Joe Sandbox Cloud BASIC

ID: 501914
Sample Name: AfWu3i35ny.exe
Cookbook: default.jbs
Time: 12:07:33
Date: 13/10/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

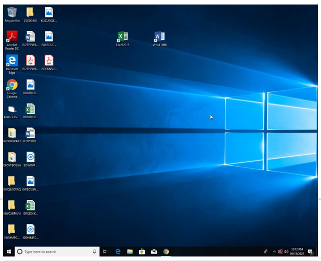
Windows Analysis Report AfWu3i35ny.exe

Overview

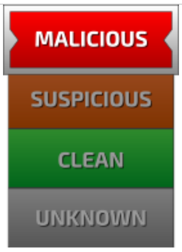
General Information

Sample Name:	AfWu3i35ny.exe
Analysis ID:	501914
MD5:	25aa37e21c29b7..
SHA1:	4374948e203cba..
SHA256:	740a2bc7e9c8ee..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection



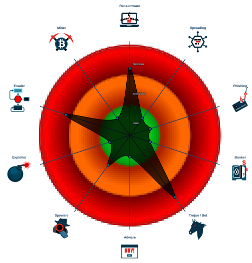
FormBook GuLoader

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

Signatures

- Antivirus / Scanner detection for sub…
- Found malware configuration
- Potential malicious icon found
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected GuLoader
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Found potential dummy code loops (…
- Machine Learning detection for samp…
- Creates a DirectInput object (often fo…
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64**
- AfWu3i35ny.exe (PID: 4536 cmdline: 'C:\Users\user\Desktop\AfWu3i35ny.exe' MD5: 25AA37E21C29B7CFF02509533B585ED7)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://45.137.22.91/blm.bin"
}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
AfWu3i35ny.exe	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
AfWu3i35ny.exe	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cococoding dot com	• 0x379b5:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x37d4f:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x1ac62:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x1a74e:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1ad64:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1aedc:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x38767:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x199c9:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x394df:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x20134:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x211d7:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Copyright Joe Security LLC 2021

Source	Rule	Description	Author	Strings
AfWu3i35ny.exe	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	- 0x1d066:$sqlite3step: 68 34 1C 7B E1 - 0x1d179:$sqlite3step: 68 34 1C 7B E1 - 0x1d095:$sqlite3text: 68 38 2A 90 C5 - 0x1d1ba:$sqlite3text: 68 38 2A 90 C5 - 0x1d0a8:$sqlite3blob: 68 53 D8 7F 8C - 0x1d1d0:$sqlite3blob: 68 53 D8 7F 8C

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.834854327.00000000021C0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000000.00000000.306440334.0000000000401000.00000020.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000000.00000000.306440334.0000000000401000.00000020.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	- 0x369b5:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC - 0x36d4f:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC - 0x19c62:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 - 0x1974e:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 - 0x19d64:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F - 0x19edc:$sequence_4: 5D C3 8D 50 7C 80 FA 07 - 0x37767:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 - 0x189c9:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 - 0x384df:$sequence_7: 66 89 0C 02 5B 8B E5 5D - 0x1f134:$sequence_8: 3C 54 74 04 3C 74 75 F4 - 0x201d7:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000000.00000000.306440334.0000000000401000.00000020.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	- 0x1c066:$sqlite3step: 68 34 1C 7B E1 - 0x1c179:$sqlite3step: 68 34 1C 7B E1 - 0x1c095:$sqlite3text: 68 38 2A 90 C5 - 0x1c1ba:$sqlite3text: 68 38 2A 90 C5 - 0x1c0a8:$sqlite3blob: 68 53 D8 7F 8C - 0x1c1d0:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000002.833081784.0000000000401000.00000020.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Click to see the 2 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.AfWu3i35ny.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.AfWu3i35ny.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	- 0x379b5:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC - 0x37d4f:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC - 0x1ac62:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 - 0x1a74e:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 - 0x1ad64:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F - 0x1aedc:$sequence_4: 5D C3 8D 50 7C 80 FA 07 - 0x38767:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 - 0x199c9:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 - 0x394df:$sequence_7: 66 89 0C 02 5B 8B E5 5D - 0x20134:$sequence_8: 3C 54 74 04 3C 74 75 F4 - 0x211d7:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0.2.AfWu3i35ny.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	- 0x1d066:$sqlite3step: 68 34 1C 7B E1 - 0x1d179:$sqlite3step: 68 34 1C 7B E1 - 0x1d095:$sqlite3text: 68 38 2A 90 C5 - 0x1d1ba:$sqlite3text: 68 38 2A 90 C5 - 0x1d0a8:$sqlite3blob: 68 53 D8 7F 8C - 0x1d1d0:$sqlite3blob: 68 53 D8 7F 8C
0.0.AfWu3i35ny.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.0.AfWu3i35ny.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	- 0x379b5:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC - 0x37d4f:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC - 0x1ac62:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 - 0x1a74e:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 - 0x1ad64:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F - 0x1aedc:$sequence_4: 5D C3 8D 50 7C 80 FA 07 - 0x38767:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 - 0x199c9:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 - 0x394df:$sequence_7: 66 89 0C 02 5B 8B E5 5D - 0x20134:$sequence_8: 3C 54 74 04 3C 74 75 F4 - 0x211d7:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 1 entries

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Found malware configuration

Yara detected FormBook

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Potential malicious icon found

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Found potential dummy code loops (likely to delay analysis)

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

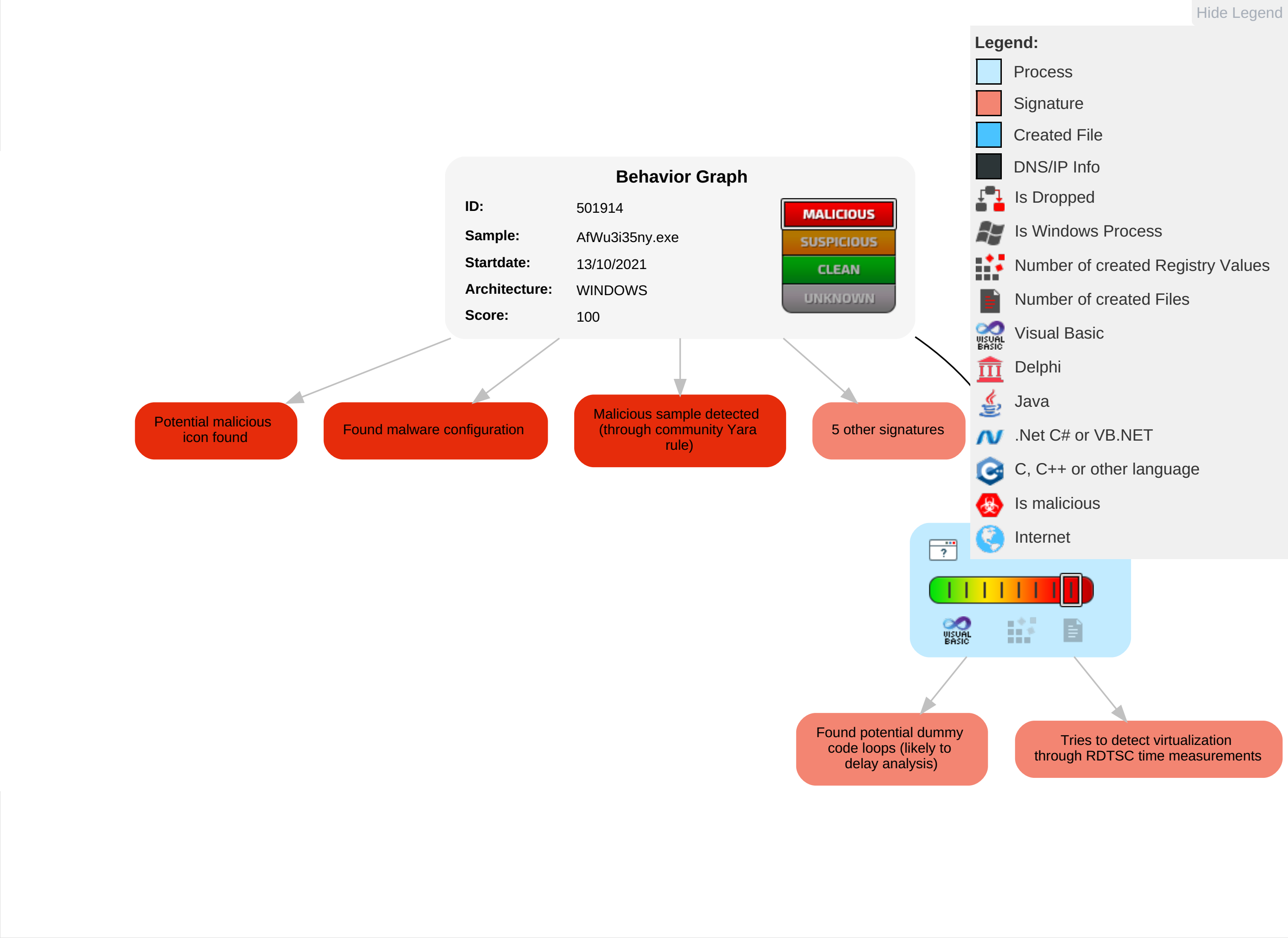
Yara detected FormBook

Mitre Att&ck Matrix

Copyright Joe Security LLC 2021

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Ef
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	Input Capture 1	Security Software Discovery 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Re Tr W Au
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Software Packing 2	LSASS Memory	Virtualization/Sandbox Evasion 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Re W W Au
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Ol De Cl Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	System Information Discovery 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

Behavior Graph



Behavior Graph

ID: 501914

Sample: AfWu3i35ny.exe

Startdate: 13/10/2021

Architecture: WINDOWS

Score: 100

Legend:

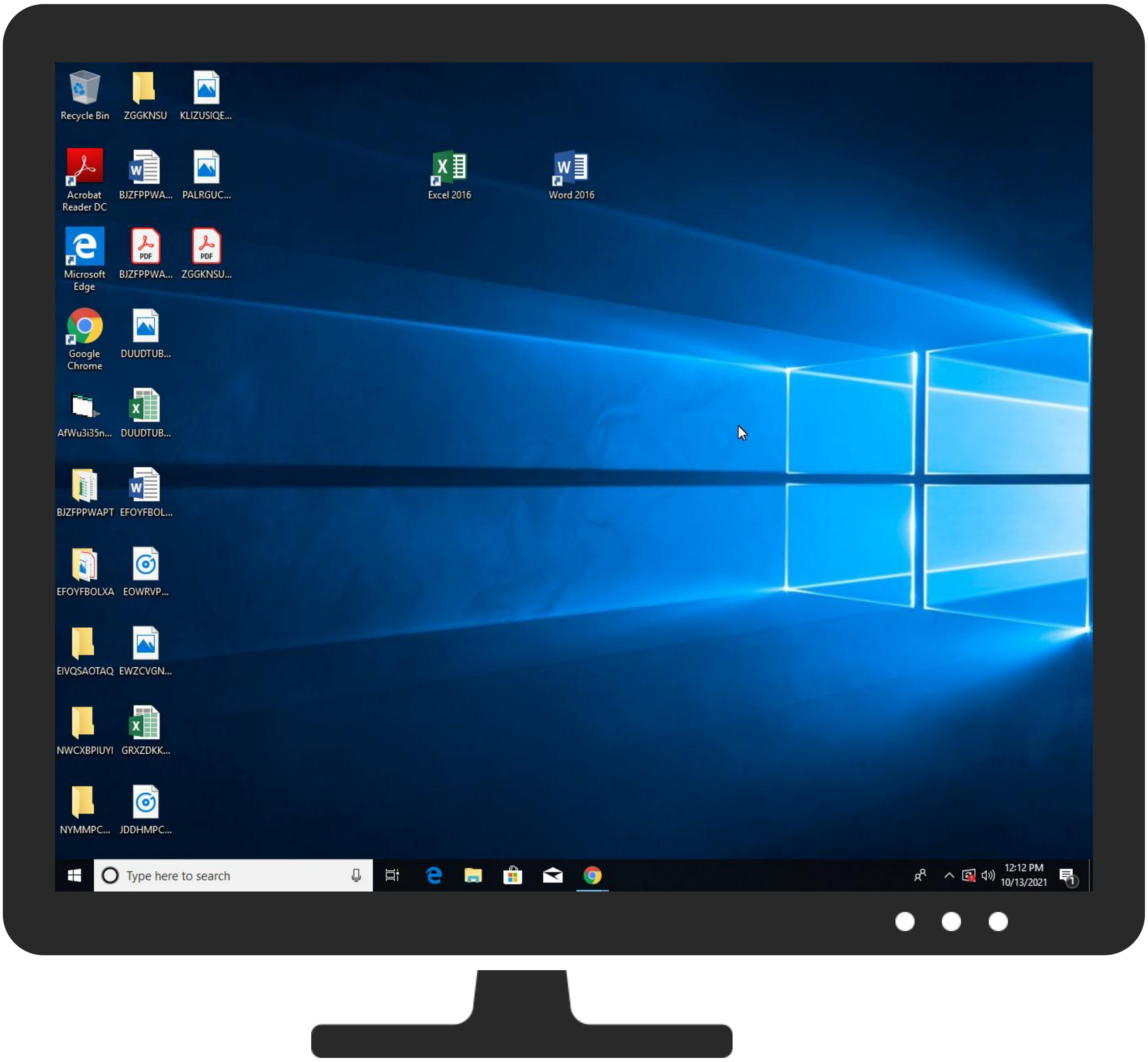
- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

Hide Legend
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Potential malicious icon found
Found malware configuration
Malicious sample detected (through community Yara rule)
5 other signatures
Found potential dummy code loops (likely to delay analysis)
Tries to detect virtualization through RDTSC time measurements

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
AfWu3i35ny.exe	100%	Avira	TR/Dropper.Gen2	
AfWu3i35ny.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link	Download
0.0.AfWu3i35ny.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen2		Download File
0.2.AfWu3i35ny.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen2		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://45.137.22.91/blm.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://45.137.22.91/blm.bin	true	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	501914
Start date:	13.10.2021
Start time:	12:07:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 20s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	AfWu3i35ny.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:	19
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.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 15.5% (good quality ratio 14.8%) • Quality average: 67.7% • Quality standard deviation: 28.1%
HCA Information:	Failed

Cookbook Comments:	- Adjust boot time - Enable AMSI - Found application associated with file extension: .exe - Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

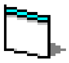
General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.957088133300485
TrID:	- Win32 Executable (generic) a (10002005/4) 99.15% - Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% - Generic Win/DOS Executable (2004/3) 0.02% - DOS Executable Generic (2002/1) 0.02% - Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	AfWu3i35ny.exe
File size:	307200
MD5:	25aa37e21c29b7cff02509533b585ed7
SHA1:	4374948e203cba151ebdc43e11e6e115046270e9

General

SHA256:	740a2bc7e9c8eeed76ef0f812c6c89af35c414317d76ac5b50b28ca0728d103b
SHA512:	8cb7b92766fd27a1bc888f39e3dedbb73b5e8ca58b8790a9818d8d08f0964fa4c1bc5528d9ea062a76293cdf101d43fbd0790ed8bf7fca9c251825a4ce7d61ae
SSDEEP:	6144:w7XxnWJoyJuoMQF9CxX/tO7JS4PIcJaL:w7BnkRMQHg/tGTPBU
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........#...B...B...B..L^...B...`...B...d...B..Rich.B..........PE..L.....TR.................@...`......h........P....@.............B..

File Icon



Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401868
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x52548ACC [Tue Oct 8 22:44:28 2013 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:	c727a98e677fb7bd25bb06d2a2d956f1

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x43690	0x44000	False	0.670539407169	data	7.17479842318	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x45000	0xaf0	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x46000	0x4562	0x5000	False	0.3958984375	data	4.60998662802	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: AfWu3i35ny.exe PID: 4536 Parent PID: 5552

General

Start time:	12:08:38
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\AfWu3i35ny.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\AfWu3i35ny.exe'
Imagebase:	0x400000
File size:	307200 bytes
MD5 hash:	25AA37E21C29B7CFF02509533B585ED7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.834854327.00000000021C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000000.306440334.0000000000401000.00000020.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000000.306440334.0000000000401000.00000020.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000000.306440334.0000000000401000.00000020.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.833081784.0000000000401000.00000020.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.833081784.0000000000401000.00000020.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.833081784.0000000000401000.00000020.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis