

JOeSandbox Cloud BASIC



**ID:** 458358

**Sample Name:** Weemaes B.V.-  
PO74748392.exe

**Cookbook:** default.jbs

**Time:** 09:42:13

**Date:** 03/08/2021

**Version:** 33.0.0 White Diamond

## Table of Contents

Table of Contents	2
Windows Analysis Report Weemaes B.V.-PO74748392.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
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
Authenticode Signature	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: Weemaes B.V.-PO74748392.exe PID: 5656 Parent PID: 5700	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10

# Windows Analysis Report Weemaes B.V.-PO74748392.exe

## Overview

### General Information

Sample Name:

Weemaes B.V.-PO74748392.exe

Analysis ID:

458358

MD5:

a08f23a15ef10b1..

SHA1:

7cc53628714dd9..




SHA256:

cc8e7690934b90..

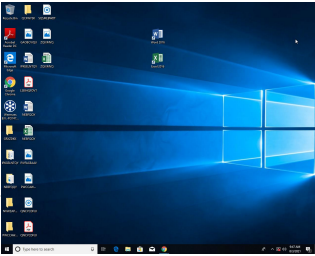
Tags:

exe

Infos:

Most interesting Screenshot:



### Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

GuLoader

Score:

84

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...

Found potential dummy code loops (...)

Potentially malicious time measurem...

Tries to detect virtualization through...

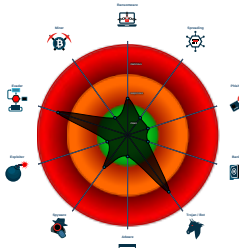
Abnormal high CPU Usage

Contains functionality for execution ...

Contains functionality to call native f...


Contains functionality to query CPU ...

### Classification



## Process Tree

System is w10x64

 Weemaes B.V.-PO74748392.exe (PID: 5656 cmdline: 'C:\Users\user\Desktop\Weemaes B.V.-PO74748392.exe' MD5: A08F23A15EF10B17370668CF5B9947AD)

cleanup

## Malware Configuration

Threatname: GuLoader

{

"Payload URL": "http://rossettlee.ddnsgeek.com/x/5bab0b1d864615bab0b1d864b3/2"

}

## Yara Overview

### Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.758678567.00000000021C 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

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)

Tries to detect virtualization through RDTSC time measurements

## Anti Debugging:



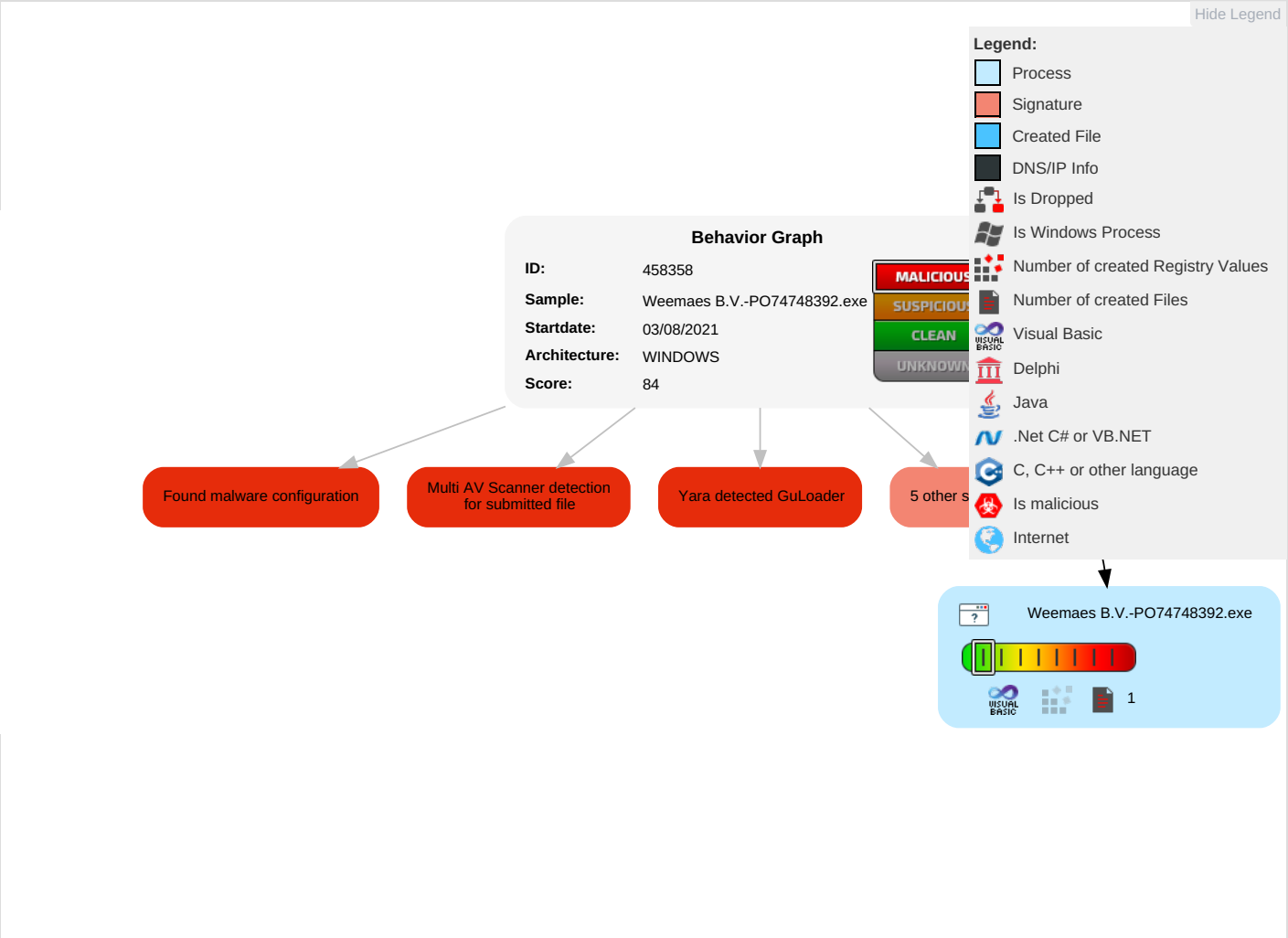
Found potential dummy code loops (likely to delay analysis)

