ID: 403128
Sample Name: fixxing.exe
Cookbook: default.jbs
Time: 19:47:16
Date: 03/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

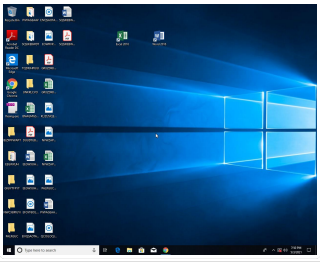
Analysis Report fixxing.exe

Overview

General Information

Sample Name:	fixxing.exe
Analysis ID:	403128
MD5:	0d50c8e7c3f0440..
SHA1:	538871e91c9cac..
SHA256:	91f6fc2ae99e090..
Tags:	exe NanoCore
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

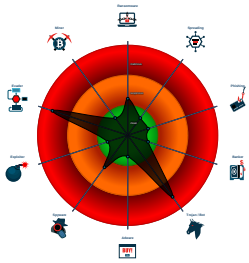
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM3
- 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…

Classification



Startup

- **System is w10x64**
- fixxing.exe (PID: 5808 cmdline: 'C:\Users\user\Desktop\fixxing.exe' MD5: 0D50C8E7C3F044099056BFB318F108C6)
  - schtasks.exe (PID: 4736 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\xQGPeospVmcjdT' /XML 'C:\Users\user\AppData\Local\Temp\tmp86B5.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3412 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - fixxing.exe (PID: 4700 cmdline: C:\Users\user\Desktop\fixxing.exe MD5: 0D50C8E7C3F044099056BFB318F108C6)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "cbea22e5-f897-4039-a352-cfbfd96f",
  "Group": "chase1",
  "Domain1": "45.137.22.50",
  "Domain2": "127.0.0.1",
  "Port": 4557,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "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
00000005.00000002.489550549.0000000005F5 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x4bbb:$x1: NanoCore.ClientPluginHost • 0x4be5:$x2: IClientNetworkHost
00000005.00000002.489550549.0000000005F5 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x4bbb:$x2: NanoCore.ClientPluginHost • 0x6a6b:$s4: PipeCreated
00000005.00000002.488981996.000000000531 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000005.00000002.488981996.000000000531 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
00000005.00000002.486030987.00000000037A 9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 22 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.3.fixxing.exe.43962f5.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x605:$x1: NanoCore.ClientPluginHost • 0x3bd6:$x1: NanoCore.ClientPluginHost • 0x63e:$x2: IClientNetworkHost
5.3.fixxing.exe.43962f5.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x605:$x2: NanoCore.ClientPluginHost • 0x3bd6:$x2: NanoCore.ClientPluginHost • 0x720:$s4: PipeCreated • 0x3cb4:$s4: PipeCreated • 0x61f:$s5: IClientLoggingHost • 0x3bf0:$s5: IClientLoggingHost
5.2.fixxing.exe.42c3717.12.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1deb:$x1: NanoCore.ClientPluginHost • 0x1e24:$x2: IClientNetworkHost
5.2.fixxing.exe.42c3717.12.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1deb:$x2: NanoCore.ClientPluginHost • 0x1f36:$s4: PipeCreated • 0x1e05:$s5: IClientLoggingHost
5.2.fixxing.exe.27d47cc.5.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2dbb:$x1: NanoCore.ClientPluginHost • 0x2de5:$x2: IClientNetworkHost
Click to see the 91 entries				

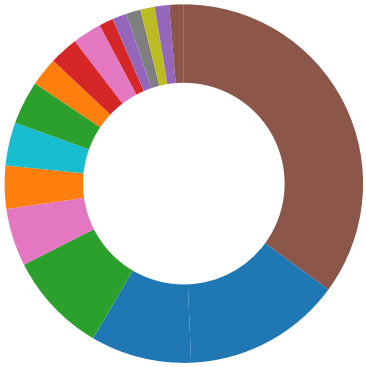
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

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:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

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:

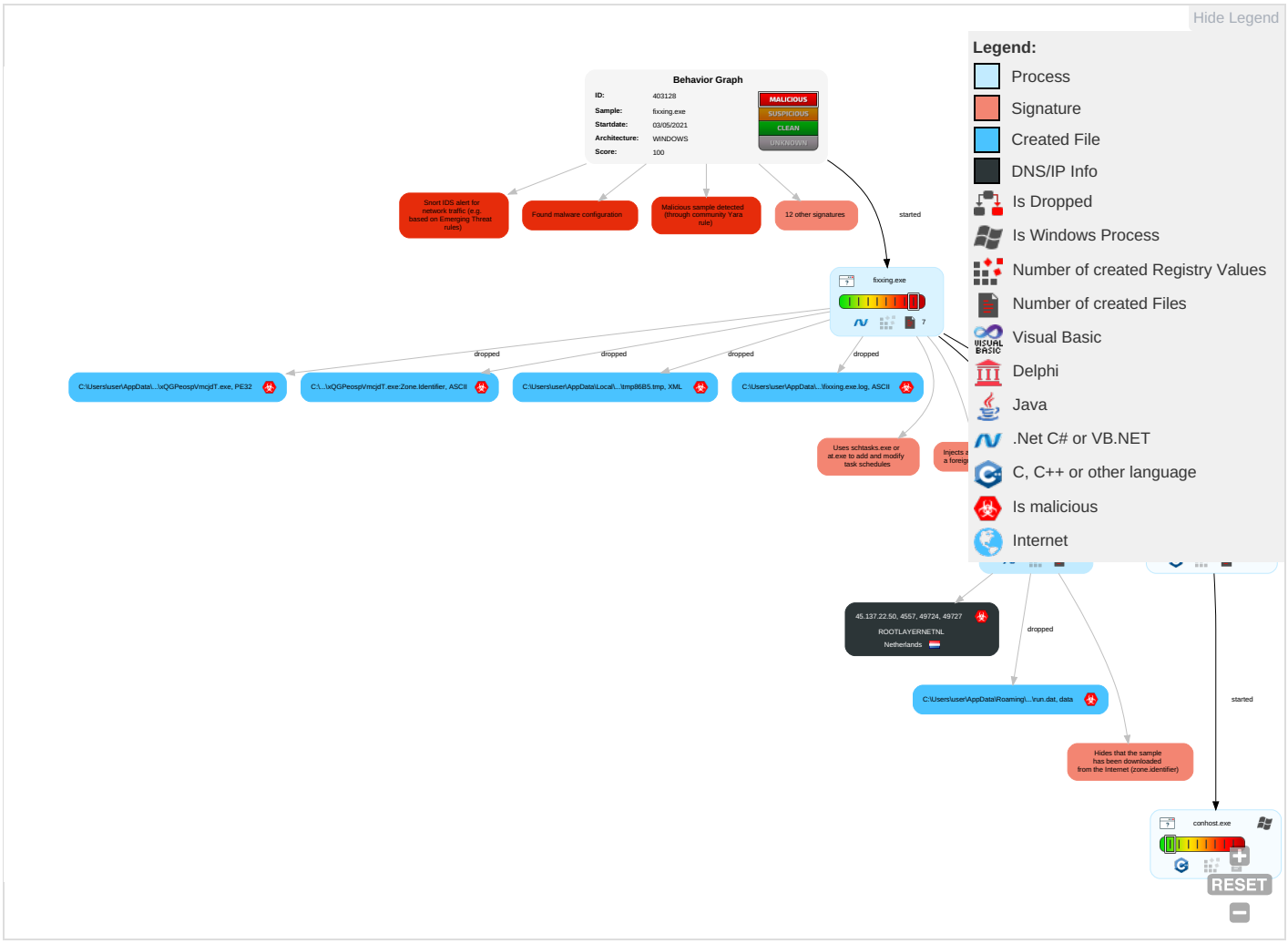
Detected Nanocore Rat

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
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1	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 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2 2 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 4 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 4 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	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	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	File and Directory Discovery 1	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	System Information Discovery 1 2	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

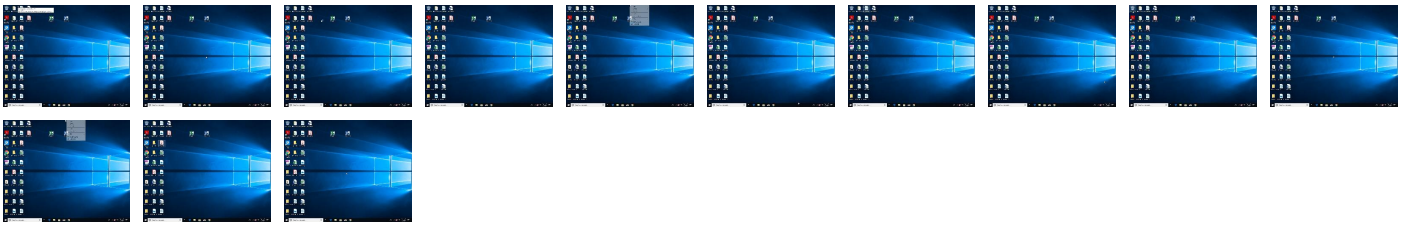
Behavior Graph



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
fixxing.exe	32%	Virustotal		Browse
fixxing.exe	18%	Metadefender		Browse
fixxing.exe	60%	ReversingLabs	ByteCode-MSIL.Trojan.Agentesla	
fixxing.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\xQGPeospVmcjdT.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\xQGPeospVmcjdT.exe	18%	Metadefender		Browse
C:\Users\user\AppData\Roaming\xQGPeospVmcjdT.exe	60%	ReversingLabs	ByteCode-MSIL.Trojan.Agentesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.fixxing.exe.37b8a20.7.unpack	100%	Avira	TR/NanoCore.fadte		Download File
5.2.fixxing.exe.5a50000.20.unpack	100%	Avira	TR/NanoCore.fadte		Download File
5.2.fixxing.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
45.137.22.50	1%	Virustotal		Browse
45.137.22.50	0%	Avira URL Cloud	safe	
http://https://www.rtctel.com/	0%	Virustotal		Browse
http://https://www.rtctel.com/	0%	Avira URL Cloud	safe	
127.0.0.1	0%	Virustotal		Browse
127.0.0.1	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

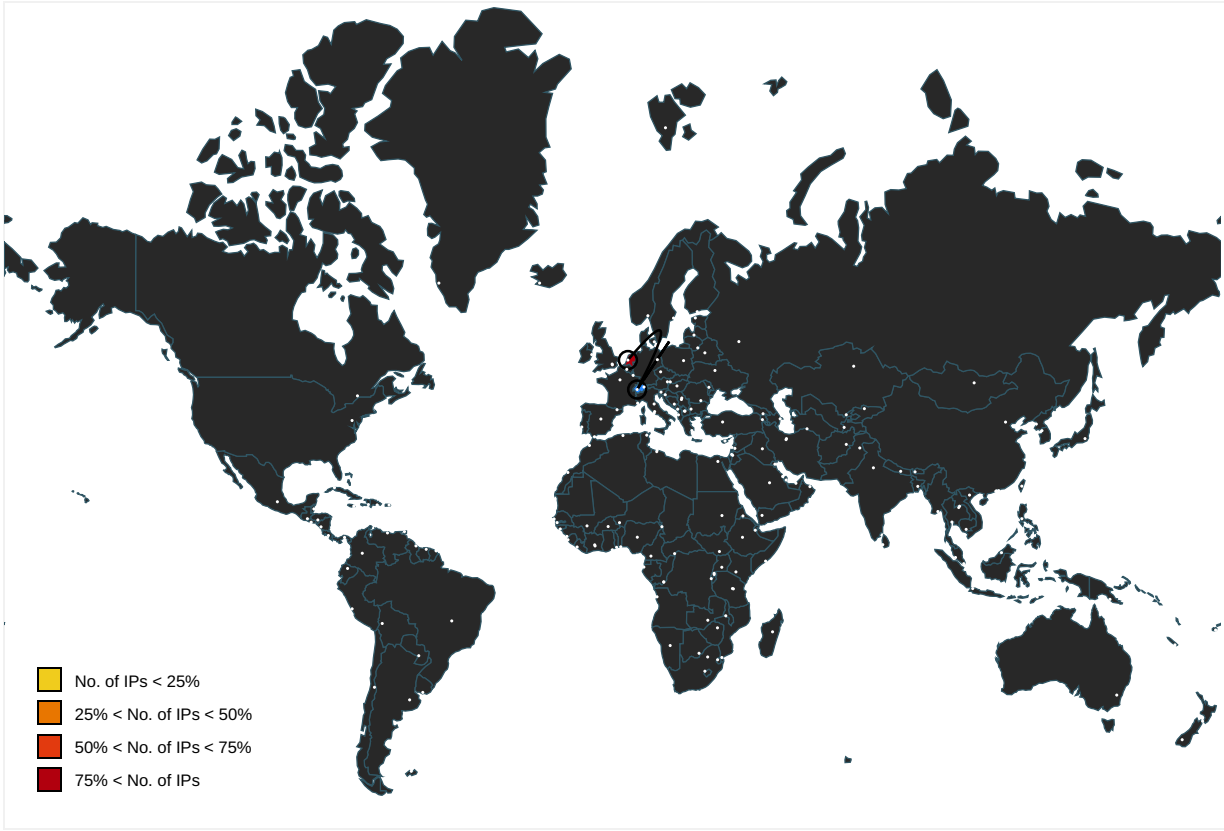
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
45.137.22.50	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
127.0.0.1	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://support.bandwidth.com/hc/en-us/restricted?return_to=https%3A%2F%2Fsupport.bandwidth.com%2Fhc	fixxing.exe	false		high
http://https://support.neonova.net/login.php	fixxing.exe	false		high
http://https://admin.neonova.net/index.php	fixxing.exe	false		high
http://https://www.rtctel.com/	fixxing.exe	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://admin.neonova.net/index.phpKhttps://support.neonova.net/login.phpmhttps://calix.force.com/id	fixxing.exe	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	fixxing.exe, 00000000.00000002.224977939.00000000028E1000.00000004.00000001.sdmp	false		high
http://https://calix.force.com/idp/login?app=0sp70000000001i#	fixxing.exe	false		high
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	fixxing.exe, 00000000.00000002.224977939.00000000028E1000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.137.22.50	unknown	Netherlands		51447	ROOTLAYERNETNL	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403128
Start date:	03.05.2021
Start time:	19:47:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	fixxing.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:	27
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@6/8@0/1
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 • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:48:08	API Interceptor	1025x Sleep call for process: fixxing.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.137.22.50	note-mxm.exe	Get hash	malicious	Browse	
	purchase order confirmation.exe	Get hash	malicious	Browse	
	purchase order acknowledgement.exe	Get hash	malicious	Browse	
	TBBurmah Trading Co., Ltd - products inquiry .exe	Get hash	malicious	Browse	
	PURCHASE ORDER - #0022223 DATED 29042021.exe	Get hash	malicious	Browse	
	PURCHASE ORDER - #0022223, date29042021.exe	Get hash	malicious	Browse	
	B_N SAO SWIFT MT103.exe	Get hash	malicious	Browse	
	PURCHASE ORDER - #0022223 DATED 28042021.exe	Get hash	malicious	Browse	
	Al kabous group Ltd - purchase order #04272021.exe	Get hash	malicious	Browse	
	Mack Trading Limited - products list.exe	Get hash	malicious	Browse	
	Kim Quy Trading - PRODUCTS LISTS.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ROOTLAYERNETNL	note-mxm.exe	Get hash	malicious	Browse	• 45.137.22.50
	purchase order confirmation.exe	Get hash	malicious	Browse	• 45.137.22.50
	purchase order acknowledgement.exe	Get hash	malicious	Browse	• 45.137.22.50
	TBBurmah Trading Co., Ltd - products inquiry .exe	Get hash	malicious	Browse	• 45.137.22.50
	FRIEGHT PAYMENT 41,634.20 USD..exe	Get hash	malicious	Browse	• 45.137.22.107
	Due Invoices.exe	Get hash	malicious	Browse	• 45.137.22.107
	PURCHASE ORDER - #0022223 DATED 29042021.exe	Get hash	malicious	Browse	• 45.137.22.50
	PURCHASE ORDER - #0022223, date29042021.exe	Get hash	malicious	Browse	• 45.137.22.50
	B_N SAO SWIFT MT103.exe	Get hash	malicious	Browse	• 45.137.22.50
	PO0900009.exe	Get hash	malicious	Browse	• 185.222.58.152

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PURCHASE ORDER - #0022223 DATED 28042021.exe	Get hash	malicious	Browse	• 45.137.22.50
	Order ConfirmationSANQAW12NC9W03.exe	Get hash	malicious	Browse	• 185.222.57.152
	PO MT2249C.exe	Get hash	malicious	Browse	• 185.222.57.152
	Al kabous LtdPurchase order NO#00421876.exe	Get hash	malicious	Browse	• 185.222.57.152
	Al kabous group Ltd - purchase order #04272021.exe	Get hash	malicious	Browse	• 45.137.22.50
	0900000000000000000900.exe	Get hash	malicious	Browse	• 185.222.58.152
	P08240421_CIF-Pdf.exe	Get hash	malicious	Browse	• 45.137.22.123
	ORD-63648.exe	Get hash	malicious	Browse	• 45.137.22.123
	FA0900009000.exe	Get hash	malicious	Browse	• 185.222.58.152
	Packinglist&certificate of imports.exe	Get hash	malicious	Browse	• 185.222.57.152

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\xQGPeospVmcjdT.exe	purchase order confirmation.exe	Get hash	malicious	Browse	

Created / dropped Files

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

Process:	C:\Users\user\Desktop\fixxing.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
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\Temp\tmp86B5.tmp

Process:	C:\Users\user\Desktop\fixxing.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1647
Entropy (8bit):	5.1976832556708175
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBVqBtn:cbh47TlNQ//rydbz9I3YODOLNdq3j+
MD5:	711F9E16C0FBC75B09CFA0CDFD720915
SHA1:	F21F57A9E5ED5894D4743A3F3DE0CE3D3B9FBE3B
SHA-256:	1E6B7105305FAE8EC803C5669EFCE337B1207AC0B38B19AA2C3513C0D1C88D54
SHA-512:	59FCFAB5AB3913FBD90F5AF156C496130DB4162256E150DE2AB3E2207F239B99490AAA84F759F016FCFC6184E8E3A7479EB13C8B11D5236236094D09A5680F27
Malicious:	**true**
Reputation:	low

C:\Users\user\AppData\Local\Temp\tmp86B5.tmp	
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\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\fixxing.exe
File Type:	data
Category:	dropped
Size (bytes):	1856
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrw8:flC0IIC0IIC0IIC0IIC0IIC0IIC0IICr
MD5:	838CD9DBC78EA45A5406EAE23962086D
SHA1:	C8273AACDEE03AC0CDCDDBAA83F51D04D6A4203C
SHA-256:	6E11A62511C5BBC0413128305069B780C448684B54FAA3E8DD0B4FD3DB8C9867
SHA-512:	F7D25EF1FA6F50667DD6785CC774E0AA6BC52A2231FE96E7C59D14EFDFDDA076F6399288CF6EAC8EFA8A75727893432AA155DA0E392F8CD1F26C5C5871EAC6B5
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\fixxing.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:PCot:6ot
MD5:	FE39AF73DBC3CEDCDE515A5AC1E37181
SHA1:	7A09829329D36895F3DF3426447D30B832A83658
SHA-256:	05FBCBC3F0AE751B30F246D1336A6ADDC4DE211B480CAB5F34410B795D39C9FB
SHA-512:	1B5D97B15A9C4AAE09CC869E870ABE1F7ADDB9C584DFCAA8FDA3FFF67DEAA826CE877DBC53E74F449F9CB39A09D1D3A5FE30007327C33C9D64519AA2F592C130
Malicious:	**true**
Reputation:	low
Preview:	.vM....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\fixxing.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671BCB
Malicious:	false
Reputation:	moderate, very likely benign file
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\fixxing.exe
File Type:	data

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

C:\Users\user\AppData\Roaming\xQGPeospVmcjdT.exe	
Process:	C:\Users\user\Desktop\fixxing.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	730112
Entropy (8bit):	7.682661934320617
Encrypted:	false
SSDEEP:	12288:ctl3e+PHoCAQ1q5y/e2h3QFRiFD94KnBedBJmrRiD8pBf5rcrM:ctl3e+foC/q4oDiFJRBedOrQYpR5rm
MD5:	0D50C8E7C3F044099056BFB318F108C6
SHA1:	538871E91C9CAC38AF31BD09FE456843D841F586
SHA-256:	91F6FC2AE99E090DAD56E53C7BF258DD4F43DF79AC02A11F2620C31F045FC87F
SHA-512:	5364611735FE235A94A0339EAE7511472EEAB0B892E9E1A17DA46F23802F82C4C2B225BED37953226A1B8B84D6711F16EEE15F28254D5A4D68BC26E378B7C7AD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 18%, Browse • Antivirus: ReversingLabs, Detection: 60%
Joe Sandbox View:	• Filename: purchase order confirmation.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P.....b-... ...@....@.. ..... ..@.....-..O....@..8.....`..... ....H.....text...h.... ....`.rsrc...8....@.....@..@.rel oc.....`.....".....@..B.....D-.....H.....-.....:.p.....0.....(....(.....(.....o....*.....(.....(!.....("....(#.....($....*N..(....o.... (%....*&..(&....*.s'.....s(.....s).....s*.....s+.....*....0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0..<.....~.....(1.....!r...p.....(2...o3...s4.....~.....+..*.0.....

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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.682661934320617

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	fixxing.exe
File size:	730112
MD5:	0d50c8e7c3f044099056bfb318f108c6
SHA1:	538871e91c9cac38af31bd09fe456843d841f586
SHA256:	91f6fc2ae99e090dad56e53c7bf258dd4f43df79ac02a11f2620c31f045fc87f
SHA512:	5364611735fe235a94a0339eae7511472eeab0b892e9e1a17da46f23802f82c4c2b225bed37953226a1b8b84d6711f16eee15f28254d5a4d68bc26e378b7c7ad
SSDEEP:	12288:ctl3e+PHoCAQ1q5y/e2h3QFRiFD94KnBedBJmrRiD8pBf5rcrM:ctl3e+foC/q4oDiFJRBedOrQYpR5rm
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P.....b-... ...@....@.. .....@.....

File Icon

Icon Hash:	849494a4a4a4e464

Static PE Info

General

Entrypoint:	0x4a2d62
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:	0x608D050B [Sat May 1 07:36:43 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
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa2d10	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa4000	0x11138	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb6000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa0d68	0xa0e00	False	0.853620337995	data	7.76210474352	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa4000	0x11138	0x11200	False	0.11155622719	data	5.26971437241	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb6000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xa4130	0x10828	data		
RT_GROUP_ICON	0xb4958	0x14	data		
RT_VERSION	0xb496c	0x30c	data		
RT_MANIFEST	0xb4c78	0x4bd	XML 1.0 document, UTF-8 Unicode (with BOM) text		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	
Assembly Version	1.0.0.0
InternalName	Debugger.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	RogueButtons
ProductVersion	1.0.0.0
FileDescription	RogueButtons
OriginalFilename	Debugger.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/03/21-19:48:16.892186	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49724	4557	192.168.2.3	45.137.22.50
05/03/21-19:48:23.328869	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49727	4557	192.168.2.3	45.137.22.50
05/03/21-19:48:28.259692	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49728	4557	192.168.2.3	45.137.22.50
05/03/21-19:48:34.313765	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49732	4557	192.168.2.3	45.137.22.50
05/03/21-19:48:40.300527	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49735	4557	192.168.2.3	45.137.22.50
05/03/21-19:48:46.350416	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49736	4557	192.168.2.3	45.137.22.50
05/03/21-19:48:52.395241	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49737	4557	192.168.2.3	45.137.22.50
05/03/21-19:48:58.513579	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49741	4557	192.168.2.3	45.137.22.50
05/03/21-19:49:05.642550	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49742	4557	192.168.2.3	45.137.22.50
05/03/21-19:49:11.743009	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49748	4557	192.168.2.3	45.137.22.50
05/03/21-19:49:17.725023	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49750	4557	192.168.2.3	45.137.22.50
05/03/21-19:49:23.741350	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49751	4557	192.168.2.3	45.137.22.50
05/03/21-19:49:29.790151	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49752	4557	192.168.2.3	45.137.22.50
05/03/21-19:49:35.792248	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49753	4557	192.168.2.3	45.137.22.50
05/03/21-19:49:41.791022	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49756	4557	192.168.2.3	45.137.22.50
05/03/21-19:49:47.805502	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49757	4557	192.168.2.3	45.137.22.50
05/03/21-19:49:53.947358	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49758	4557	192.168.2.3	45.137.22.50
05/03/21-19:49:59.949354	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49759	4557	192.168.2.3	45.137.22.50
05/03/21-19:50:06.047937	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49761	4557	192.168.2.3	45.137.22.50
05/03/21-19:50:12.307942	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49762	4557	192.168.2.3	45.137.22.50

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 19:48:16.770478010 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:16.817135096 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:16.817271948 CEST	49724	4557	192.168.2.3	45.137.22.50

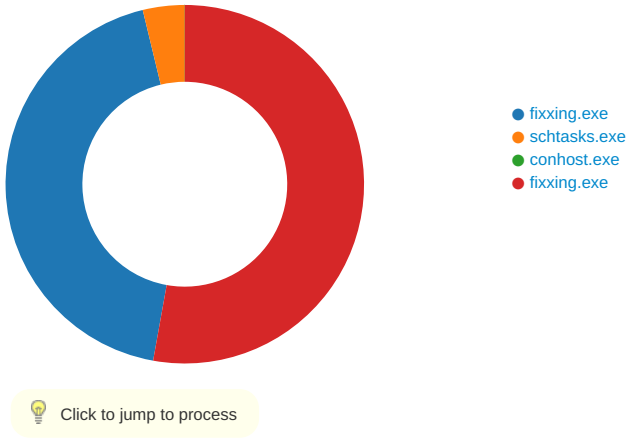
Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 19:48:16.892185926 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:16.961973906 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:16.981944084 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.029064894 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.056797028 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.125231028 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.125410080 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.158269882 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.158327103 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.158365965 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.158413887 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.158423901 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.158452034 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.158452988 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.158519983 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.203636885 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.205080986 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.205136061 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.205174923 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.205235958 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.205291033 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.205348015 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.205442905 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.205492973 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.205519915 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.205658913 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.252422094 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.252463102 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.252496958 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.252538919 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.252587080 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.252592087 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.252624035 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.252628088 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.252659082 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.252687931 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.252691984 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.252717972 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.252746105 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.252747059 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.252777100 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.252808094 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.252836943 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.252852917 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.252892971 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.299448013 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.299506903 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.299546957 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.299583912 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.299655914 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.299695015 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.299710989 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.299742937 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.299782038 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.299786091 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.299789906 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.299814939 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.299853086 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.299880028 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.299890995 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.299928904 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.299963951 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.299966097 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.300004005 CEST	4557	49724	45.137.22.50	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 19:48:17.300050974 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.300055027 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.300092936 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.300118923 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.300131083 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.300168991 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.300206900 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.300242901 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.300266981 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.300281048 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.300282001 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.300321102 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.300368071 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.300393105 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.300410032 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.300447941 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.300451040 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.300477982 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.300538063 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.347068071 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.347121954 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.347157001 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.347188950 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.347222090 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.347244024 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.347254038 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.347285032 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.347295046 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.347327948 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.347347975 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.347352028 CEST	4557	49724	45.137.22.50	192.168.2.3
May 3, 2021 19:48:17.347384930 CEST	49724	4557	192.168.2.3	45.137.22.50
May 3, 2021 19:48:17.347392082 CEST	4557	49724	45.137.22.50	192.168.2.3

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: fixxing.exe PID: 5808 Parent PID: 5564

General

Start time:	19:48:07
Start date:	03/05/2021
Path:	C:\Users\user\Desktop\fixxing.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\fixxing.exe'
Imagebase:	0x510000
File size:	730112 bytes
MD5 hash:	0D50C8E7C3F044099056BFB318F108C6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.224977939.00000000028E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.225554713.00000000038E9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.225554713.00000000038E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.225554713.00000000038E9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	unknown
C:\Users\user\AppData\Roaming\xQGPeospVmcjdT.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CEFDD66	CopyFileW
C:\Users\user\AppData\Roaming\xQGPeospVmcjdT.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CEFDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp86B5.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CEF7038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\fixxing.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3BC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp86B5.tmp	success or wait	1	6CEF6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\xQGPeospVmcjdT.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 0b 05 8d 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 0e 0a 00 00 14 01 00 00 00 00 00 62 2d 0a 00 00 20 00 00 00 40 0a 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 0b 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......`.......... ....P.............b-... ...@....@.. ....@.................	success or wait	3	6CEFDD66	CopyFileW
C:\Users\user\AppData\Roaming\ xQGPeospVmcjdT.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CEFDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp86B5.tmp	unknown	1647	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.mic roso ft.com/windows/2004/02/m it/task">.. <RegistrationInfo>.. <Date>2014-10- 25T14:27:44.892 9027</Date>.. <Author>compu ter\user</Author>.. </RegistrationIn	success or wait	1	6CEF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\fixxing.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	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.	success or wait	1	6E3BC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile

Analysis Process: schtasks.exe PID: 4736 Parent PID: 5808

General

Start time:	19:48:11
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\xQGPeospVmcjdT' /XML 'C:\Users\user\AppData\Local\Temp\tmp86B5.tmp'
Imagebase:	0x1000000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp86B5.tmp	unknown	2	success or wait	1	100AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp86B5.tmp	unknown	1648	success or wait	1	100ABD9	ReadFile

Analysis Process: conhost.exe PID: 3412 Parent PID: 4736

General

Start time:	19:48:11
Start date:	03/05/2021
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: fixxing.exe PID: 4700 Parent PID: 5808

General

Start time:	19:48:12
Start date:	03/05/2021
Path:	C:\Users\user\Desktop\fixxing.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\fixxing.exe
Imagebase:	0x450000
File size:	730112 bytes
MD5 hash:	0D50C8E7C3F044099056BFB318F108C6
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: 00000005.00000002.489550549.0000000005F50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.489550549.0000000005F50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.488981996.0000000005310000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.488981996.0000000005310000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.486030987.00000000037A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.489178214.0000000005A50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.489178214.0000000005A50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.489178214.0000000005A50000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000003.250512467.0000000004373000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.479168192.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.479168192.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.479168192.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.487530331.0000000004352000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.487530331.0000000004352000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.481816000.0000000002751000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.487434335.0000000004267000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.489813017.0000000006430000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.489813017.0000000006430000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.481888361.00000000027BD000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ACF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CEFBEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CEF1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CEFBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CEFBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	19	6CEF1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CEF1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CEF1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\fixxing.exe:Zone.Identifier	success or wait	1	6CE72935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	bf 76 4d 10 a7 0e d9 48	.vM....H	success or wait	1	6CEF1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	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.....&.	success or wait	8	6CEF1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	327432	70 54 c7 ab ad 21 b0 08 57 f6 fa 47 14 4a ba aa 61 dd a0 29 17 40 c6 8b 69 8b df 77 70 4b 98 73 6f 40 e2 06 e5 35 e7 b7 3d e9 b8 90 5e ab 1d 51 82 6f 79 f9 3d 65 40 39 c3 42 8d f7 95 46 bc cb 30 39 75 22 33 8b f5 20 30 74 c0 19 52 44 6e 5f 34 64 fb b8 17 02 df 45 c0 90 06 69 f4 08 9f ae bb 8a 7e 0c 89 85 7c 87 eb 66 58 5f 0e c2 ed 58 66 88 70 5e e2 f5 ff 94 03 e5 3e 61 db 8b 91 24 8d 8a 8f 65 05 36 3a 37 64 b6 28 61 05 41 e4 fe e0 3d be 29 2a 0d 96 a8 90 8e 7b 42 1c 5b ab 87 cb 79 25 b3 2a e4 b8 b1 9f 69 a7 51 84 3c f3 94 a2 90 78 74 c4 a9 58 13 11 48 09 d7 20 ad cc a4 48 46 37 67 0f e0 c5 49 96 2a 33 03 7b 0c 6e 92 bf 90 be 4c d1 9b 79 3b 69 87 bc 73 2d 1e b6 f9 b8 28 35 69 c2 8b 92 d6 10 ac a7 02 93 ee 89 08 17 4a 09 35 62 37 7d fe 86 66 4b af ab 48 56	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.. ...HF7g...I.*3.{.n... .L..y;i..s-....(5i..... .J.5b7}..fK..HV	success or wait	1	6CEF1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 7e 61 d3 f8 a3 01 06 96 0c a9 7e ba 7e 86 90 d9 e5 05 8d ca 33 e7 55 0b	9iH....}Z..4..f.~a.....~.~. .....3.U.	success or wait	1	6CEF1B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E085705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E08CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DFE03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DFE03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E085705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CEF1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CEF1B4F	ReadFile
C:\Users\user\Desktop\fixxing.exe	unknown	4096	success or wait	1	6E06D72F	unknown
C:\Users\user\Desktop\fixxing.exe	unknown	512	success or wait	1	6E06D72F	unknown

Disassembly

Code Analysis