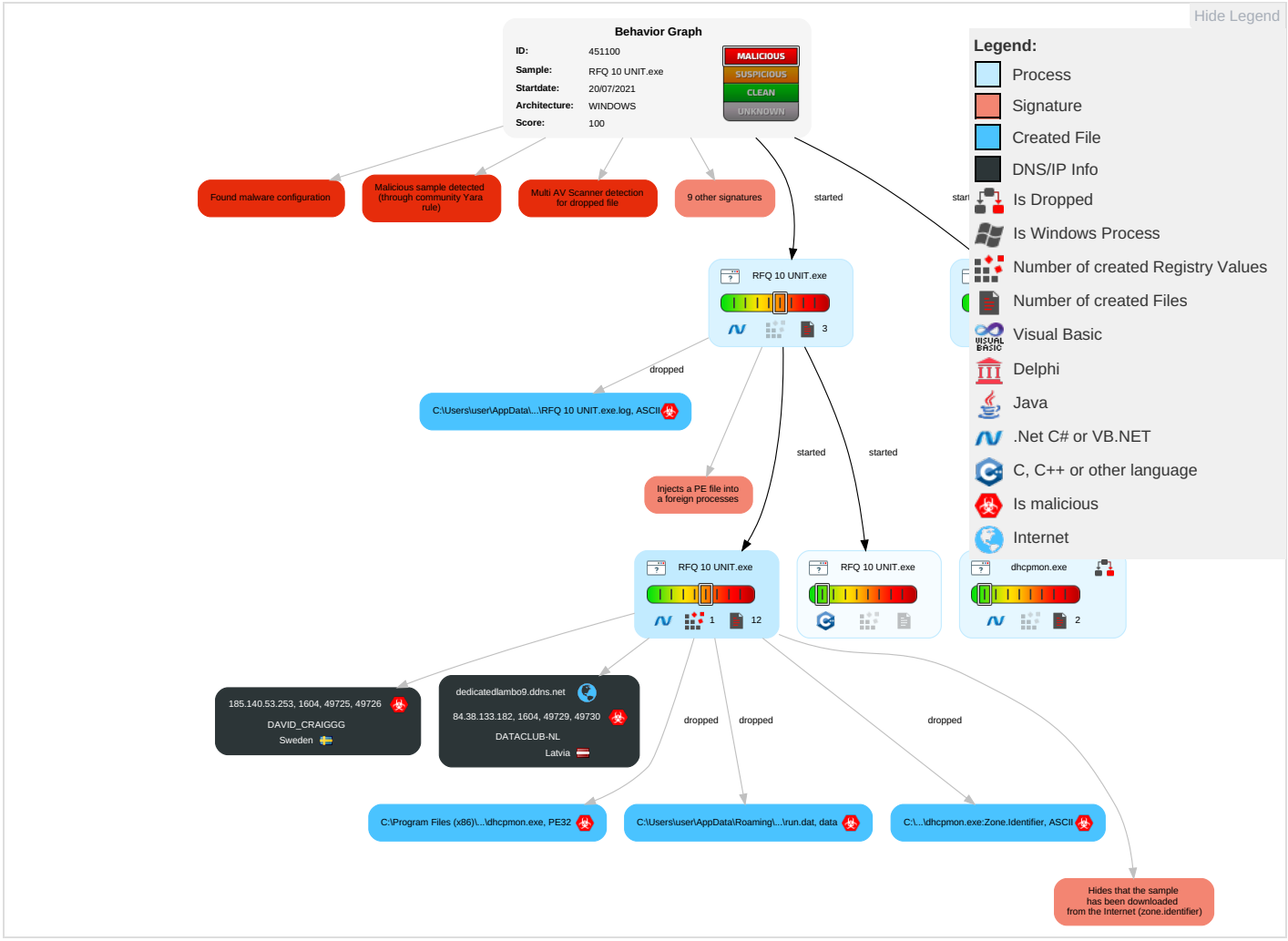
Detected Nanocore Rat

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
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 1 1 2	Masquerading 2	Input Capture 1 1	Query Registry 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 1 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Timestomp 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

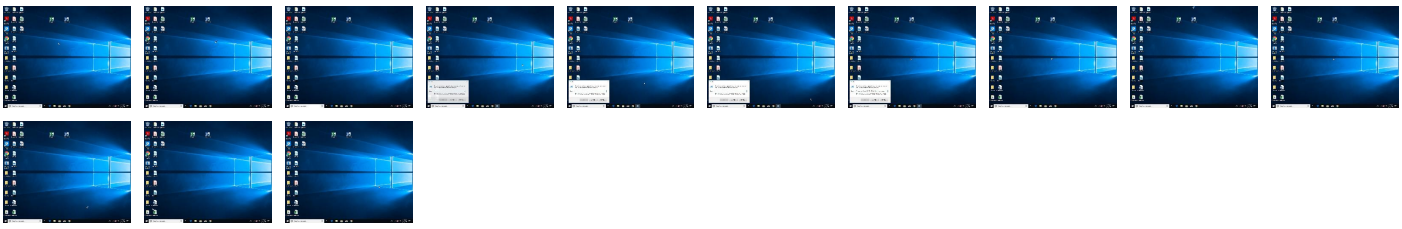
Behavior Graph



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
RFQ 10 UNIT.exe	20%	ReversingLabs	Win32.Trojan.AgentTesla	
RFQ 10 UNIT.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	20%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.RFQ 10 UNIT.exe.4438a40.6.unpack	100%	Avira	TR/NanoCore.fadte		Download File
8.2.RFQ 10 UNIT.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
24.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
dedicatedlambo9.ddns.net	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.fonts.comic	0%	URL Reputation	safe	
http://www.founder.com.cn/cnayov	0%	Avira URL Cloud	safe	
http://www.fonts.comcJ	0%	Avira URL Cloud	safe	
185.140.53.253	0%	Avira URL Cloud	safe	
http://www.tiro.comA	0%	Avira URL Cloud	safe	
http://www.fonts.comc(	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dedicatedlambo9.ddns.net	84.38.133.182	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
dedicatedlambo9.ddns.net	true	• Avira URL Cloud: safe	unknown
185.140.53.253	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
84.38.133.182	dedicatedlambo9.ddns.net	Latvia		203557	DATACLUB-NL	true
185.140.53.253	unknown	Sweden		209623	DAVID_CRAIGGG	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	451100
Start date:	20.07.2021
Start time:	08:30:30
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RFQ 10 UNIT.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:	28
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@8/8@12/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
08:31:49	API Interceptor	792x Sleep call for process: RFQ 10 UNIT.exe modified
08:31:56	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
08:32:40	API Interceptor	1x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.140.53.253	NEWORDERrefno0992883jpg.exe	Get hash	malicious	Browse	
	CompanyLicense.exe	Get hash	malicious	Browse	
	16Product Specifications list -Order PCT1086586 1st Video.exe	Get hash	malicious	Browse	
	15Order PCT1086586 - Project Commercial Conditions.exe	Get hash	malicious	Browse	
	58Product Specifications list -Order PCT1086586 1st Video.exe	Get hash	malicious	Browse	
	57Order PCT1086586 - Project Commercial Conditions.exe	Get hash	malicious	Browse	
	15Product Specifications list -Order PCT1086586 1st Video.exe	Get hash	malicious	Browse	
	14Order PCT1086586 - Project Commercial Conditions.exe	Get hash	malicious	Browse	
	57Product Specifications list -Order PCT1086586 1st Video.exe	Get hash	malicious	Browse	
	56Order PCT1086586 - Project Commercial Conditions.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	A2CGhuioKe.exe	Get hash	malicious	Browse	• 185.244.30.28
	0kEuVjiCbh.exe	Get hash	malicious	Browse	• 185.244.30.28
	RFQ_Order WT013 - A11197322,pdf.exe	Get hash	malicious	Browse	• 185.244.30.18
	ORDER.exe	Get hash	malicious	Browse	• 185.140.53.132
	DHL_119040 receipt document,pdf.exe	Get hash	malicious	Browse	• 185.244.30.18
	Img 673t5718737.exe	Get hash	malicious	Browse	• 91.193.75.202

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Parts_Enquiry_450kr6CRT.vbs	Get hash	malicious	Browse	• 185.140.53.169
	Itemsreceipt975432907.exe	Get hash	malicious	Browse	• 185.244.30.19
	H194 #U5146#U57fa - Payment.exe	Get hash	malicious	Browse	• 185.140.53.135
	Parts-Enquiry_OYU08W0VCWRDLPA.vbs	Get hash	malicious	Browse	• 185.140.53.169
	OneDrive.exe	Get hash	malicious	Browse	• 185.140.53.194
	CVhssiltQ9.exe	Get hash	malicious	Browse	• 185.140.53.9
	rz89FRwKvB.exe	Get hash	malicious	Browse	• 185.244.30.92
	doc030WA0004-55YH701-75IMG0012.exe	Get hash	malicious	Browse	• 185.140.53.230
	Request For Quotation.xlsx	Get hash	malicious	Browse	• 185.140.53.154
	CV CREDENTIALS.exe	Get hash	malicious	Browse	• 185.140.53.8
	ARRIVAL NOTICEPDF.EXCL.exe	Get hash	malicious	Browse	• 185.140.53.142
	WeASwOPOdNuVKbq.exe	Get hash	malicious	Browse	• 185.140.53.8
	New Order# 11009947810.exe	Get hash	malicious	Browse	• 185.140.53.216
	vEJ2Mfxn6p.exe	Get hash	malicious	Browse	• 185.140.53.134
DATACLUB-NL	FacebookSecurityUpdate.exe	Get hash	malicious	Browse	• 84.38.133.101
	v1hBv6A71M.exe	Get hash	malicious	Browse	• 84.38.133.24
	Standardequips_Quote.ppt	Get hash	malicious	Browse	• 185.29.11.15
	XsNgUDFxLw.exe	Get hash	malicious	Browse	• 84.38.133.117
	18Order.exe	Get hash	malicious	Browse	• 185.29.11.103
	56New Order oct 2018230090.exe	Get hash	malicious	Browse	• 185.29.11.103

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\RFQ 10 UNIT.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1098240
Entropy (8bit):	7.622687617903329
Encrypted:	false
SSDEEP:	24576:+bnQK7ECKrvDBI1/jUHsvoCzA+7ZAkwVileDd2A0iM3/4UF+voC:DBW1/aunlikidX0iM3/pmd
MD5:	97904D814BCDA66EFE2D278EF92DA65F
SHA1:	6CE40705C8DE4E3C8EFB1857DEB76357AC500DF7
SHA-256:	D4A810DC5C1BF6CFCEDAF05D46A9230250CE314CC19082CA044763DCD9FF7135
SHA-512:	ADB1CCA1A4ED550CE3B0339CB60ECDC22EFB2A7EA3315137CFA31934C73DCAC9E61308D9E964C6F187E55496439E0D26582E26ADCC519D6ABDEEF7DA1A9F F4C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 20%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....P..... .....@.. ....@.....P...O.....4..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....\|\|.....l...<.....0.....(....(.....(.....o!....*.....("......(#.....($.....(%.....(&....*N..(....o....('....*&..((. ...*.s).....s*.....s+.....s,.....s-.....*....0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*&..(3....*...0..<.....~..... (4.....,!r...p.....(5...o6...s7.....~.....

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\RFQ 10 UNIT.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

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
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 10 UNIT.exe.log	
Process:	C:\Users\user\Desktop\RFQ 10 UNIT.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=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:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\RFQ 10 UNIT.exe
File Type:	data
Category:	dropped
Size (bytes):	1624
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrw8:flC0IlC0IlC0IlC0IlC0IlC0IlC08
MD5:	0D79388CEC6619D612C2088173BB6741
SHA1:	8A312E3198009C545D0CF3254572189D29A03EA7
SHA-256:	D7D423B23D932E306F3CCB2F7A984B7036A042C007A43FD655C6B57B960BB8DF

