

JOeSandbox Cloud BASIC



ID: 434546

Sample Name:

fN2QHk2XYG.exe

Cookbook: default.jbs

Time: 08:36:46

Date: 15/06/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report fN2QHk2XYG.exe	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Threatname: GuLoader	3
Yara Overview	3
Memory Dumps	3
Sigma Overview	3
Signature Overview	3
AV Detection:	4
Networking:	4
System Summary:	4
Data Obfuscation:	4
Malware Analysis System Evasion:	4
Anti Debugging:	4
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	7
Contacted Domains	7
Contacted IPs	7
General Information	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	8
IPs	8
Domains	8
ASN	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	8
General	8
File Icon	8
Static PE Info	8
General	9
Entrypoint Preview	9
Data Directories	9
Sections	9
Resources	9
Imports	9
Version Infos	9
Possible Origin	9
Network Behavior	9
Code Manipulations	9
Statistics	9
System Behavior	10
Analysis Process: fN2QHk2XYG.exe PID: 6652 Parent PID: 5984	10
General	10
Disassembly	10
Code Analysis	10

Windows Analysis Report fN2QHk2XYG.exe

Overview

General Information

Sample Name:

fN2QHk2XYG.exe

Analysis ID:

434546

MD5:

3d900d56e0e828..

SHA1:

bf0e7023d260fb5..

SHA256:




686b8fac1748af7..

Tags:

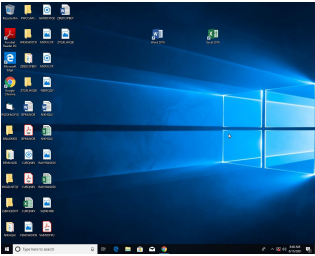
exe

GuLoader

Infos:

Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

GuLoader

Score:

92

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Antivirus / Scanner detection for sub...

Found malware configuration

Multi AV Scanner detection for subm...

Potential malicious icon found

Yara detected GuLoader

C2 URLs / IPs found in malware con...

Found potential dummy code loops (...)

Tries to detect virtualization through...

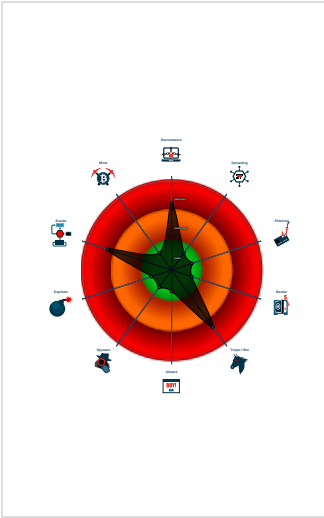
Abnormal high CPU Usage

Detected potential crypto function

PE file contains strange resources

Program does not show much activi...

Classification



Process Tree

System is w10x64

 fN2QHk2XYG.exe (PID: 6652 cmdline: 'C:\Users\user\Desktop\fn2QHk2XYG.exe' MD5: 3D900D56E0E8284F5FEA7752051FE727)

cleanup

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://theater.expodium.net/wp-content/plugins/m/agent_RgbAiUJQ186.bin, https://meatflesh.com/b/agent_RgbAiUJQ186.bin"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.696727696.000000000218 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

AV Detection:



Antivirus / Scanner detection for submitted sample

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:



C2 URLs / IPs found in malware configuration

System Summary:



Potential malicious icon found

Data Obfuscation:



Yara detected GuLoader

Malware Analysis System Evasion:



Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

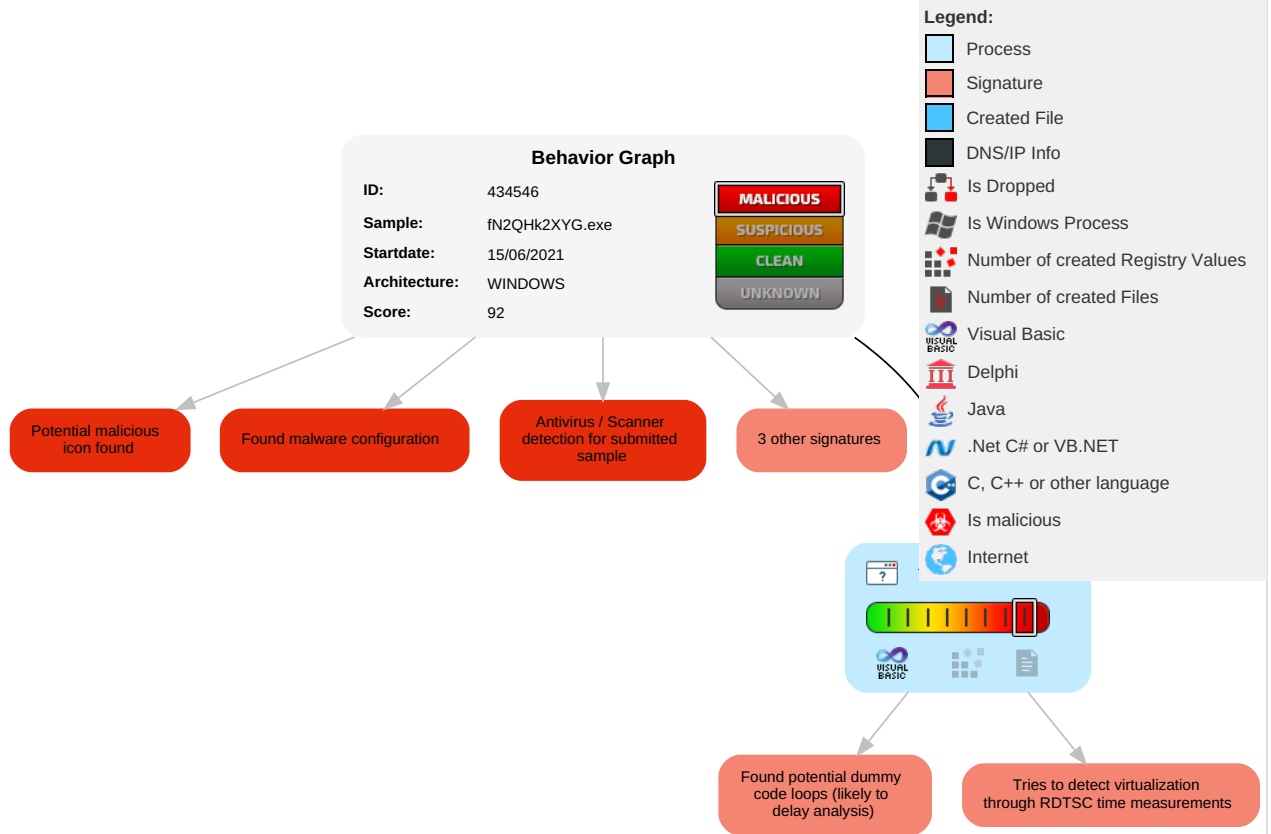


Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Recovery
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Recovery
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	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Recovery
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	Recovery
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Recovery

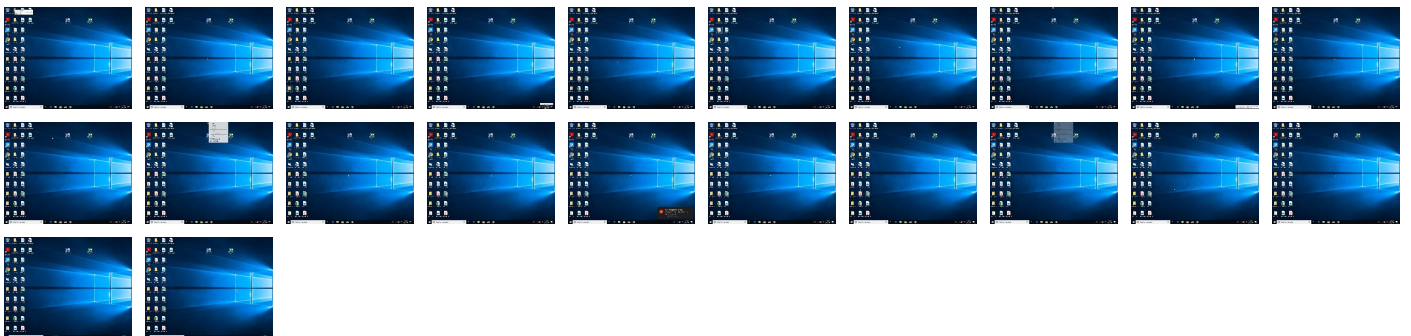
Behavior Graph



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
fN2QHk2XYG.exe	36%	VirusTotal		Browse
fN2QHk2XYG.exe	24%	ReversingLabs	Win32.Trojan.Graftor	
fN2QHk2XYG.exe	100%	Avira	HEUR/AGEN.1134908	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.fN2QHk2XYG.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1134908		Download File
0.0.fN2QHk2XYG.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1134908		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	434546
Start date:	15.06.2021
Start time:	08:36:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	fN2QHk2XYG.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:	18
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:	<ul style="list-style-type: none">• HCA enabled• EGA enabled• HDC enabled• AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal92.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none">• Successful, ratio: 34.2% (good quality ratio 15.7%)• Quality average: 19.8%• Quality standard deviation: 23.2%
HCA Information:	Failed
Cookbook Comments:	<ul style="list-style-type: none">• 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):	5.8068117659035945
TrID:	<ul style="list-style-type: none">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:	fN2QHk2XYG.exe
File size:	147456
MD5:	3d900d56e0e8284f5fea7752051fe727
SHA1:	bf0e7023d260fb580b0ad196d6135d4e5f34968c
SHA256:	686b8fac1748af72f6e0a35af456c7f473de446ba5df5430411c9ffd4c8943a0
SHA512:	2e41dd45b4ca614fea7e4129b99365d795546931b24a11681bdf123547a7923c7baf3fc95dad4a362ab3a748651aa019f1ce934bbe908796e5300b2592c05ef
SSDEEP:	1536:odUkRSto0lStokgoofDDTTMpK31whjEVsZCmsRfJeyftNB6zy:0GoFgX//31whqsZafJR9
File Content Preview:	MZ.....@.....!..!Th is program cannot be run in DOS mode...\$.....#...B...B ...B..L^..B...`...B...d...B..Rich.B.....PE..L....G.W.....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:	0x57AB47F9 [Wed Aug 10 15:27:53 2016 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	0x20cfc	0x21000	False	0.381495620265	data	6.06044220649	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	0x948	0x1000	False	0.172607421875	data	2.02366150258	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: fn2QHk2XYG.exe PID: 6652 Parent PID: 5984

General

Start time:	08:37:36
Start date:	15/06/2021
Path:	C:\Users\user\Desktop\fn2QHk2XYG.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\fn2QHk2XYG.exe'
Imagebase:	0x400000
File size:	147456 bytes
MD5 hash:	3D900D56E0E8284F5FEA7752051FE727
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	<ul style="list-style-type: none">Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.696727696.0000000002180000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis