ID: 458362
Sample Name: ftyaXQevlQ.exe
Cookbook: default.jbs
Time: 09:45:19
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

Windows Analysis Report ftyaXQevlQ.exe

Overview

General Information

Sample Name:	ftyaXQevlQ.exe
Analysis ID:	458362
MD5:	7a90c8f725811e5.
SHA1:	d09f363cefebf38…
SHA256:	2d2796f4298b67f..
Tags:	exe
Infos:	

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

GuLoader

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Found malware configuration
Multi AV Scanner detection for subm…
Yara detected GuLoader
C2 URLs / IPs found in malware con…
Contains functionality to detect hard…
Found potential dummy code loops (…
Machine Learning detection for samp…
Tries to detect virtualization through…
Abnormal high CPU Usage
Contains functionality for execution …
Contains functionality to call native f…
Contains functionality to query CPU …

Classification
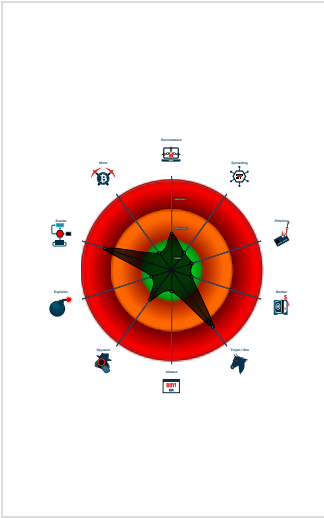
Process Tree

- **System is w10x64**
- ftyaXQevlQ.exe (PID: 6588 cmdline: 'C:\Users\user\Desktop\ftyaXQevlQ.exe' MD5: 7A90C8F725811E53A27ECB8E2C6A952B)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://101.99.94.119/WEALTHKELLS_QhOVDYr246"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.1173739995.00000000020 F0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re S E
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 3 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	R Tr W A
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Software Packing 1	LSASS Memory	Virtualization/Sandbox Evasion 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	R W A
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	O D C B
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	System Information Discovery 2 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Behavior Graph

Behavior Graph

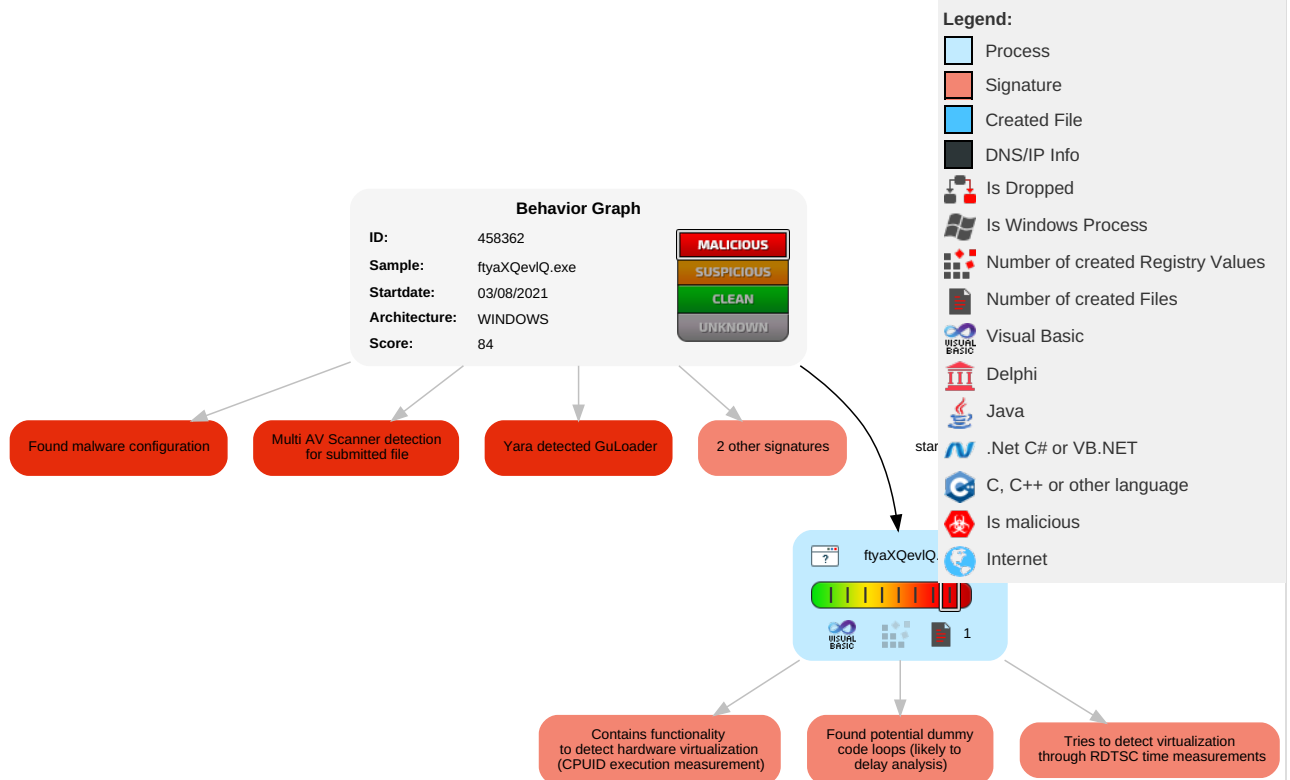|	
ID:	458362
Sample:	ftyaXQevlQ.exe
Startdate:	03/08/2021
Architecture:	WINDOWS
Score:	84

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected GuLoader

2 other signatures

started

ftyaXQevlQ.

Visual Basic — 1

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Found potential dummy code loops (likely to delay analysis)

Tries to detect virtualization through RDTSC time measurements

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
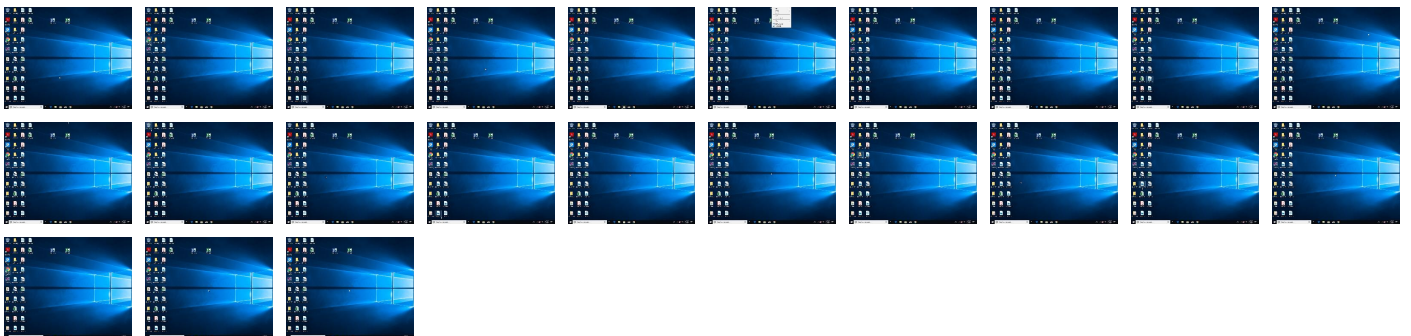
Screenshots

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
ftyaXQevlQ.exe	24%	Virustotal		Browse
ftyaXQevlQ.exe	21%	ReversingLabs	Win32.Trojan.Vebzenpak	
ftyaXQevlQ.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://101.99.94.119/WEALTHKELLS_QhOVDYr246	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://101.99.94.119/WEALTHKELLS_QhOVDYr246	true	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458362
Start date:	03.08.2021
Start time:	09:45:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ftyaXQevlQ.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:	15
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:	mal84.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 3.7% (good quality ratio 1.7%) • Quality average: 21.5% • Quality standard deviation: 28.9%
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):	6.64426057840022
TrID:	- Win32 Executable (generic) a (10002005/4) 99.96% - 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:	ftyaXQevlQ.exe
File size:	114688
MD5:	7a90c8f725811e53a27ecb8e2c6a952b
SHA1:	d09f363cefebf3877a29f250fba3ba7affe6549f
SHA256:	2d2796f4298b67f77555e446cfe4eca0559ddee6cdf6371524051a42f8dbd291
SHA512:	3bc71a4b42afbc5dc2423a9a75c325f08d3b2bfd2560d02d28fb5954786e932d2375434df8f761af2dd39bb47cfbd349efbe583dbfd2a34dccaffeb19d34354c
SSDEEP:	1536:Pe4mNWSCMiBwblmQEPpzjASVevRvGDmjkQmiPYnSigBwqSSCEe4mN:cRiOgAoevJGCj+n0Oq9
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...Cx.M.................@..........D........P....@................

File Icon

Icon Hash:	d5d5959595d5d595

Static PE Info

General

Entrypoint:	0x401144
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:	0x4D157843 [Sat Dec 25 04:51:15 2010 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:	5565993a5a9f2bfb76f28ab304be6bc1

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x13e24	0x14000	False	0.649719238281	data	7.06319493547	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x15000	0x115c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x17000	0x5b9e	0x6000	False	0.546020507812	data	6.0337725973	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
Chinese	Taiwan	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: ftyaXQevlQ.exe PID: 6588 Parent PID: 5908

General

Start time:	09:46:08
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\ftyaXQevlQ.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ftyaXQevlQ.exe'
Imagebase:	0x400000
File size:	114688 bytes
MD5 hash:	7A90C8F725811E53A27ECB8E2C6A952B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.1173739995.00000000020F0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities   Show Windows behavior

Disassembly

Code Analysis

Joe Sandbox Cloud Basic 33.0.0 White Diamond