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
SHA-512:	53BB3E9263DFD746E7E8159466E220E6EC9D81E9D3F0E1D191E09CD511B7EB93B0BA65D13CE0C97C652ECD0F69BB991E6B1840F961BC65003C4DD7AA93EED 13
Malicious:	false
Reputation:	moderate, very likely benign file
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\Desktop\RFQ 10 UNIT.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:b+:S
MD5:	2E61B957E818BFB06D029DFFAD9186CA
SHA1:	D4950C122F3C8F85DECC2A8EAF4A7307F6E0EBB9
SHA-256:	5686B94B5CE4C8B0D3A479A2856CE1AAFFAEF5B3A75901F45F530470031F1090
SHA-512:	EE64E72026088B64B7BC7BFAF152D261E23A1F76EC9517B4C4103332AA3FBE836BFC110183F70F6412E6A5B8221EF56D4D0793FADCA4DC0DC00B4829EC36616 D
Malicious:	**true**
Preview:	.....K.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\RFQ 10 UNIT.exe
File Type:	data
Category:	modified
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671E CB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\RFQ 10 UNIT.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
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..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n._+.e.d'..}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.Ql..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.|i4...i...;O...n.?.,. ....v?.5}.OY@.dG|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..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.....I..o...u1..8i=.z.W..7

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.622687617903329
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:	RFQ 10 UNIT.exe
File size:	1098240
MD5:	97904d814bcda66efe2d278ef92da65f
SHA1:	6ce40705c8de4e3c8efb1857deb76357ac500df7
SHA256:	d4a810dc5c1bf6cfcedaf05d46a9230250ce314cc19082ca044763dcd9ff7135
SHA512:	adb1cca1a4ed550ce3b0339cb60ecdc22efb2a7ea3315137cfa31934c73dcac9e61308d9e964c6f187e55496439e0d26582e26adcc519d6abdeef7da1a9f8f4c
SSDEEP:	24576:+bnQK7ECKrvDBI1/jUHsvoCzA+7ZAkwVileDd2A0iM3/4UF+voC:DBW1/aunlikidX0iM3/pmd
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....P..... .....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x50d9a2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xBA9DB0CD [Tue Mar 19 05:29:49 2069 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	0x10b9a8	0x10ba00	False	0.76949658454	data	7.62768729612	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x10e000	0x3a8	0x400	False	0.3779296875	data	2.93439777021	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x110000	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
Jul 20, 2021 08:32:10.239372015 CEST	192.168.2.3	8.8.8.8	0xf5e8	Standard query (0)	dedicatedl ambo9.ddns.net	A (IP address)	IN (0x0001)
Jul 20, 2021 08:32:16.790425062 CEST	192.168.2.3	8.8.8.8	0xda52	Standard query (0)	dedicatedl ambo9.ddns.net	A (IP address)	IN (0x0001)
Jul 20, 2021 08:32:23.156908989 CEST	192.168.2.3	8.8.8.8	0x2592	Standard query (0)	dedicatedl ambo9.ddns.net	A (IP address)	IN (0x0001)
Jul 20, 2021 08:32:30.050033092 CEST	192.168.2.3	8.8.8.8	0xe404	Standard query (0)	dedicatedl ambo9.ddns.net	A (IP address)	IN (0x0001)
Jul 20, 2021 08:32:36.270360947 CEST	192.168.2.3	8.8.8.8	0x798a	Standard query (0)	dedicatedl ambo9.ddns.net	A (IP address)	IN (0x0001)
Jul 20, 2021 08:32:43.285545111 CEST	192.168.2.3	8.8.8.8	0xba51	Standard query (0)	dedicatedl ambo9.ddns.net	A (IP address)	IN (0x0001)
Jul 20, 2021 08:32:51.645318031 CEST	192.168.2.3	8.8.8.8	0xc6d4	Standard query (0)	dedicatedl ambo9.ddns.net	A (IP address)	IN (0x0001)
Jul 20, 2021 08:32:57.678112984 CEST	192.168.2.3	8.8.8.8	0x1088	Standard query (0)	dedicatedl ambo9.ddns.net	A (IP address)	IN (0x0001)
Jul 20, 2021 08:33:04.925019026 CEST	192.168.2.3	8.8.8.8	0xc933	Standard query (0)	dedicatedl ambo9.ddns.net	A (IP address)	IN (0x0001)
Jul 20, 2021 08:33:11.913871050 CEST	192.168.2.3	8.8.8.8	0x2465	Standard query (0)	dedicatedl ambo9.ddns.net	A (IP address)	IN (0x0001)
Jul 20, 2021 08:33:18.958626032 CEST	192.168.2.3	8.8.8.8	0x9d36	Standard query (0)	dedicatedl ambo9.ddns.net	A (IP address)	IN (0x0001)
Jul 20, 2021 08:33:25.125401020 CEST	192.168.2.3	8.8.8.8	0x7b7a	Standard query (0)	dedicatedl ambo9.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

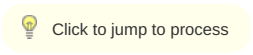
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 20, 2021 08:32:10.301805019 CEST	8.8.8.8	192.168.2.3	0xf5e8	No error (0)	dedicatedl ambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)
Jul 20, 2021 08:32:16.850102901 CEST	8.8.8.8	192.168.2.3	0xda52	No error (0)	dedicatedl ambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)
Jul 20, 2021 08:32:23.218106031 CEST	8.8.8.8	192.168.2.3	0x2592	No error (0)	dedicatedl ambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)
Jul 20, 2021 08:32:30.106918097 CEST	8.8.8.8	192.168.2.3	0xe404	No error (0)	dedicatedl ambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)
Jul 20, 2021 08:32:36.328798056 CEST	8.8.8.8	192.168.2.3	0x798a	No error (0)	dedicatedl ambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)
Jul 20, 2021 08:32:43.346647978 CEST	8.8.8.8	192.168.2.3	0xba51	No error (0)	dedicatedl ambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)
Jul 20, 2021 08:32:51.704998970 CEST	8.8.8.8	192.168.2.3	0xc6d4	No error (0)	dedicatedl ambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 20, 2021 08:32:57.735357046 CEST	8.8.8.8	192.168.2.3	0x1088	No error (0)	dedicatedlambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)
Jul 20, 2021 08:33:04.985399008 CEST	8.8.8.8	192.168.2.3	0xc933	No error (0)	dedicatedlambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)
Jul 20, 2021 08:33:11.963673115 CEST	8.8.8.8	192.168.2.3	0x2465	No error (0)	dedicatedlambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)
Jul 20, 2021 08:33:19.011656046 CEST	8.8.8.8	192.168.2.3	0x9d36	No error (0)	dedicatedlambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)
Jul 20, 2021 08:33:25.185560942 CEST	8.8.8.8	192.168.2.3	0x7b7a	No error (0)	dedicatedlambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: RFQ 10 UNIT.exe PID: 3096 Parent PID: 5556

General

Start time:	08:31:22
Start date:	20/07/2021
Path:	C:\Users\user\Desktop\RFQ 10 UNIT.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RFQ 10 UNIT.exe'
Imagebase:	0x4a0000
File size:	1098240 bytes
MD5 hash:	97904D814BCDA66EFE2D278EF92DA65F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: RFQ 10 UNIT.exe PID: 4572 Parent PID: 3096

General

Start time:	08:31:50
Start date:	20/07/2021
Path:	C:\Users\user\Desktop\RFQ 10 UNIT.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\RFQ 10 UNIT.exe
Imagebase:	0x370000
File size:	1098240 bytes
MD5 hash:	97904D814BCDA66EFE2D278EF92DA65F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: RFQ 10 UNIT.exe PID: 1540 Parent PID: 3096

General

Start time:	08:31:51
Start date:	20/07/2021
Path:	C:\Users\user\Desktop\RFQ 10 UNIT.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\RFQ 10 UNIT.exe
Imagebase:	0xe70000
File size:	1098240 bytes
MD5 hash:	97904D814BCDA66EFE2D278EF92DA65F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.485058731.0000000004419000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.485186935.00000000044C0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.485635523.0000000004706000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.485779990.00000000047F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.485779990.00000000047F1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: dhcpmon.exe PID: 4076 Parent PID: 3388

General

Start time:	08:32:05
Start date:	20/07/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x2e0000
File size:	1098240 bytes
MD5 hash:	97904D814BCDA66EFE2D278EF92DA65F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 20%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: dhcpmon.exe PID: 1396 Parent PID: 4076

General

Start time:	08:32:41
Start date:	20/07/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0xc30000
File size:	1098240 bytes
MD5 hash:	97904D814BCDA66EFE2D278EF92DA65F
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: 00000018.00000002.401016722.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.401016722.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.401016722.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis