ID: 502575
Sample Name: correction
HAWB.exe
Cookbook: default.jbs
Time: 04:25:07
Date: 14/10/2021
Version: 33.0.0 White Diamond

Table of Contents

Windows Analysis Report correction HAWB.exe

Overview

General Information

Sample Name:	correction HAWB.exe
Analysis ID:	502575
MD5:	8a29580d47943a..
SHA1:	e4cdec934b4bfc2..
SHA256:	53c0cf2d25f350a..
Tags:	exe
Infos:	

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

GuLoader

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Found malware configuration

Potential malicious icon found

Yara detected GuLoader

Found potential dummy code loops (…

Machine Learning detection for samp…

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 (…

Classification
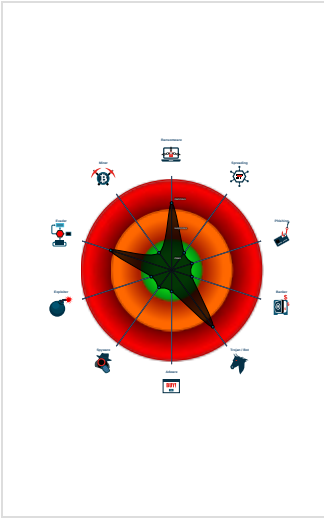
Process Tree

- **System is w10x64**
  - correction HAWB.exe (PID: 4784 cmdline: 'C:\Users\user\Desktop\correction HAWB.exe' MD5: 8A29580D47943A0F2C61CA552A63BC30)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=d"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.758213767.000000000211 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

AV Detection:

Found malware configuration

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Potential malicious icon found

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	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	Software Packing 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 A
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 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)	Deobfuscate/Decode Files or Information 1	NTDS	System Information Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

Behavior Graph

Behavior Graph

ID: 502575
Sample: correction HAWB.exe
Startdate: 14/10/2021
Architecture: WINDOWS
Score: 76

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

Legend:
- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

Potential malicious icon found

Found malware configuration

Yara detected GuLoader

3 other

correction HAWB.exe

Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.
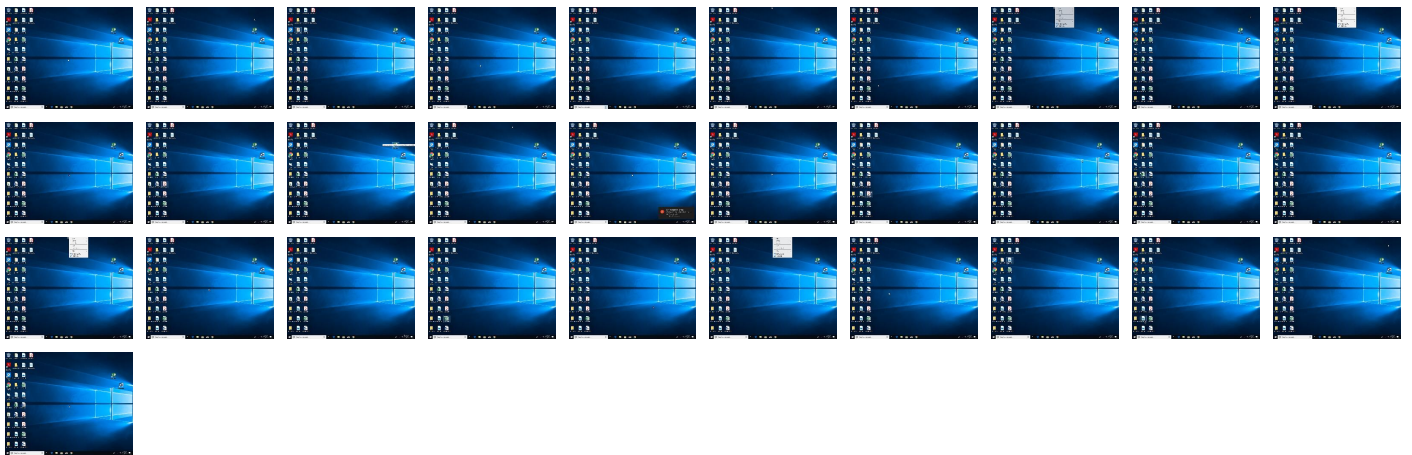
Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
correction HAWB.exe	100%	Joe Sandbox ML		

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:	33.0.0 White Diamond
Analysis ID:	502575
Start date:	14.10.2021
Start time:	04:25:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	correction HAWB.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:	32
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:	mal76.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	- Successful, ratio: 3.7% (good quality ratio 3%) - Quality average: 37.6% - Quality standard deviation: 20.2%
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

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.349869263832848
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:	correction HAWB.exe
File size:	135168
MD5:	8a29580d47943a0f2c61ca552a63bc30
SHA1:	e4cdec934b4bfc2e055216c03ac7056069100b05
SHA256:	53c0cf2d25f350a579729af76c466b68b899586b620ffae8 925fcb4d831dc2c8
SHA512:	358c751d102753fd81e1d527a438ca7aed36dec3d605e8 70a4bf3f3232027ae1d66db2c8c70771c6e781f3a52317d dec0e483b4dce501c5ef30cc1189f217177
SSDEEP:	1536:VTbVTmIJnm6UC/HuomaUi0gAC6/lHzDc7uWWD NvtKyUrWBeSVpynmKTGYFZnymht:V/VTVnbHJ/Tkl/e S3ybzH
File Content Preview:	MZ....................@...............................!..L.!Th is program cannot be run in DOS mode....$........#...B...B ...B..L^...B...`...B...d...B..Rich.B.........PE..L......Y............ ........`......h.............@.............B..

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401868

General

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:	0x59B6E088 [Mon Sep 11 19:14:16 2017 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:	c727a98e677fb7bd25bb06d2a2d956f1

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x19ee0	0x1a000	False	0.56938288762	data	6.82320580255	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1b000	0xaf0	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1c000	0x456a	0x5000	False	0.396240234375	data	4.60844428158	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: correction HAWB.exe PID: 4784 Parent PID: 5188

General

Start time:	04:25:59
Start date:	14/10/2021
Path:	C:\Users\user\Desktop\correction HAWB.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\correction HAWB.exe'
Imagebase:	0x400000
File size:	135168 bytes
MD5 hash:	8A29580D47943A0F2C61CA552A63BC30
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.758213767.0000000002110000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities   Show Windows behavior

Disassembly

Code Analysis

Joe Sandbox Cloud Basic 33.0.0 White Diamond