ID: 539387
Sample Name: SWIFT_ACK-89813.02.exe
Cookbook: default.jbs
Time: 08:26:42
Date: 14/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

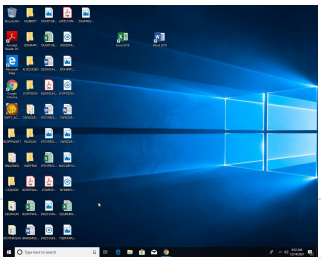
Windows Analysis Report SWIFT_ACK-89813.02.exe

Overview

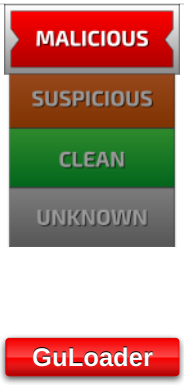
General Information

Sample Name:	SWIFT_ACK-89813.02.exe
Analysis ID:	539387
MD5:	2f19182da895afc..
SHA1:	7d111bd6284cdd..
SHA256:	24d5129d6ecbe5..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

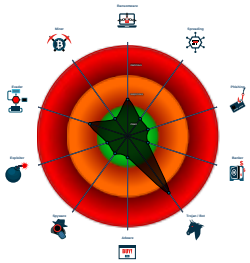


Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- Contains functionality to call native f…
- Sample file is different than original …
- PE file contains strange resources
- Contains functionality to read the PEB
- Uses code obfuscation techniques (…
- Contains functionality for execution …
- Abnormal high CPU Usage
- Detected potential crypto function

Classification



Process Tree

- **System is w10x64**
- SWIFT_ACK-89813.02.exe (PID: 6420 cmdline: "C:\Users\user\Desktop\SWIFT_ACK-89813.02.exe" MD5: 2F19182DA895AFC914C7B9851A4F2D49)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?expor"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.824783872.00000000023F0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Networking:

C2 URLs / IPs found in malware configuration

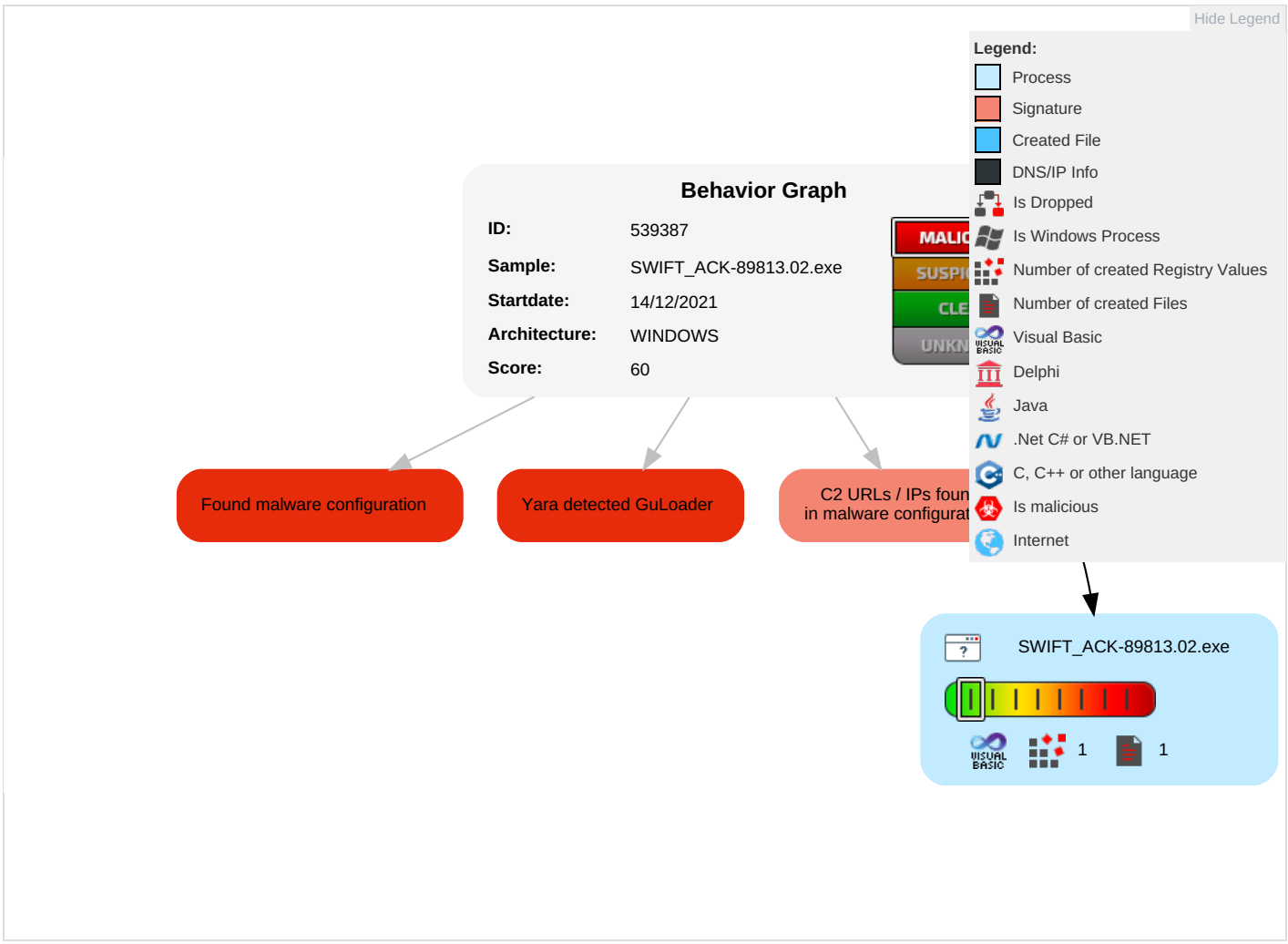
Data Obfuscation:

Yara detected GuLoader

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impa
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Software Packing 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modi Syst Parti
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Devi Lock
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Dele Devi Data

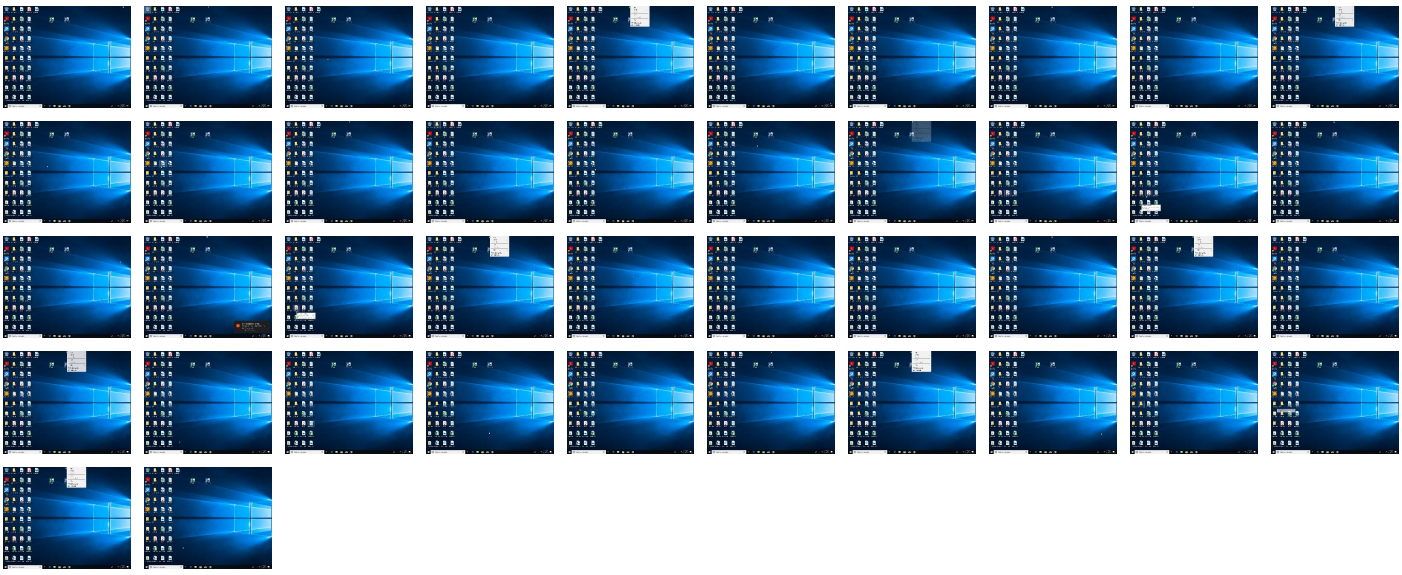
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

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:	34.0.0 Boulder Opal
Analysis ID:	539387
Start date:	14.12.2021
Start time:	08:26:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SWIFT_ACK-89813.02.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:	mal60.troj.winEXE@1/1@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 38% (good quality ratio 24%) • Quality average: 36.6% • Quality standard deviation: 33.5%
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

C:\Users\user\AppData\Local\Temp\~DFA1C4850DA9C6EF9A.TMP	
Process:	C:\Users\user\Desktop\SWIFT_ACK-89813.02.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.9710024410534099
Encrypted:	false
SSDEEP:	24:rohDKrA3iuOH/3+apRIJ0lBefVYyy/iolnBX2Vr:r4KrAyx5o03weyy/iolnB2
MD5:	52AA63688AAC03A75A4231F6519EBA14
SHA1:	7BAA47908391E462A575DF51EBCE7F3EFF076B17
SHA-256:	FB8C5BC990C88E0716500458D7685B934A75580DDB42DDC9D616FF0E2A2E6ADC
SHA-512:	0F59A09835916E6B556EF8B31E74776105FCD0A3E0BBF77015A39720E5C2C31C3E825DEE7989D3284281713CA0621673A0C7B1E5B10351C627910905B3C4B203
Malicious:	false
Reputation:	low
Preview:	.....>..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.88855983952812
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:	SWIFT_ACK-89813.02.exe
File size:	167936
MD5:	2f19182da895afc914c7b9851a4f2d49
SHA1:	7d111bd6284cdd87498e72d90a595aea9fc35d5d
SHA256:	24d5129d6ecbe5ba5e88077d1207bc09fc68d076dea00892bc614a267f9f0b1b
SHA512:	33d80fe64688914261600b5de5ba2f984206c0574db2dc357da3966429034e23ea06308f30d399564a8b4a49ed521c27584f7b0d43445c7eaad00ff178edbb52

General

SSDEEP:	1536:w4P8PO3YuBX0051Zy0U4SfGaIsmJNa+I37KTqzc9TPVhp4N3L32DdX0:nP8mVVztUjBmJNS7hzc9c32DdX0
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W.x.....\.....%.....Rich.....PE..L...E.7W.....`...P.....\.....p....@

File Icon

Icon Hash:	93f1e4c8d2e4f9fb

Static PE Info

General

Entrypoint:	0x40195c
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:	0x57371745 [Sat May 14 12:17:09 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:	e7597de960f525af7c9e8aa5873fcec3

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x25ba0	0x26000	False	0.556775544819	data	7.1391806469	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x27000	0x36e4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2b000	0x850	0x1000	False	0.32080078125	data	3.07841521901	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: SWIFT_ACK-89813.02.exe PID: 6420 Parent PID: 5480

General

Start time:	08:28:33
Start date:	14/12/2021
Path:	C:\Users\user\Desktop\SWIFT_ACK-89813.02.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SWIFT_ACK-89813.02.exe"
Imagebase:	0x400000
File size:	167936 bytes
MD5 hash:	2F19182DA895AFC914C7B9851A4F2D49
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.824783872.00000000023F0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis