ID: 680396
Sample Name: FT - 08082022.exe
Cookbook: default.jbs
Time: 14:49:49
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

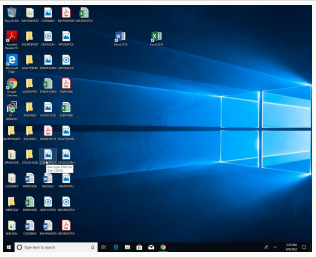
Windows Analysis Report

FT - 08082022.exe

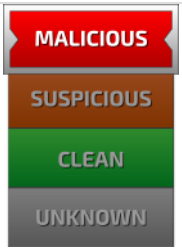
Overview

General Information

Sample Name:	FT - 08082022.exe
Analysis ID:	680396
MD5:	70b100ea1e1466.
SHA1:	aa775a962d1a17.
SHA256:	58f41297482040..
Tags:	exe
Infos:	



Detection



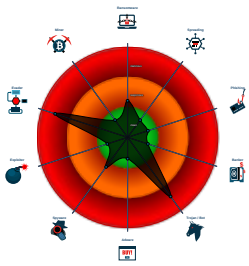
FormBook

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

Signatures

- Yara detected FormBook
- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- Maps a DLL or memory area into an…
- Machine Learning detection for sam…
- .NET source code contains potentia…
- Yara detected Generic Downloader
- Queues an APC in another process …
- .NET source code contains very larg…
- Tries to detect virtualization through…
- Modifies the context of a thread in a…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- FT - 08082022.exe (PID: 1144 cmdline: "C:\Users\user\Desktop\FT - 08082022.exe" MD5: 70B100EA1E1466A56A78D3A31DAE1E2A)
  - InstallUtil.exe (PID: 5412 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
    - explorer.exe (PID: 3616 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.mcphiecabinetry.site/iw01/"
  ],
  "decoy": [
    "searchandreach.com",
    "exhaustinternational.com",
    "megadarknetz.online",
    "naiti.pro",
    "bizcon-h.com",
    "unitatem.com",
    "sangeetapallai.site",
    "tradingwithwallstreet.com",
    "wwwvestmed.com",
    "tendful.top",
    "sezonuyakala.com",
    "mindlabpublishing.com",
    "barnwoodconnection.com",
    "smokehighsociety.com",
    "axelarigatosaopaulo.com",
    "cadence.ink",
    "zhaokl.net",
    "lwz168.com",
    "aladdinmkstore.com",
    "beyondexpawtationpetcare.com",
    "buckscountyprolife.info",
    "myangel.today",
    "haxtrldesign.xyz",
    "inselite.com",
    "hamshor.com",
    "soulpets.net",
    "cassettebeauty.com",
    "begonvilrestaurant.com",
    "preciuss.info",
    "bbjmw.com",
    "engr360.site",
    "sv388vip.xyz",
    "wealthofawoman.net",
    "futuresmartafricanonprofit.net",
    "dgshanteng.com",
    "hongtaoshunshun.top",
    "thebrowandbeautyplug.com",
    "bkeight.xyz",
    "aaguiapousou.com",
    "swingsandthings.store",
    "pdsbxw.com",
    "925xd.com",
    "huntervalley.online",
    "dostuff.tech",
    "tgydf.com",
    "texasexchange.info",
    "ralonllc.net",
    "deneyimrulman.online",
    "1xbet-wix.top",
    "aqnest.net",
    "worthdisk.com",
    "bpw-finland.com",
    "secured-vision-unit.com",
    "bc6029.com",
    "theunrulyplot.co.uk",
    "mvvezasi.site",
    "saferhennepin.com",
    "sunscreensale.store",
    "sdplci.com",
    "sou1xia.net",
    "gzgztf.top",
    "airriflehunt.com",
    "accwatercraft.com",
    "rscorecalculator.com"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.354778776.0000000003E79000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000000.00000002.354778776.0000000003E79000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6389:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1ccf8:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 7 0 01 0F B6 00 8D 55 • 0xab07:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 7 5 11 8A D0 80 E2 01 • 0x159ef:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000000.00000002.354778776.0000000003E79000.00000004.00000800.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9a40:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9cba:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x157ed:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x152d9:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x158ef:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x15a67:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa6d2:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x14554:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb3cb:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ba5f:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ca62:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
00000000.00000002.354778776.0000000003E79000.00000004.00000800.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18981:$sqlite3step: 68 34 1C 7B E1 • 0x18a94:$sqlite3step: 68 34 1C 7B E1 • 0x189b0:$sqlite3text: 68 38 2A 90 C5 • 0x18ad5:$sqlite3text: 68 38 2A 90 C5 • 0x189c3:$sqlite3blob: 68 53 D8 7F 8C • 0x18aeb:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000002.359453722.000000000D480000.00000004.08000000.00040000.00000000.sdmp	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	

Click to see the 19 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
14.0.InstallUtil.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
14.0.InstallUtil.exe.400000.0.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x5451:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1bdc0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 7 0 01 0F B6 00 8D 55 • 0x9bcf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 7 5 11 8A D0 80 E2 01 • 0x14ab7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
14.0.InstallUtil.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x143a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x979a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1361c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa493:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab27:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
14.0.InstallUtil.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a49:$sqlite3step: 68 34 1C 7B E1 • 0x17b5c:$sqlite3step: 68 34 1C 7B E1 • 0x17a78:$sqlite3text: 68 38 2A 90 C5 • 0x17b9d:$sqlite3text: 68 38 2A 90 C5 • 0x17a8b:$sqlite3blob: 68 53 D8 7F 8C • 0x17bb3:$sqlite3blob: 68 53 D8 7F 8C
0.2.FT - 08082022.exe.d480000.0.raw.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Yara detected FormBook

Antivirus / Scanner detection for submitted sample

Machine Learning detection for sample

Networking

Yara detected Generic Downloader

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation

.NET source code contains potential unpacker

Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

Maps a DLL or memory area into another process

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information

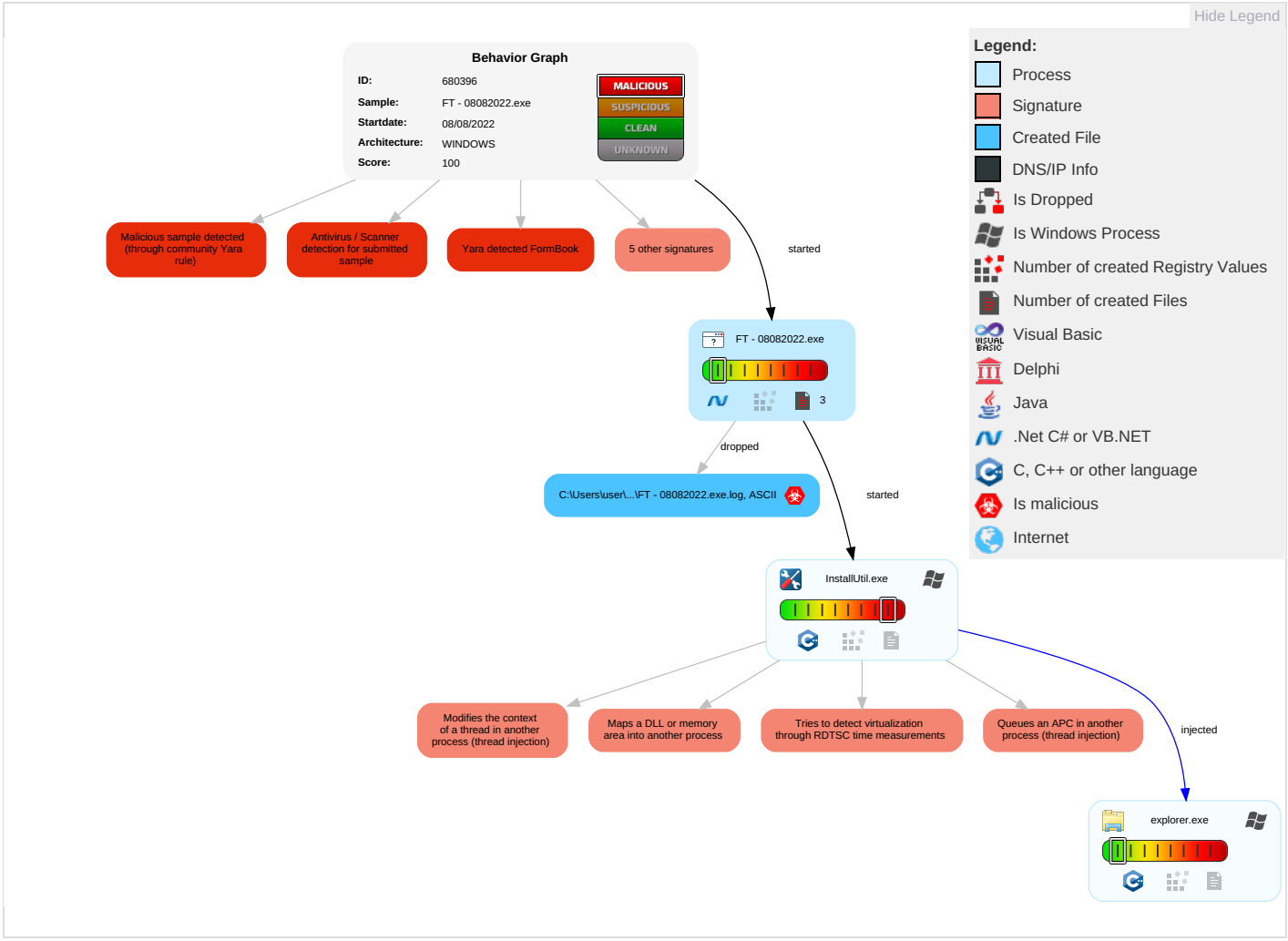
Yara detected FormBook

Remote Access Functionality

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	3 1 2 Process Injection	1 Masquerading	OS Credential Dumping	1 2 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 1 2 Process Injection	NTDS	1 1 2 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 2 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

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
FT - 08082022.exe	100%	Avira	HEUR/AGEN.1232160	
FT - 08082022.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.FT - 08082022.exe.680000.0.unpack	100%	Avira	HEUR/AGEN.1232160		Download File
14.0.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.mcphiecabinetry.site/iw01/	0%	Avira URL Cloud	safe	
http://james.newtonking.com/projects/json	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.mcphiecabinetry.site/iw01/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://www.nuget.org/packages/Newtonsoft.Json.Bson	FT - 08082022.exe, 00000000.00000002.354778776.0000000003E79000.00000004.00000800.00020000.00000000.sdmp, FT - 08082022.exe, 00000000.00000002.359453722.000000000D480000.00000004.08000000.00040000.00000000.sdmp	false		high
http://google.com	FT - 08082022.exe, 00000000.00000002.346131077.0000000002D31000.00000004.00000800.00020000.00000000.sdmp	false		high
http://james.newtonking.com/projects/json	FT - 08082022.exe, 00000000.00000002.348247508.0000000002E4F000.00000004.00000800.00020000.00000000.sdmp, FT - 08082022.exe, 00000000.00000002.346772186.0000000002D7A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.newtonsoft.com/jsonschema	FT - 08082022.exe, 00000000.00000002.354778776.0000000003E79000.00000004.00000800.00020000.00000000.sdmp, FT - 08082022.exe, 00000000.00000002.359453722.000000000D480000.00000004.08000000.00040000.00000000.sdmp	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680396
Start date and time: 08/08/202214:49:49	2022-08-08 14:49:49 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	FT - 08082022.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:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@3/1@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 92.5% (good quality ratio 79.3%) • Quality average: 70.5% • Quality standard deviation: 34.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 52.152.110.14, 20.54.89.106, 20.223.24.244, 40.125.122.176
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, e12564.dspb.akamaiedge.net, rp-consumer-prod-displaycatalog-geomap.trafficmanager.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\FT - 08082022.exe.log

Process:	C:\Users\user\Desktop\FT - 08082022.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1537
Entropy (8bit):	5.3478589519339295
Encrypted:	false
SSDEEP:	48:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzvFHLHKdHKBqHKs:Pq5qXEwCYqhQnoPtIxHeqzNrqdq4qs
MD5:	F6D3657BD1FBEF54E7F7BACB2497E327
SHA1:	A0A712015C242DCC28B69CDF567F594627C9CFA0
SHA-256:	5B16B4A3E65F04484B12171163A2A739409FA7F8C3D69BF9BAD961618D973301
SHA-512:	0231195A111259A3AA48526DCBEA98394099794C710C3FB8E0E12E2B4D30C60FB4064F7F4F671866FB0D94585E23B73C1270440242B25DA60CCFFA82B0B74306
Malicious:	**true**
Reputation:	moderate, 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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.849185992513857
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:	FT - 08082022.exe
File size:	2009088
MD5:	70b100ea1e1466a56a78d3a31dae1e2a
SHA1:	aa775a962d1a1714f06e15f03e244435b52eedfc
SHA256:	58f41297482040338766f554cca18e61888eaf9a9123e2570f48b89a31b601ac
SHA512:	ff41bda505f73c456dbded14078610abaed21dd4a4949d42b3079d3db19e5a623c78b2245e2a4bb88ddce27a59cbd4a4b3ae9ce8b304fbec6bfa6f097e47ac00
SSDEEP:	24576:OPR4a1YlrlM0iylybOe+5V0g3WqtkxOlhRdYWegGXzfMAw2:KxyAOe+5/31rjdYRf
TLSH:	DE957C15B0C228D84FFE066D2039CD09F4C8953898529E3968F3B6BFDBDE4465A56F0E
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....0..... .....@.. .....`.....

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x5eb9ce
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE

DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62F0C5B9 [Mon Aug 8 08:13:45 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1eb974	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1ec000	0xa00	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x1ee000	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	0x1e99d4	0x1e9a00	False	0.531388618521828	data	6.846947333897607	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x1ec000	0xa00	0xa00	False	0.426953125	data	4.30622895672951	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1ee000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1ec100	0x2e8	data		
RT_GROUP_ICON	0x1ec3f8	0x14	data		
RT_VERSION	0x1ec41c	0x3b6	data		
RT_MANIFEST	0x1ec7e4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

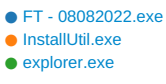
DLL	Import
mscoree.dll	_CorExeMain

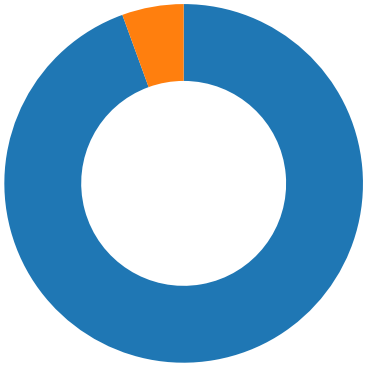
Network Behavior

No network behavior found

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: FT - 08082022.exe PID: **1144**, Parent PID: **3076**

General

Target ID:	0
Start time:	14:50:52
Start date:	08/08/2022
Path:	C:\Users\user\Desktop\FT - 08082022.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\FT - 08082022.exe"
Imagebase:	0x680000
File size:	2009088 bytes
MD5 hash:	70B100EA1E1466A56A78D3A31DAE1E2A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.354778776.0000000003E79000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.354778776.0000000003E79000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.354778776.0000000003E79000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.354778776.0000000003E79000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: 00000000.00000002.359453722.000000000D480000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.353706396.0000000003DDE000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.353706396.0000000003DDE000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.353706396.0000000003DDE000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.353706396.0000000003DDE000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.347927328.0000000002E22000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6CF1CF06	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	6CF1CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\FT - 08082022.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D22C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\FT - 08082022.exe.log	0	1537	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6D22C907	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	6CEF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6CEF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6CE503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CEFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6CE503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6CE503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6CE503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6CE503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6CEF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6CEF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BD61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BD61B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	6CE503DE	ReadFile

Analysis Process: InstallUtil.exe PID: **5412**, Parent PID: **1144**

General

Target ID:	14
Start time:	14:51:39
Start date:	08/08/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe
Imagebase:	0x7c0000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000000.336455722.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000E.00000000.336455722.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000000.336455722.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000000.336455722.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41A457	NtReadFile

Analysis Process: explorer.exe PID: **3616**, Parent PID: **5412**

General

Target ID:	15
Start time:	14:51:46
Start date:	08/08/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f3b00000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000000.471439159.000000000D40C000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000000.471439159.000000000D40C000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000000.471439159.000000000D40C000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000000.471439159.000000000D40C000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000F.00000000.445698170.000000000D40C000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000F.00000000.445698170.000000000D40C000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000F.00000000.445698170.000000000D40C000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000F.00000000.445698170.000000000D40C000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Disassembly

No disassembly