

ID: 501939
Sample Name: correction HAWB.exe
Cookbook: default.jbs
Time: 12:40:00
Date: 13/10/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report correction HAWB.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
Jbx Signature Overview 3
AV Detection: 4
Networking: 4
System Summary: 4
Data Obfuscation: 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 9
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 10
Code Manipulations 10
Statistics 10
System Behavior 10
Analysis Process: correction HAWB.exe PID: 4868 Parent PID: 2336 10
General 10
File Activities 10
Disassembly 10
Code Analysis 10

Copyright Joe Security LLC 2021

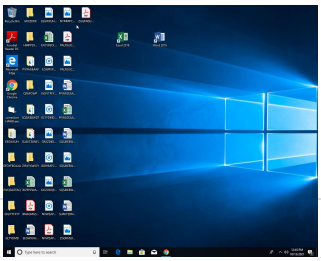
Windows Analysis Report correction HAWB.exe

Overview

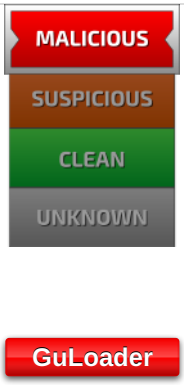
General Information

Sample Name:	correction HAWB.exe
Analysis ID:	501939
MD5:	a4ef1695bddce65.
SHA1:	3905f0749e1c55a.
SHA256:	64939ef2abe9b39.
Tags:	exe guloader
Infos:	

Most interesting Screenshot:



Detection

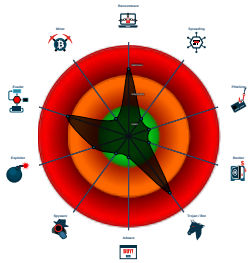


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Potential malicious icon found
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Found potential dummy code loops (…
- Uses 32bit PE files
- Found inlined nop instructions (likely…
- Sample file is different than original …
- PE file contains strange resources
- Contains functionality to read the PEB
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- correction HAWB.exe (PID: 4868 cmdline: 'C:\Users\user\Desktop\correction HAWB.exe' MD5: A4EF1695BDDCE6530A28E0D72AE7F8C4)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&M-"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.818731947.00000000020D0000.00000040.00000001.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

System Summary:



Potential malicious icon found

Data Obfuscation:



Yara detected GuLoader

Anti Debugging:

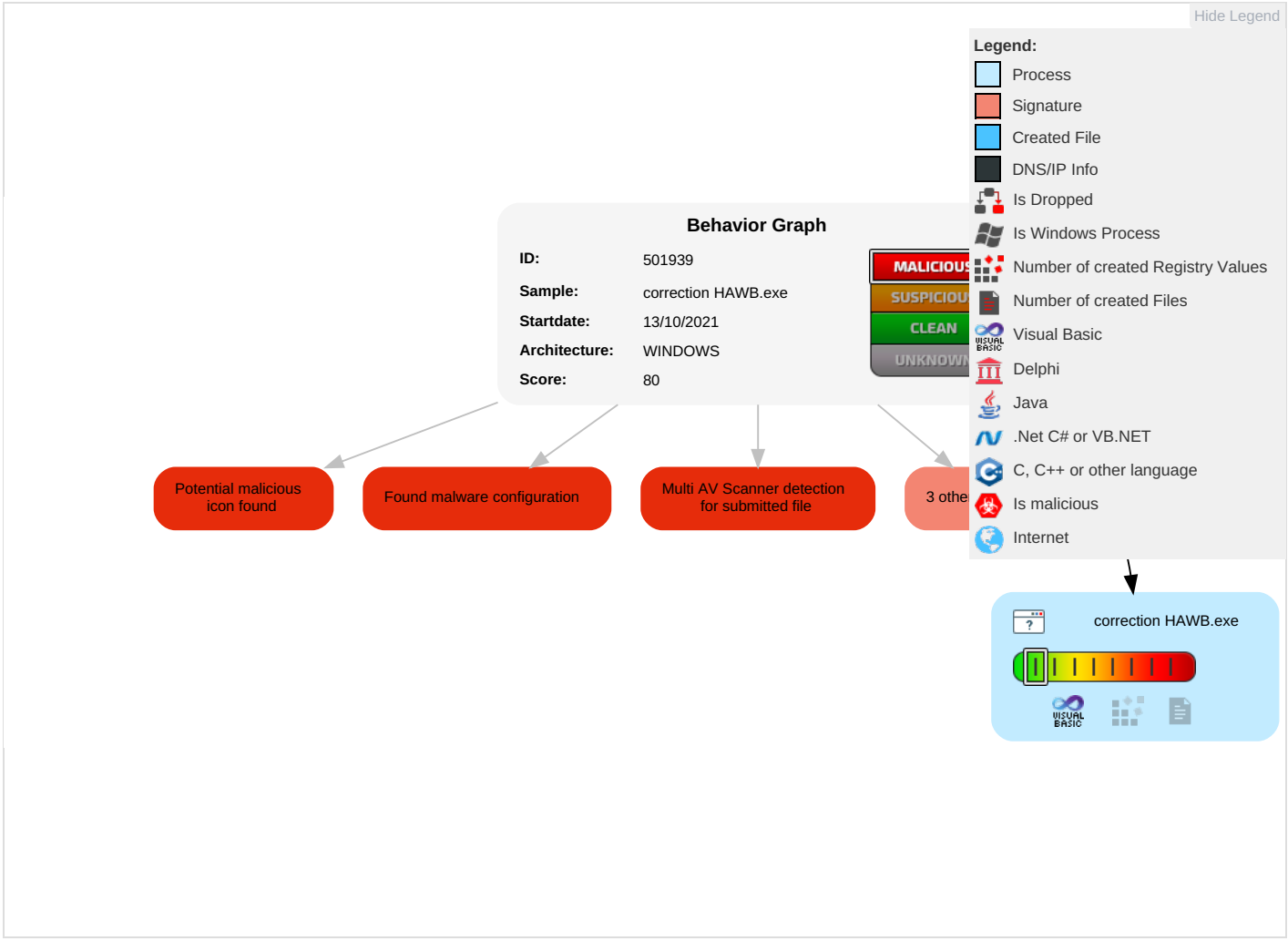


Found potential dummy code loops (likely to delay analysis)

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 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)	Deobfuscate/Decode 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)	Obfuscated Files or Information 3	NTDS	System Information Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

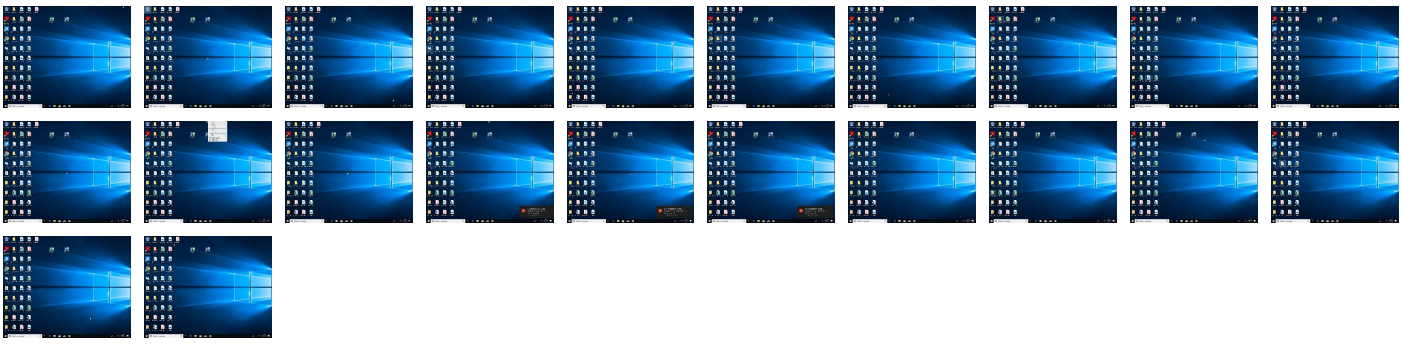
Behavior Graph



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
correction HAWB.exe	26%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
windowsupdate.s.llnwi.net	0%	Virustotal		Browse

URLs

No Antivirus matches

Copyright Joe Security LLC 2021

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
windowsupdate.s.llnwi.net	178.79.242.0	true	false	• 0%, Virustotal, Browse	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	501939
Start date:	13.10.2021
Start time:	12:40:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 47s
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:	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:	mal80.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.3% (good quality ratio 1.1%) • Quality average: 37.8% • Quality standard deviation: 19.8%
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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
windowsupdate.s.llnwi.net	Statement of Account.exe	Get hash	malicious	Browse	• 178.79.242.128
	Statement of Account.exe	Get hash	malicious	Browse	• 178.79.242.128
	jh6KzwrXQp.exe	Get hash	malicious	Browse	• 178.79.242.0
	heX1kOkwqy.exe	Get hash	malicious	Browse	• 178.79.242.0
	mixsix_20211013-084409.exe	Get hash	malicious	Browse	• 178.79.242.0
	2rd Quater Order Quotation.zip.xls	Get hash	malicious	Browse	• 178.79.242.128
	DOC REC EIPT.html	Get hash	malicious	Browse	• 178.79.242.128
	Efe-8 GPP Project Steel Pipe Tender.exe	Get hash	malicious	Browse	• 178.79.242.128
	emil.franchi@global.com #Ud83d#Udce0 VGX47BBSBJ44838.HTM	Get hash	malicious	Browse	• 178.79.242.128
	DHL Lieferschein,pdf.exe	Get hash	malicious	Browse	• 178.79.242.128
	Payment_MT103.exe	Get hash	malicious	Browse	• 178.79.242.0
	Doc-CS3.exe	Get hash	malicious	Browse	• 178.79.242.128
	SecuriteInfo.com.Suspicious.Win32.Save.a.28039.exe	Get hash	malicious	Browse	• 178.79.242.0
	oG3zl54AA5.exe	Get hash	malicious	Browse	• 178.79.242.128
	dNlT8STqLN.exe	Get hash	malicious	Browse	• 178.79.242.128
	Revised Quotation F657.exe	Get hash	malicious	Browse	• 178.79.242.0
	Quotation Request.pdf.exe	Get hash	malicious	Browse	• 178.79.242.0
	Proof of payment.jpg.exe	Get hash	malicious	Browse	• 178.79.242.128
	vk5MXd2Rxm.msi	Get hash	malicious	Browse	• 178.79.242.0
	jjBv8SpZXm.exe	Get hash	malicious	Browse	• 178.79.242.128

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):	6.269963148035969
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

General

File size:	139264
MD5:	a4ef1695bddce6530a28e0d72ae7f8c4
SHA1:	3905f0749e1c55ad4d8fb2a1969cf3f74bc0aeb4
SHA256:	64939ef2abe9b397b1f99bb4ba00c7e49be75f14013647c8e0605fb5fdb3b14b
SHA512:	8d29dfd66c896cfa378c4828f55b65f03d99091058d74214ce16f0a1592fbced48963424b9c526b8176d2cdd9f229477d9e54b9762e349576af5742a1aeb9578
SSDEEP:	1536:b60o3DE9DAGxjVgGRye1a8/RCqnDc2zp9f91pgSvcXvgsuY6FqJZ8wYut55mhLB:u0o36MBEyydnDjg4klut5M
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L...9e.T.....`.....h.....@.....B..

File Icon



Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401868
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:	0x54E06539 [Sun Feb 15 09:22:01 2015 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	0x1a180	0x1b000	False	0.552580656829	data	6.72479841323	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1c000	0xaf0	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1d000	0x456a	0x5000	False	0.396484375	data	4.60940282091	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: 4868 Parent PID: 2336

General

Start time:	12:40:57
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\correction HAWB.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\correction HAWB.exe'
Imagebase:	0x400000
File size:	139264 bytes
MD5 hash:	A4EF1695BDDCE6530A28E0D72AE7F8C4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.818731947.00000000020D0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021