ID: 433989
Sample Name: EXErprijFY
Cookbook: default.jbs
Time: 09:17:28
Date: 14/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

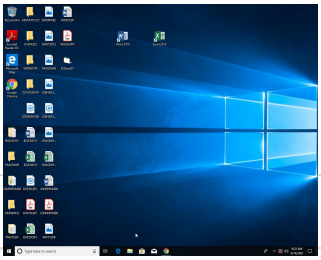
Analysis Report EXErprijFY

Overview

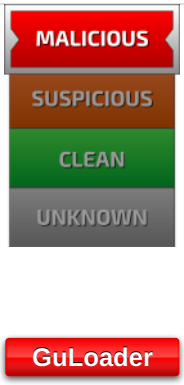
General Information

Sample Name:	EXErprijFY (renamed file extension from none to exe)
Analysis ID:	433989
MD5:	ee83942376ea57..
SHA1:	ec75b10c6ef046c..
SHA256:	b3498937a71913..
Tags:	32 exe GuLoader trojan
Infos:	

Most interesting Screenshot:



Detection

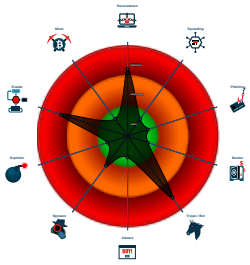


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Found malware configuration
- Potential malicious icon found
- Yara detected GuLoader
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Detected RDTSC dummy instruction…
- Found potential dummy code loops (…
- Tries to detect virtualization through…
- Abnormal high CPU Usage
- Creates a DirectInput object (often fo…

Classification



Process Tree

- **System is w10x64**
- EXErprijFY.exe (PID: 6896 cmdline: 'C:\Users\user\Desktop\EXErprijFY.exe' MD5: EE83942376EA5717149517FCC832AB9F)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://bara-seck.com/bin_NpuMLUuCfC62.bin, http://farmersschool.ge/bin_NpuMLUuCfC62.bin"
}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
EXErprijFY.exe	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.1164652170.00000000022 30000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.EXErprijFY.exe.400000.0.unpack	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

Source	Rule	Description	Author	Strings
0.2.EXErprijFY.exe.400000.0.unpack	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Found malware configuration

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Potential malicious icon found

Data Obfuscation:

Yara detected GuLoader

Yara detected GuLoader

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

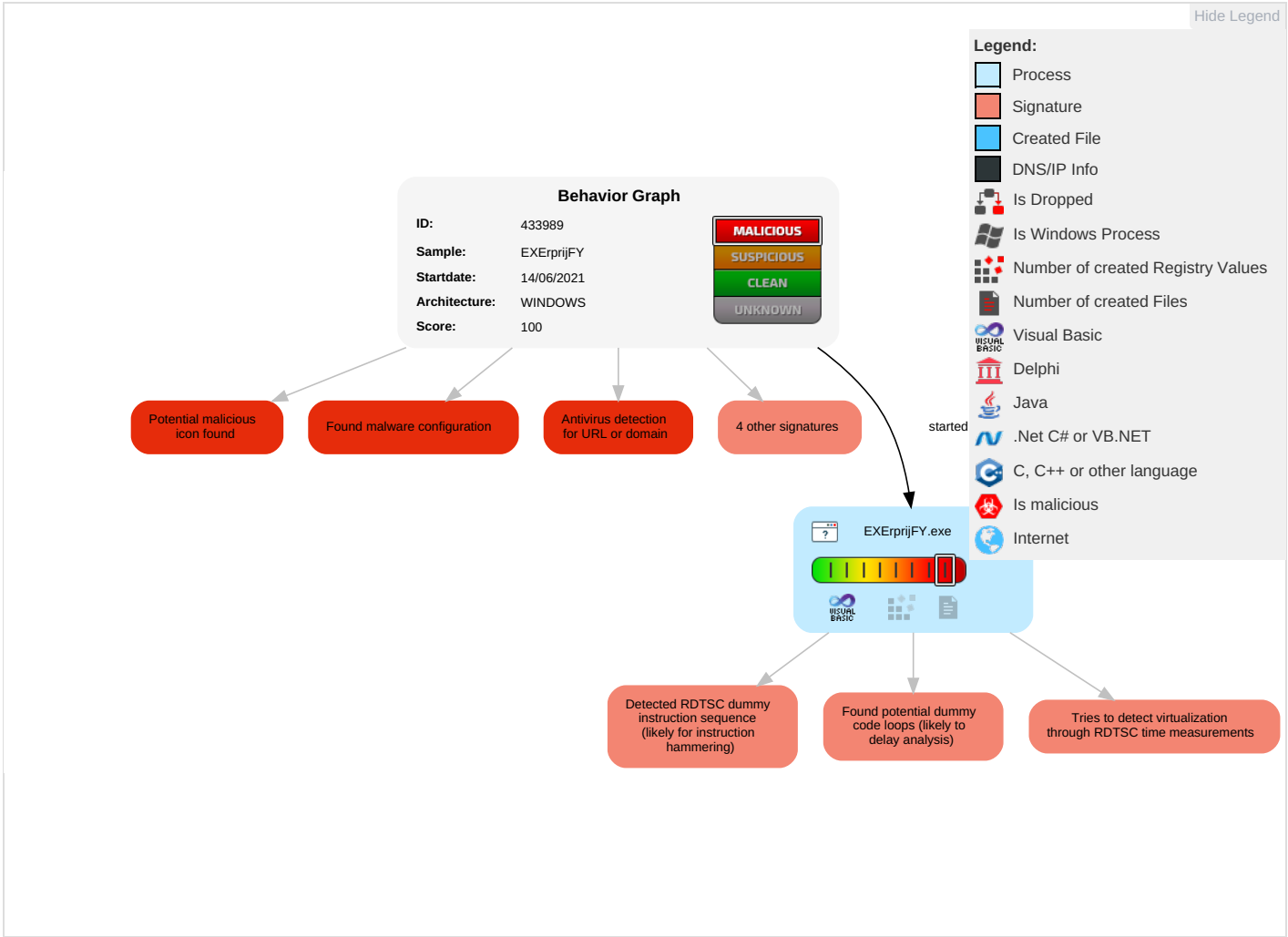
Found potential dummy code loops (likely to delay analysis)

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 Se Ef
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	Input Capture 1	Security Software Discovery 3	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	Process Injection 1	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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Ef
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 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)	Binary Padding	NTDS	System Information Discovery 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

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
EXErprijFY.exe	9%	ReversingLabs	Win32.Malware.Generic	
EXErprijFY.exe	100%	Avira	HEUR/AGEN.1134908	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.EXErprijFY.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1134908		Download File
0.0.EXErprijFY.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1134908		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://bara-seck.com/bin_NpuMLUuCfC62.bin, farmersschool.ge/bin_NpuMLUuCfC62.bin	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://bara-seck.com/bin_NpuMLUuCfC62.bin, farmersschool.ge/bin_NpuMLUuCfC62.bin	true	• Avira URL Cloud: malware	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433989
Start date:	14.06.2021
Start time:	09:17:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	EXErprijFY (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	17
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: 44.8% (good quality ratio 14.8%) • Quality average: 16.1% • Quality standard deviation: 26.4%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • 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):	5.822963661672907
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:	EXErprijFY.exe
File size:	147456
MD5:	ee83942376ea5717149517fcc832ab9f
SHA1:	ec75b10c6ef046cb63eaa20470ac94529fb4873a
SHA256:	b3498937a71913d7101fafb04eb48a791106bec97e2183 b2e1be8bb55a3f5fc
SHA512:	431cdd7e43fd6a4c4df862297eebc42e9cb68909647b572 88a63bfe036d9d0560cc0e97d759bda096e1389e3cd18d 243e627cce692660e2a384be430623b2551
SSDEEP:	1536:zK7pvMMhAYlnYgtuELhUQwe6KjEw5bMNccnuM G5reMFbCJQ:zCBqg197dvjEw5yccw5r7d
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...@.`R.....0..... ....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x4018a4
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:	0x5260BB40 [Fri Oct 18 04:38:24 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:	2c08d8f9644132654eb702b279083d5c

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x20e9c	0x21000	False	0.381784150095	data	6.07881532282	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x22000	0x1278	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x24000	0x930	0x1000	False	0.16943359375	data	2.02923021572	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
English	United States	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: EXErprijFY.exe PID: 6896 Parent PID: 5956

General

Start time:	09:18:13
Start date:	14/06/2021
Path:	C:\Users\user\Desktop\EXErprijFY.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\EXErprijFY.exe'
Imagebase:	0x400000
File size:	147456 bytes
MD5 hash:	EE83942376EA5717149517FCC832AB9F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.1164652170.0000000002230000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis