ID: 530857
Sample Name: CI_PL_BL_
4100675407_xls.exe
Cookbook: default.jbs
Time: 03:30:24
Date: 30/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2021

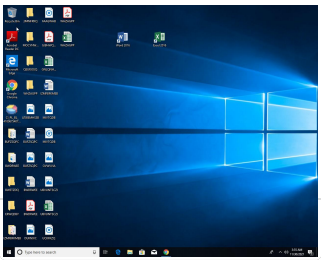
Windows Analysis Report CI_PL_BL_ 4100675407_xls.e…

Overview

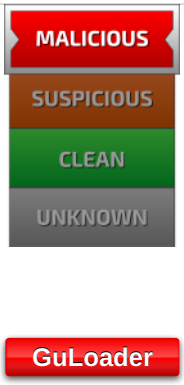
General Information

Sample Name:	CI_PL_BL_ 4100675407_xls.exe
Analysis ID:	530857
MD5:	94cb19d0951996..
SHA1:	fa319fb54dfb0b1…
SHA256:	4ff14d83a926458..
Tags:	exe guloader
Infos:	

Most interesting Screenshot:



Detection



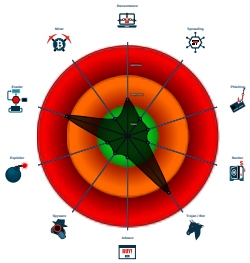
GuLoader

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Found potential dummy code loops (…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- Sample file is different than original …
- PE file contains strange resources
- Contains functionality to read the PEB
- Program does not show much activi…
- Uses code obfuscation techniques (…
- Contains functionality for execution …

Classification



Process Tree

- **System is w10x64**
- CI_PL_BL_ 4100675407_xls.exe (PID: 1556 cmdline: "C:\Users\user\Desktop\CI_PL_BL_ 4100675407_xls.exe" MD5: 94CB19D0951996CDB8B4CB914248763E)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://bgreenidaho.com/Crur/bin_TLiGMZYC180.bin"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.1175743788.00000000021A0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Copyright Joe Security LLC 2021

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

C2 URLs / IPs found in malware configuration

Data Obfuscation:

Yara detected GuLoader

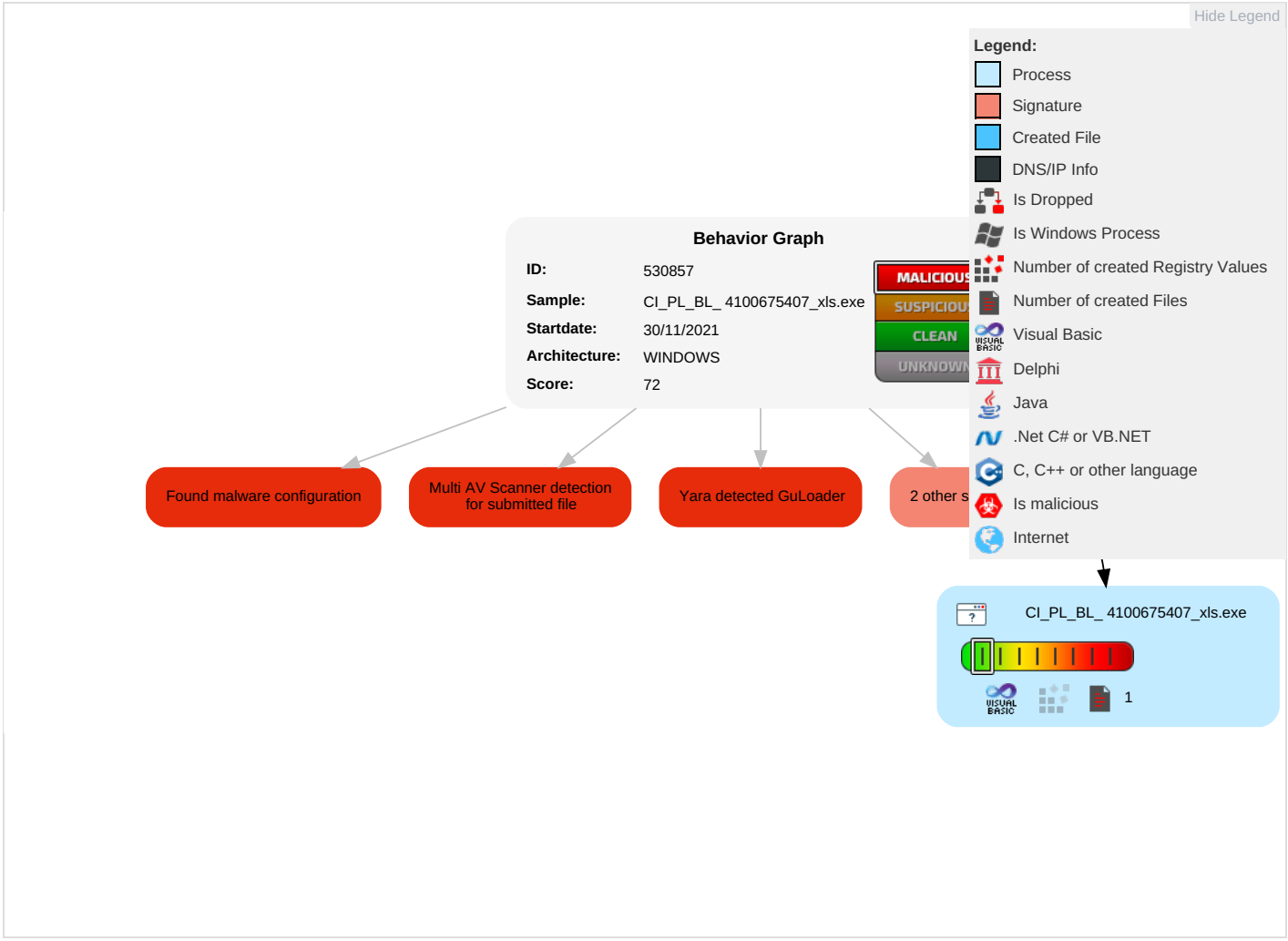
Anti Debugging:

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	R S E
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	R T W A
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	R W W A
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	O D C B
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 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
CI_PL_BL_ 4100675407_xls.exe	36%	ReversingLabs	Win32.Trojan.Shelsy	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://bgreenidaho.com/Crur/bin_TLiGMZYC180.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://bgreenidaho.com/Crur/bin_TLiGMZYC180.bin	true	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	530857
Start date:	30.11.2021
Start time:	03:30:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CI_PL_BL_ 4100675407_xls.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:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal72.troj.evad.winEXE@1/1@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 3.7% (good quality ratio 0%) • Quality average: 0% • Quality standard deviation: 0%
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

Copyright Joe Security LLC 2021

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\~DF86C6EDC191096B55.TMP	
Process:	C:\Users\user\Desktop\CI_PL_BL_ 4100675407_xls.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.8889429216618719
Encrypted:	false
SSDEEP:	12:rl3lKFQCb77aqWPp8aFW3gJH6OXkDgIOJefKadcMqpwbmHZbGzJzzz/jP5prGI:rQYH6OCgLAMibm5bGzJzX/
MD5:	E114AD50630A185807BCDFF5F7DACEF6
SHA1:	5091C562986C0A729FF4AC836083EFFBB4257977
SHA-256:	8C0B8DE53510102223758C6543D9EB102BC7423B83BDF902975FB221AB77E945
SHA-512:	F8C4FA0ABA5BD5CE8246A9C2A0A525129B5461E90634FE406A1704F8E42240174C6D1D8CCBC42EBE14EE777F79A5C7E32618CC2ED532CA6264D614337840BF1 A
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.045005360835647
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:	CI_PL_BL_ 4100675407_xls.exe
File size:	143360

Copyright Joe Security LLC 2021

General

MD5:	94cb19d0951996cdb8b4cb914248763e
SHA1:	fa319fb54dfb0b1f715a19924087cacef22ccbcf
SHA256:	4ff14d83a926458439f039ea2e756a646b2bb63be4fd22ed8559138214efcaf8
SHA512:	b06b3df9de83932c9f5013ce90720710ba9645c5bcce4b46dd377c541343b8095742a7923634805a61214ba1eda4ac3ecaaee935b73942c53c27190e792dc007
SSDEEP:	1536:5oDAE4euYT88tnh07k177v10aeb/by8W1hgW3rAITGLKy:ZEvuYT8CQm/v10aeixxCKy
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7b..s...s...s.....r...<!..v...E%..r...Richs.....PE..L.....G.....0.....@

File Icon

Icon Hash:	28f0da9af0f0f034

Static PE Info

General

Entrypoint:	0x4016a4
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:	0x47BEE20B [Fri Feb 22 14:54:03 2008 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:	9b824bd6da8a9367fa6d96e7ab5dc79d

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1f7cc	0x20000	False	0.547492980957	data	6.30287654494	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x21000	0x19ec	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x23000	0xf3e	0x1000	False	0.27490234375	data	3.55639650835	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: CI_PL_BL_ 4100675407_xls.exe PID: 1556 Parent PID: 5836

General

Start time:	03:31:14
Start date:	30/11/2021
Path:	C:\Users\user\Desktop\CI_PL_BL_ 4100675407_xls.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\CI_PL_BL_ 4100675407_xls.exe"
Imagebase:	0x400000
File size:	143360 bytes
MD5 hash:	94CB19D0951996CDB8B4CB914248763E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.1175743788.00000000021A0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021