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	OS Credential Dumping	Security Software Discovery 3 1	Remote Services	Archive Collected Data 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	Data from Removable Media	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	Reputation
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 2 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Reputation

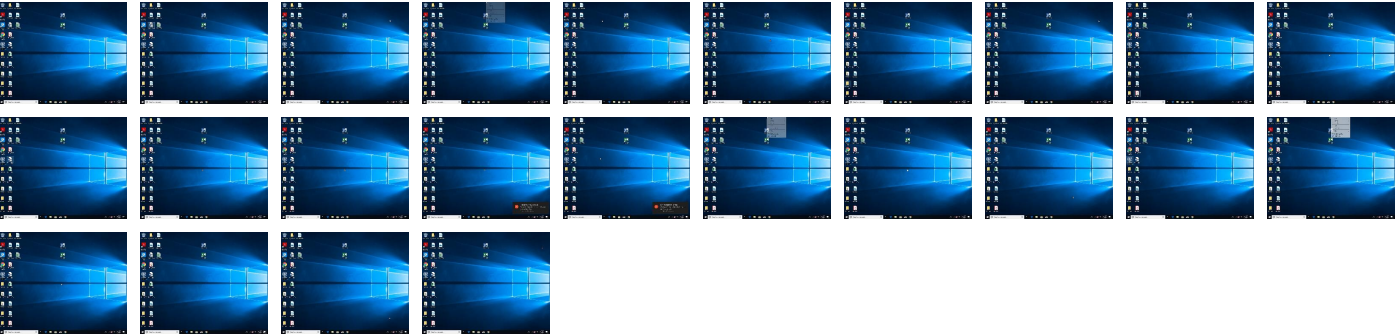
## Behavior Graph



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
Weemaes B.V.-PO74748392.exe	36%	Virustotal		<a href="#">Browse</a>

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

Source	Detection	Scanner	Label	Link
<a href="http://rossettle.dnsgeek.com/x/5bab0b1d864615bab0b1d864b3/2">http://rossettle.dnsgeek.com/x/5bab0b1d864615bab0b1d864b3/2</a>	0%	Avira URL Cloud	safe	

## Domains and IPs

### Contacted Domains

No contacted domains info

### Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
<a href="http://rossettlee.ddnsgeek.com/x/5bab0b1d864615bab0b1d864b3/2">http://rossettlee.ddnsgeek.com/x/5bab0b1d864615bab0b1d864b3/2</a>	true	<ul style="list-style-type: none"><li>Avira URL Cloud: safe</li></ul>	unknown

### Contacted IPs

No contacted IP infos

## General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458358
Start date:	03.08.2021
Start time:	09:42:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Weemaes B.V.-PO74748392.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:	25
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"><li>HCA enabled</li><li>EGA enabled</li><li>HDC enabled</li><li>AMSI enabled</li></ul>
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none"><li>Successful, ratio: 16.1% (good quality ratio 8.2%)</li><li>Quality average: 35.7%</li><li>Quality standard deviation: 39.3%</li></ul>
HCA Information:	Failed
Cookbook Comments:	<ul style="list-style-type: none"><li>Adjust boot time</li><li>Enable AMSI</li><li>Found application associated with file extension: .exe</li><li>Override analysis time to 240s for sample files taking high CPU consumption</li></ul>
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):	6.023550955444461
TrID:	<ul style="list-style-type: none"><li>Win32 Executable (generic) a (10002005/4) 99.96%</li><li>Generic Win/DOS Executable (2004/3) 0.02%</li><li>DOS Executable Generic (2002/1) 0.02%</li><li>Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%</li></ul>
File name:	Weemaes B.V.-PO74748392.exe
File size:	148824
MD5:	a08f23a15ef10b17370668cf5b9947ad
SHA1:	7cc53628714dd9d69881be1d186adf7b3e7af9cd
SHA256:	cc8e7690934b9059a1613d246a6c933df5dd7b1e333038dc76f7839dcc5697cd
SHA512:	3856222ba3b1f19abe6658edd081e2be5f3bfea12542f6bc4da54ab0396abd97f177a8c0857b8501f19e2addb2c3d4f1429d63e086bb13d27ae819b7aa784287
SSDEEP:	3072:7YIocqtkj0ufJOWJDZZWUVEZj9GQMUqxkKQX+Zz5U:8llqtlA83WUVEZj9GQMUqxkKQuZz5U
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$......u...1..1. ..1.....0...~...0.....0...Rich1.....PE..L....C.H..... .....p.....@.....

### File Icon



Icon Hash:

f092d47154d692f0



## Static PE Info

<b>General</b>	
Entrypoint:	0x401460
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x48164384 [Mon Apr 28 21:37:08 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:	3f04be9c844308940905412ae6398e70

## Authenticode Signature

Signature Valid:	false
Signature Issuer:	E=Bojarers4@YNGELPLEJERNE.Dec, CN=KOMMUNIKATIONSPORT, OU=FORVRELSERS, O=Smugkroernes7, L=DISILLUSIONIST, S=underthane, C=SZ
Signature Validation Error:	<b>A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider</b>
Error Number:	-2146762487
Not Before, Not After	<ul style="list-style-type: none"><li>8/2/2021 3:42:32 PM 8/2/2022 3:42:32 PM</li></ul>
Subject Chain	<ul style="list-style-type: none"><li>E=Bojarers4@YNGELPLEJERNE.Dec, CN=KOMMUNIKATIONSPORT, OU=FORVRELSERS, O=Smugkroernes7, L=DISILLUSIONIST, S=underthane, C=SZ</li></ul>
Version:	3
Thumbprint MD5:	FBE54C5E9F4823869F0A4679D90E0A7F
Thumbprint SHA-1:	06527A5BDEB0338B966DE1A96DB2ADCE4BB32D18
Thumbprint SHA-256:	C9FD39A34B58F4B82A00777D99B72B82EEA9A4BEC7DB78568EEA00B0A60A5578
Serial:	00

## Entrypoint Preview

## Data Directories

## Sections


Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1ab34	0x1b000	False	0.488389756944	data	6.47586194473	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1c000	0xaac	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1d000	0x5b9e	0x6000	False	0.213745117188	data	3.87033603675	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: Weemaes B.V.-PO74748392.exe PID: 5656 Parent PID: 5700

### General

Start time:	09:43:04
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Weemaes B.V.-PO74748392.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Weemaes B.V.-PO74748392.exe'
Imagebase:	0x400000
File size:	148824 bytes
MD5 hash:	A08F23A15EF10B17370668CF5B9947AD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	<ul style="list-style-type: none"><li>Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.758678567.00000000021C0000.00000040.00000001.sdmp, Author: Joe Security</li></ul>
Reputation:	low

### File Activities

Show Windows behavior

## Disassembly

## Code Analysis