

ID: 432802
Sample Name: 7lQnHeq3XF
Cookbook: default.jbs
Time: 19:03:07
Date: 10/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report 7lQnHeq3XF 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: 6
E-Banking Fraud: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Signature Overview 6
AV Detection: 7
Networking: 7
E-Banking Fraud: 7
System Summary: 7
Data Obfuscation: 7
Boot Survival: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
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 11
URLs 11
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 12
Contacted IPs 13
Public 13
Private 13
General Information 13
Simulations 13
Behavior and APIs 13
Joe Sandbox View / Context 14
IPs 14
Domains 14
ASN 14
JA3 Fingerprints 14
Dropped Files 14
Created / dropped Files 14
Static File Info 17
General 17
File Icon 17
Static PE Info 17
General 17
Entrypoint Preview 18
Data Directories 18
Sections 18
Resources 18
Imports 18
Version Infos 18
Network Behavior 18
Network Port Distribution 18
TCP Packets 18
Code Manipulations 18
Statistics 18
Behavior 18

Copyright Joe Security LLC 2021

System Behavior 18
Analysis Process: 7lQnHeq3XF.exe PID: 5360 Parent PID: 5840 18
General 18
File Activities 19
File Created 19
File Deleted 19
File Written 19
File Read 19
Analysis Process: schtasks.exe PID: 3688 Parent PID: 5360 19
General 19
File Activities 19
File Read 19
Analysis Process: conhost.exe PID: 4128 Parent PID: 3688 19
General 19
Analysis Process: 7lQnHeq3XF.exe PID: 784 Parent PID: 5360 20
General 20
File Activities 21
File Created 21
File Deleted 21
File Written 21
File Read 21
Analysis Process: schtasks.exe PID: 3032 Parent PID: 784 21
General 21
File Activities 22
File Read 22
Analysis Process: conhost.exe PID: 4280 Parent PID: 3032 22
General 22
Analysis Process: 7lQnHeq3XF.exe PID: 3088 Parent PID: 528 22
General 22
File Activities 23
File Created 23
File Deleted 23
File Written 23
File Read 23
Analysis Process: schtasks.exe PID: 5336 Parent PID: 3088 23
General 23
File Activities 23
File Read 23
Analysis Process: conhost.exe PID: 5568 Parent PID: 5336 23
General 23
Analysis Process: 7lQnHeq3XF.exe PID: 3508 Parent PID: 3088 23
General 23
Analysis Process: 7lQnHeq3XF.exe PID: 576 Parent PID: 3088 24
General 24
File Activities 24
File Created 24
File Read 24
Disassembly 25
Code Analysis 25

Copyright Joe Security LLC 2021

Analysis Report 7lQnHeq3XF

Overview

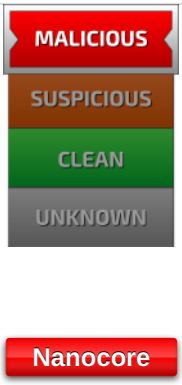
General Information

Sample Name:	7lQnHeq3XF (renamed file extension from none to exe)
Analysis ID:	432802
MD5:	9750dee05b47f07.
SHA1:	95f456ae508245b.
SHA256:	eea0f064af6e7b6..
Tags:	exe NanoCore trojan
Infos:	

Most interesting Screenshot:



Detection

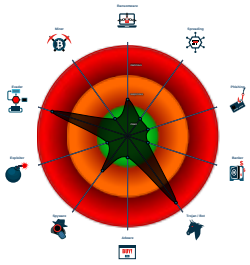


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…

Classification



- **System is w10x64**
- 7lQnHeq3XF.exe (PID: 5360 cmdline: 'C:\Users\user\Desktop\7lQnHeq3XF.exe' MD5: 9750DEE05B47F072E5975895DCF61AE5)
  - schtasks.exe (PID: 3688 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\CLJgKpOuw' /XML 'C:\Users\user\AppData\Local\Temp\tmp6F2E.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4128 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 7lQnHeq3XF.exe (PID: 784 cmdline: {path} MD5: 9750DEE05B47F072E5975895DCF61AE5)
    - schtasks.exe (PID: 3032 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp8362.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 4280 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- 7lQnHeq3XF.exe (PID: 3088 cmdline: C:\Users\user\Desktop\7lQnHeq3XF.exe 0 MD5: 9750DEE05B47F072E5975895DCF61AE5)
  - schtasks.exe (PID: 5336 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\CLJgKpOuw' /XML 'C:\Users\user\AppData\Local\Temp\tmp1E69.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5568 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 7lQnHeq3XF.exe (PID: 3508 cmdline: {path} MD5: 9750DEE05B47F072E5975895DCF61AE5)
  - 7lQnHeq3XF.exe (PID: 576 cmdline: {path} MD5: 9750DEE05B47F072E5975895DCF61AE5)
- **cleanup**

Malware Configuration

Threatname: NanoCore

Copyright Joe Security LLC 2021

```
{
  "Version": "1.2.2.0",
  "Mutex": "6ceec185-c99e-4d5c-8685-49487283",
  "Group": "Guage12",
  "Domain1": "185.136.169.24",
  "Domain2": "127.0.0.1",
  "Port": 54984,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "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",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000018.00000002.410604962.0000000003CB9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000018.00000002.410604962.0000000003CB9000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x435b5:$a: NanoCore • 0x4360e:$a: NanoCore • 0x4364b:$a: NanoCore • 0x436c4:$a: NanoCore • 0x56d6f:$a: NanoCore • 0x56d84:$a: NanoCore • 0x56db9:$a: NanoCore • 0x6fd53:$a: NanoCore • 0x6fd68:$a: NanoCore • 0x6fd9d:$a: NanoCore • 0x43617:$b: ClientPlugin • 0x43654:$b: ClientPlugin • 0x43f52:$b: ClientPlugin • 0x43f5f:$b: ClientPlugin • 0x56b2b:$b: ClientPlugin • 0x56b46:$b: ClientPlugin • 0x56b76:$b: ClientPlugin • 0x56d8d:$b: ClientPlugin • 0x56dc2:$b: ClientPlugin • 0x6fb0f:$b: ClientPlugin • 0x6fb2a:$b: ClientPlugin
0000000C.00000002.476199801.000000000326 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000010.00000002.396832392.0000000003CE 6000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x94ff5:$x1: NanoCore.ClientPluginHost • 0x95032:$x2: IClientNetworkHost • 0x98b65:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000010.00000002.396832392.0000000003CE 6000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 52 entries				

Copyright Joe Security LLC 2021

Unpacked PEs

Source	Rule	Description	Author	Strings
24.2.7lQnHeq3XF.exe.3cfb7d6.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0x145e3:$x1: NanoCore.ClientPluginHost • 0x2d5c7:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost • 0x14610:$x2: IClientNetworkHost • 0x2d5f4:$x2: IClientNetworkHost
24.2.7lQnHeq3XF.exe.3cfb7d6.5.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x145e3:$x2: NanoCore.ClientPluginHost • 0x2d5c7:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0x156be:$s4: PipeCreated • 0x2e6a2:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost • 0x145fd:$s5: IClientLoggingHost • 0x2d5e1:$s5: IClientLoggingHost
24.2.7lQnHeq3XF.exe.3cfb7d6.5.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
24.2.7lQnHeq3XF.exe.3cfb7d6.5.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xddf:$a: NanoCore • 0xe38:$a: NanoCore • 0xe75:$a: NanoCore • 0xeee:$a: NanoCore • 0x14599:$a: NanoCore • 0x145ae:$a: NanoCore • 0x145e3:$a: NanoCore • 0x2d57d:$a: NanoCore • 0x2d592:$a: NanoCore • 0x2d5c7:$a: NanoCore • 0xe41:$b: ClientPlugin • 0xe7e:$b: ClientPlugin • 0x177c:$b: ClientPlugin • 0x1789:$b: ClientPlugin • 0x14355:$b: ClientPlugin • 0x14370:$b: ClientPlugin • 0x143a0:$b: ClientPlugin • 0x145b7:$b: ClientPlugin • 0x145ec:$b: ClientPlugin • 0x2d339:$b: ClientPlugin • 0x2d354:$b: ClientPlugin
12.2.7lQnHeq3XF.exe.5b90000.10.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
Click to see the 75 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

Signature Overview

Click to jump to signature section

Copyright Joe Security LLC 2021

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

E-Banking Fraud:



- Yara detected Nanocore RAT

System Summary:



- Malicious sample detected (through community Yara rule)
- .NET source code contains very large strings

Data Obfuscation:



- .NET source code contains potential unpacker

Boot Survival:



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

Hooking and other Techniques for Hiding and Protection:



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

Malware Analysis System Evasion:



- Yara detected AntiVM3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:



- Injects a PE file into a foreign processes

Stealing of Sensitive Information:



- Yara detected Nanocore RAT

Remote Access Functionality:

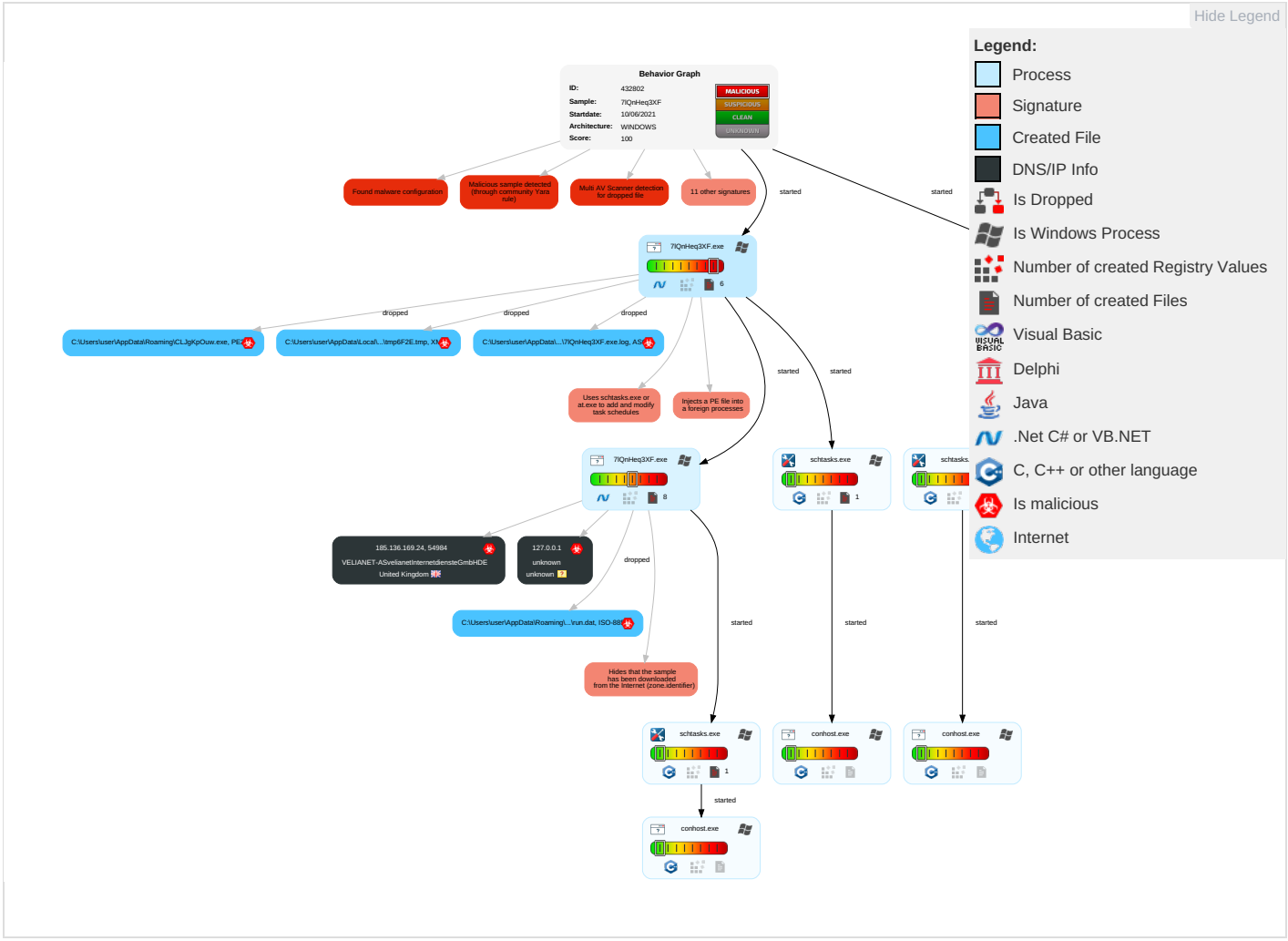


- Detected Nanocore Rat
- Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1	Input Capture 2 1	Security Software Discovery 2 1 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc

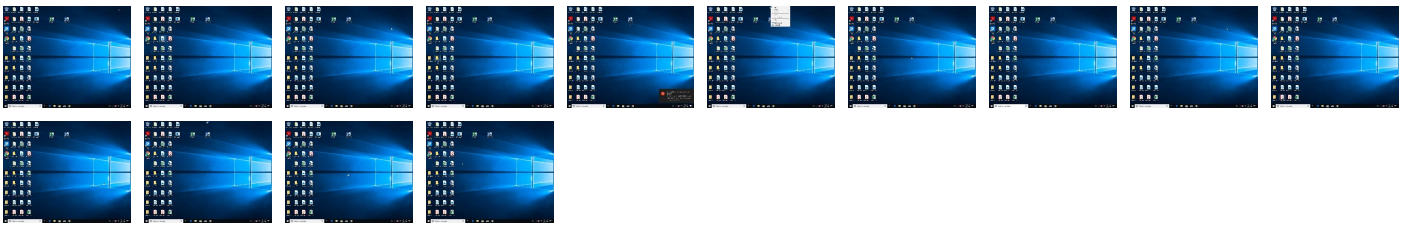
Behavior Graph



Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
7lQnHeq3XF.exe	74%	Virustotal		Browse
7lQnHeq3XF.exe	34%	Metadefender		Browse
7lQnHeq3XF.exe	79%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
7lQnHeq3XF.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\CLJgKpOuw.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\CLJgKpOuw.exe	34%	Metadefender		Browse
C:\Users\user\AppData\Roaming\CLJgKpOuw.exe	79%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
24.0.7lQnHeq3XF.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
24.0.7lQnHeq3XF.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.0.7lQnHeq3XF.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.2.7lQnHeq3XF.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link	Download
24.2.7lQnHeq3XF.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.0.7lQnHeq3XF.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
12.2.7lQnHeq3XF.exe.5b90000.10.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/lts	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/e%B	0%	Avira URL Cloud	safe	
http://www.fontbureau.comue6%	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/e%B	0%	Avira URL Cloud	safe	
http://www.fontbureau.comFA%	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/Z%K	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/l%y	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/~%g	0%	Avira URL Cloud	safe	
http://www.fontbureau.comTTF	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/8	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/8	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/8	0%	URL Reputation	safe	
http://www.fontbureau.com%	0%	Avira URL Cloud	safe	
185.136.169.24	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/%	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/%	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/%	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
127.0.0.1	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalsd	0%	URL Reputation	safe	
http://www.fontbureau.comalsd	0%	URL Reputation	safe	
http://www.fontbureau.comalsd	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/wa	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/vno	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Z%K	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp//%	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/~%g	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/H%	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/ge	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.fontbureau.comcom~%g	0%	Avira URL Cloud	safe	
http://www.fontbureau.comtuede%B	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.jiyu-kobo.co.jp/6%	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.fontbureau.comld%	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
185.136.169.24	true	• Avira URL Cloud: safe	unknown
127.0.0.1	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.136.169.24	unknown	United Kingdom		29066	VELIANET-ASvelianetInternetdiensteGmbHDE	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432802
Start date:	10.06.2021
Start time:	19:03:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	7lQnHeq3XF (renamed file extension from none to 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:	34
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@17/7@0/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0% (good quality ratio 0%) • Quality average: 80% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:04:41	API Interceptor	684x Sleep call for process: 7lQnHeq3XF.exe modified
19:04:42	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\7lQnHeq3XF.exe" s>$(Arg0)

Copyright Joe Security LLC 2021

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.136.169.24	41d0d4f9999b50bd9636508b7a247b04e6b919b8ed32d.exe	Get hash	malicious	Browse	
	cd933deed6ad151dbc88561ea55dc128b464843b481a4.exe	Get hash	malicious	Browse	
	Letter of Demand.doc	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VELIANET-ASvelianetInternetdiensteGmbHDE	pivaa.apk	Get hash	malicious	Browse	• 92.204.221.12
	Doc2000120201.xls	Get hash	malicious	Browse	• 185.136.169.163
	220bb2b7deba41f53a8d86d677691aff283314a29c27c.exe	Get hash	malicious	Browse	• 185.136.169.163
	Scan003.doc	Get hash	malicious	Browse	• 185.136.169.109
	cce53a67bb01a8f71b21fbdbf1b8a32345d81bbec12df.exe	Get hash	malicious	Browse	• 185.136.169.109
	RFQ#20053491.xlsx	Get hash	malicious	Browse	• 92.204.160.45
	no.IV640381 refer PO 4500260781.xlsx	Get hash	malicious	Browse	• 92.204.160.45
	Ultimate-File(1).docm	Get hash	malicious	Browse	• 134.119.181.142
	Ultimate-File(1).docm	Get hash	malicious	Browse	• 134.119.181.142
	AnyDesk (Sample).exe	Get hash	malicious	Browse	• 78.138.106.22
	41d0d4f9999b50bd9636508b7a247b04e6b919b8ed32d.exe	Get hash	malicious	Browse	• 185.136.169.24
	cd933deed6ad151dbc88561ea55dc128b464843b481a4.exe	Get hash	malicious	Browse	• 185.136.169.24
	Letter of Demand.doc	Get hash	malicious	Browse	• 185.136.169.24
	2bb0000.exe	Get hash	malicious	Browse	• 193.42.156.106
	RE New order.exe	Get hash	malicious	Browse	• 92.204.163.146
	AnyDeskCKS.exe	Get hash	malicious	Browse	• 185.136.157.77
	intercom.exe	Get hash	malicious	Browse	• 134.119.186.216
	gJvdHdeawX.exe	Get hash	malicious	Browse	• 134.119.186.216
	qbUoyUZWnC.exe	Get hash	malicious	Browse	• 185.136.169.155
	SecuriteInfo.com.Ransom.Stop.P6.19307.exe	Get hash	malicious	Browse	• 134.119.186.216

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\7lQnHeq3XF.exe.log

Process:	C:\Users\user\Desktop\7lQnHeq3XF.exe
File Type:	ASCII text, with CRLF line terminators

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\7lQnHeq3XF.exe.log	
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp1E69.tmp	
Process:	C:\Users\user\Desktop\7lQnHeq3XF.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.19196486799254
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBrtn:cbh47TlNQ//rydbz9I3YODOLNdq3v
MD5:	51C03E6FFF88EF349C81FF84C2F8F94B
SHA1:	34AE6BEAB2F34E7F754973D6FC23E4AD60A3EB64
SHA-256:	E37FD145922750F95C158B07866A9D73FD9D1B2DA67B9C9A478D7A4E35EF1089
SHA-512:	997EAF31A006EDBA09D98781F96482DA716CC5805BB5125965AB9525E22D10BE1C43B438AB5EF1B277CECE23B29CFA366EF70D02669C7A6518F10CF2C94FC7A F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmp6F2E.tmp	
Process:	C:\Users\user\Desktop\7lQnHeq3XF.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.19196486799254
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBrtn:cbh47TlNQ//rydbz9I3YODOLNdq3v
MD5:	51C03E6FFF88EF349C81FF84C2F8F94B
SHA1:	34AE6BEAB2F34E7F754973D6FC23E4AD60A3EB64
SHA-256:	E37FD145922750F95C158B07866A9D73FD9D1B2DA67B9C9A478D7A4E35EF1089
SHA-512:	997EAF31A006EDBA09D98781F96482DA716CC5805BB5125965AB9525E22D10BE1C43B438AB5EF1B277CECE23B29CFA366EF70D02669C7A6518F10CF2C94FC7A F
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmp8362.tmp	
Process:	C:\Users\user\Desktop\7lQnHeq3XF.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators

C:\Users\user\AppData\Local\Temp\tmp8362.tmp	
Category:	dropped
Size (bytes):	1300
Entropy (8bit):	5.123957763857257
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0TXxtn:cbk4oL600QydbQxIYODOLedq3IXj
MD5:	9EDDF2EE551487EBE6C93C2F40EA7CAB
SHA1:	43689EB449EECAC751976B4969F5BEF0585C7057
SHA-256:	25F651D7FD2035C121EF8893AA407FEA84BF95233436AE20900418733046F26F
SHA-512:	5F293900A6A0AED425CBC384111A6A8848B0124E127E06F592502B256AC5791BB13603642A6402BF756DE0949612DF60BB33A467C1ABD9E477C1DE6C8F30337B
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\CLJgKpOuw.exe	
Process:	C:\Users\user\Desktop\7lQnHeq3XF.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	511488
Entropy (8bit):	7.692170481145156
Encrypted:	false
SSDEEP:	12288:qhBSAd7kDsfDQMZUVCfdtZqJq2QJoWr0p/zsq5X6NGmBx:qhBSo7kDsWiCKouEB6N
MD5:	9750DEE05B47F072E5975895DCF61AE5
SHA1:	95F456AE508245B4C6891AD1C847227D0C012D90
SHA-256:	EEA0F064AF6E7B61E19FF9ADE76EEAD562F5D3933D52C5CC7F2F5721D81B8C3D
SHA-512:	8C52E2F45A47D5FEE4F58C93478105E48D18D7BC9AA5FF9B3F5EA1477FB687C29037200125B38349E604CD841DCAF20D6B7B6542C57DBDC72488F9177BF7BA3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 34%, Browse • Antivirus: ReversingLabs, Detection: 79%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....3.`.....0..... .....@.. .....@..... ..@.....O..... ..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....H...(.....J...p...P.....".(.....*".(.....*^.(.....}.....}....*...0.....{.....+..*.0.....{.....+..*B...}.....}....*....0..2. .....o.....o....Y..o.....o....Y...Z..ZXl(....k...+..*...0..O.....".....+0.....,.....o.....,.....o.....X....i.....-....+...*^.(.....}.....}....*..0.....{.....+..*.0.....{.....+..*B...}.....}....*. ...0..2.....o.....o....Y..o.....o....Y...Z..ZX

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\7lQnHeq3XF.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:u:u
MD5:	56FDE996BE3F8E26310C687C0CB102EB
SHA1:	7F6DA9DA4A1AD6C4B328B4A5B89F9CA439C4D012
SHA-256:	91B9404A440B92457001305F07E97746FE279BE58DF58A2AE09D365F5084EBC0
SHA-512:	9BBA08475C6AAD7AE79041A514B793C93C04B608A70D4E212E3D2BFF4AB863F41826C86C4E5D0CD348E475ADBD2B26C8E7242F794236D0124D81369E46B78C2
Malicious:	**true**
Preview:	..E},.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\7lQnHeq3XF.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	37
Entropy (8bit):	4.496898555450565
Encrypted:	false
SSDEEP:	3:oNWXp5vSJcnCn:oNWXpFSJ/n

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
MD5:	E393A7661EB5342CB1854E7658086172
SHA1:	ABB9A18EB2C16D0EBD6AAFA86D7898B34C5BF479
SHA-256:	73DD810932A854CB4143C58082C6F21F8138223A499B68C26BAB51DF00C4DF8B
SHA-512:	E7358C03D19D88A4B9B782DC26B98B2C4A601C6CBF6B2342A62C3C73D1AFA24D4DDA157779D98ED1616D9D060DEF81292C8DAC83B7BA9BA8FB9722E6B196B46
Malicious:	false
Preview:	C:\Users\user\Desktop\7lQnHeq3XF.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.692170481145156
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	7lQnHeq3XF.exe
File size:	511488
MD5:	9750dee05b47f072e5975895dcf61ae5
SHA1:	95f456ae508245b4c6891ad1c847227d0c012d90
SHA256:	eea0f064af6e7b61e19ff9ade76eead562f5d3933d52c5cc7f2f5721d81b8c3d
SHA512:	8c52e2f45a47d5fee4f58c93478105e48d18d7bc9aa5ff9b3f5ea1477fb687c29037200125b38349e604cd841dcaf20d6b7b6542c57dbdc72488f9177bf7ba3b
SSDEEP:	12288:qhBSAd7kDsfDQMZUVCfdtZqJq2QJoWr0p/zsq5X6NGmBx:qhBSo7kDsWiCKouEB6N
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....3.`.....0..... .....@.. .....@.....@.....

File Icon



Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x47e312
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:	0x60A2331A [Mon May 17 09:10:50 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0

Copyright Joe Security LLC 2021

General

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	0x7c398	0x7c400	False	0.84128010249	data	7.70438467215	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x80000	0x5a4	0x600	False	0.416666666667	data	4.06990605525	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x82000	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

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 7lQnHeq3XF.exe PID: 5360 Parent PID: 5840

General

Start time:	19:03:54
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\7lQnHeq3XF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\7lQnHeq3XF.exe'

Copyright Joe Security LLC 2021

Imagebase:	0x230000
File size:	511488 bytes
MD5 hash:	9750DEE05B47F072E5975895DCF61AE5
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: 00000000.00000002.298237654.00000000036C6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.298237654.00000000036C6000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.298237654.00000000036C6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.297181399.0000000003529000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.297181399.0000000003529000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.297181399.0000000003529000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 3688 Parent PID: 5360

General

Start time:	19:04:35
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\CLJgKpOuw' /XML 'C:\Users\user\AppData\Local\Temp\tmp6F2E.tmp'
Imagebase:	0x370000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 4128 Parent PID: 3688

General

Start time:	19:04:36
Start date:	10/06/2021

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: 7lQnHeq3XF.exe PID: 784 Parent PID: 5360

General

Start time:	19:04:37
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\7lQnHeq3XF.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xec0000
File size:	511488 bytes
MD5 hash:	9750DEE05B47F072E5975895DCF61AE5
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: 0000000C.00000002.476199801.0000000003261000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000000.293449778.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000000.293449778.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000000.293449778.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000000.292982404.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000000.292982404.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000000.292982404.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.481846262.00000000042A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.481846262.00000000042A9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.483716211.0000000005B90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.483716211.0000000005B90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.483716211.0000000005B90000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.470249000.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.470249000.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.470249000.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.483484770.0000000005930000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000C.00000002.483484770.0000000005930000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 3032 Parent PID: 784

General

Start time:	19:04:40
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp8362.tmp'
Imagebase:	0x370000
File size:	185856 bytes

MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 4280 Parent PID: 3032

General

Start time:	19:04:40
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: 7lQnHeq3XF.exe PID: 3088 Parent PID: 528

General

Start time:	19:04:42
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\7lQnHeq3XF.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\7lQnHeq3XF.exe 0
Imagebase:	0x780000
File size:	511488 bytes
MD5 hash:	9750DEE05B47F072E5975895DCF61AE5
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: 00000010.00000002.396832392.0000000003CE6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.396832392.0000000003CE6000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.396832392.0000000003CE6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000010.00000002.395146878.0000000002B8C000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.395816202.0000000003B49000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.395816202.0000000003B49000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.395816202.0000000003B49000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities | Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 5336 Parent PID: 3088

General

Start time:	19:05:21
Start date:	10/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\CLJgKpOuw' /XML 'C:\Users\user\AppData\Local\Temp\tmp1E69.tmp'
Imagebase:	0xfb0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities | Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 5568 Parent PID: 5336

General

Start time:	19:05:21
Start date:	10/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: 7lQnHeq3XF.exe PID: 3508 Parent PID: 3088

General

Start time:	19:05:22
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\7lQnHeq3XF.exe

Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x300000
File size:	511488 bytes
MD5 hash:	9750DEE05B47F072E5975895DCF61AE5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: 7lQnHeq3XF.exe PID: 576 Parent PID: 3088

General

Start time:	19:05:22
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\7lQnHeq3XF.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x8a0000
File size:	511488 bytes
MD5 hash:	9750DEE05B47F072E5975895DCF61AE5
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: 00000018.00000002.410604962.0000000003CB9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.410604962.0000000003CB9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000000.391573162.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000000.391573162.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000000.391573162.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000002.409379306.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.409379306.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.409379306.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000000.390895301.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000000.390895301.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000000.390895301.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.410520702.0000000002CB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.410520702.0000000002CB1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021