

JoeSandbox Cloud BASIC



ID: 434445

Sample Name: URGENT
SWIFT COPY FOR JUNE 14
2021.exe

Cookbook: default.jbs

Time: 00:30:18

Date: 15/06/2021

Version: 32.0.0 Black Diamond


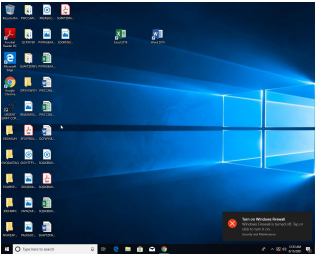
Table of Contents

Table of Contents	2
Windows Analysis Report URGENT SWIFT COPY FOR JUNE 14 2021.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	4
AV Detection:	4
Networking:	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 URLs	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	9
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	10
System Behavior	10
Analysis Process: URGENT SWIFT COPY FOR JUNE 14 2021.exe PID: 1304 Parent PID: 5728	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10

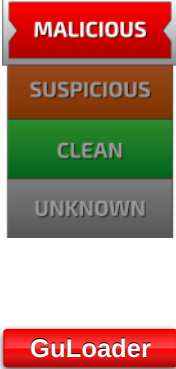
Windows Analysis Report URGENT SWIFT COPY FOR J...

Overview

General Information

Sample Name:	URGENT SWIFT COPY FOR JUNE 14 2021.exe
Analysis ID:	434445
MD5:	13fe879d4b0acd6.
SHA1:	c513f61b28a5602.
SHA256:	f3a520aa6296de5.
Tags:	exe
Infos:	
Most interesting Screenshot:	
	

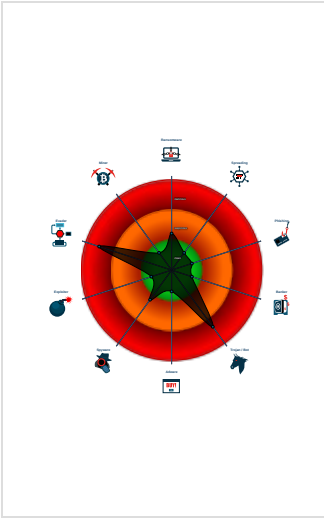
Detection

	
Score:	88
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...
Detected RDTSC dummy instruction...
Found potential dummy code loops (...)
Potentially malicious time measurem...
Tries to detect virtualization through...
Abnormal high CPU Usage
Contains functionality for execution ...
Contains functionality to call native f...

Classification



Process Tree

- System is w10x64
-  URGENT SWIFT COPY FOR JUNE 14 2021.exe (PID: 1304 cmdline: 'C:\Users\user\Desktop\URGENT SWIFT COPY FOR JUNE 14 2021.exe' MD5: 13FE879D4B0ACD6B10E9E4DB7FCF3A49)
- cleanup

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://onedrive.live.com/download?cid=BAC03012EC7BD279&resid=BAC03012EC7BD279%21114&authkey=AETxNDW7LlqQvxxw"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.575162168.00000000007D 0000.00000040.00000001.sdmmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Malware Analysis System Evasion:



Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:



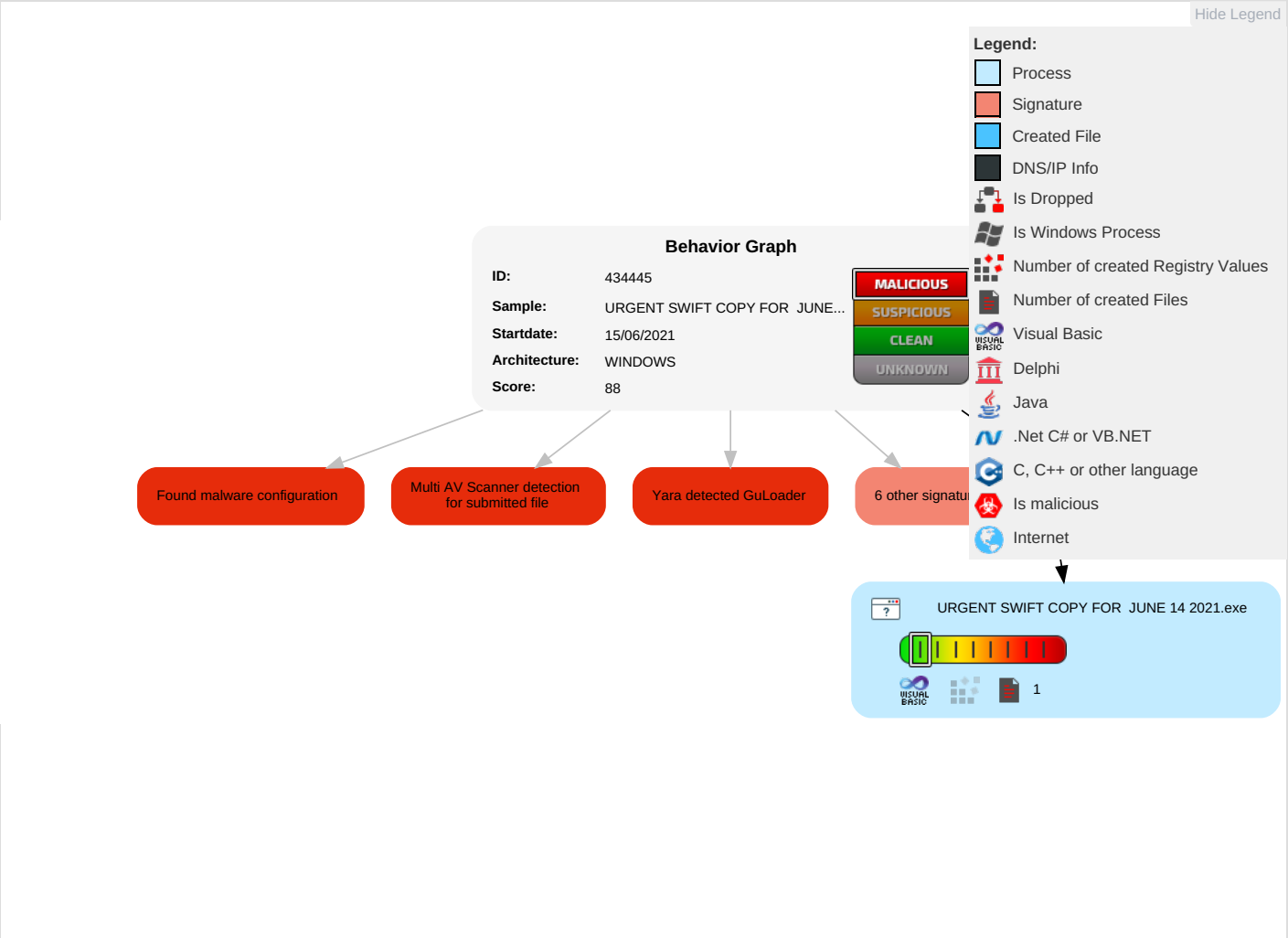
Found potential dummy code loops (likely to delay analysis)

Potentially malicious time measurement code found

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Reputation
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	Input Capture 1	Security Software Discovery 4 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Reputation
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	Reputation
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	Oldest
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Be

Behavior Graph





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
URGENT SWIFT COPY FOR JUNE 14 2021.exe	11%	ReversingLabs	Win32.Trojan.Wacatac	

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 URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com/download?cid=BAC03012EC7BD279&resid=BAC03012EC7BD279%21114&authkey=AETxWDW7LlqQv xw	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	434445
Start date:	15.06.2021
Start time:	00:30:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	URGENT SWIFT COPY FOR JUNE 14 2021.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:	28
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:	mal88.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none">• Successful, ratio: 2.5% (good quality ratio 0%)• Quality average: 0.1%• Quality standard deviation: 0.5%
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):	5.913443213153397
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:	URGENT SWIFT COPY FOR JUNE 14 2021.exe
File size:	270336
MD5:	13fe879d4b0acd6b10e9e4db7fcf3a49
SHA1:	c513f61b28a5602768fc3a07bea6efe0b743dc26
SHA256:	f3a520aa6296de59468c3a38d45660091097c056b7249a66d3443f3bd4ecf997
SHA512:	faade3ba99908dd10a0ca2f473dd55483256cdd38d795af6c1a41f97838a56f00f8cb4431477907cf099af2733893812c854b598575bd3b4dcf8970d8b61095f4
SSDEEP:	3072:HqCx EJQKX+an/XCf1Tth5P9+Zz3YaXygA1kkX31Z902v4:K3vCf1Bh51+Zsjgqdl8
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$......c.S.....&.....\$.Rich.....PE..L....}.H.....0.....{.....@.....

File Icon

	
Icon Hash:	2828baa9d2777576

Static PE Info

General

Entrypoint:	0x402894
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:	0x48F37DB6 [Mon Oct 13 16:56:22 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:	adaafa2c180ecb7addf1201d12c8322

Entrypoint Preview

Data Directories

Sections


Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x3e26c	0x3f000	False	0.288419208829	data	6.04648752589	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x40000	0x1be8	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x42000	0x9d8	0x1000	False	0.226806640625	data	2.09916860007	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: URGENT SWIFT COPY FOR JUNE 14 2021.exe PID: 1304 Parent
PID: 5728

General

Start time:	00:31:04
Start date:	15/06/2021
Path:	C:\Users\user\Desktop\URGENT SWIFT COPY FOR JUNE 14 2021.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\URGENT SWIFT COPY FOR JUNE 14 2021.exe'
Imagebase:	0x400000
File size:	270336 bytes
MD5 hash:	13FE879D4B0ACD6B10E9E4DB7FCF3A49
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: 00000000.00000002.575162168.00000000007D0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis