

JoeSandbox Cloud BASIC



ID: 491309

Sample Name: Dokument VAT I
- 85926 09 2021 MAG-8.exe

Cookbook: default.jbs

Time: 13:06:56

Date: 27/09/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report Dokument VAT I - 85926 09 2021 MAG-8.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	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 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	8
General	9
Entrypoint Preview	9
Data Directories	9
Sections	9
Resources	9
Imports	9
Version Infos	9
Possible Origin	9
Network Behavior	9
Network Port Distribution	9
UDP Packets	9
Code Manipulations	9
Statistics	10
System Behavior	10
Analysis Process: Dokument VAT I - 85926 09 2021 MAG-8.exe PID: 6420 Parent PID: 5044	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10

Windows Analysis Report Dokument VAT I - 85926 09 20...

Overview

General Information

Sample Name:

Dokument VAT I - 85926 09 2021 MAG-8.exe

Analysis ID:

491309

MD5:

0a2f51e6d3650f1..

SHA1:

6283d55e065802..

SHA256:

e49ff3e9ecbbe32..

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

Multi AV Scanner detection for subm...

Yara detected GuLoader

Tries to detect virtualization through...

C2 URLs / IPs found in malware con...

Found potential dummy code loops (...)

Creates a DirectInput object (often fo...

Uses 32bit PE files

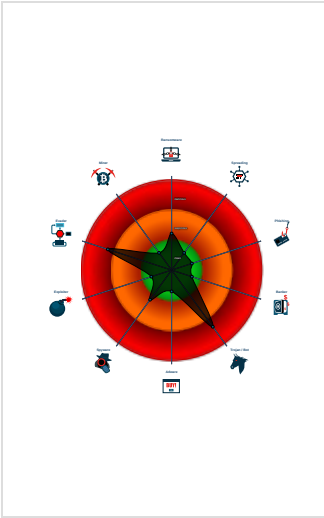
Sample file is different than original ...

PE file contains strange resources

Contains functionality to read the PEB

Uses code obfuscation techniques (...)

Classification



Process Tree

System is w10x64

Dokument VAT I - 85926 09 2021 MAG-8.exe (PID: 6420 cmdline: 'C:\Users\user\Desktop\Dokument VAT I - 85926 09 2021 MAG-8.exe' MD5: 0A2F51E6D3650F115C1B5484AFBDF3A7)

cleanup

Malware Configuration

Threatname: GuLoader

```
{  
  "Payload URL": "https://drive.google.com/uc?export=download&id=1nGji"  
}
```

Yara Overview


Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.815595666.00000000021E0000.00000040.00000001.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

Multi AV Scanner detection for submitted file

Networking:



C2 URLs / IPs found in malware configuration

Data Obfuscation:



Yara detected GuLoader

Malware Analysis System Evasion:



Tries to detect virtualization through RDTS time measurements

Anti Debugging:

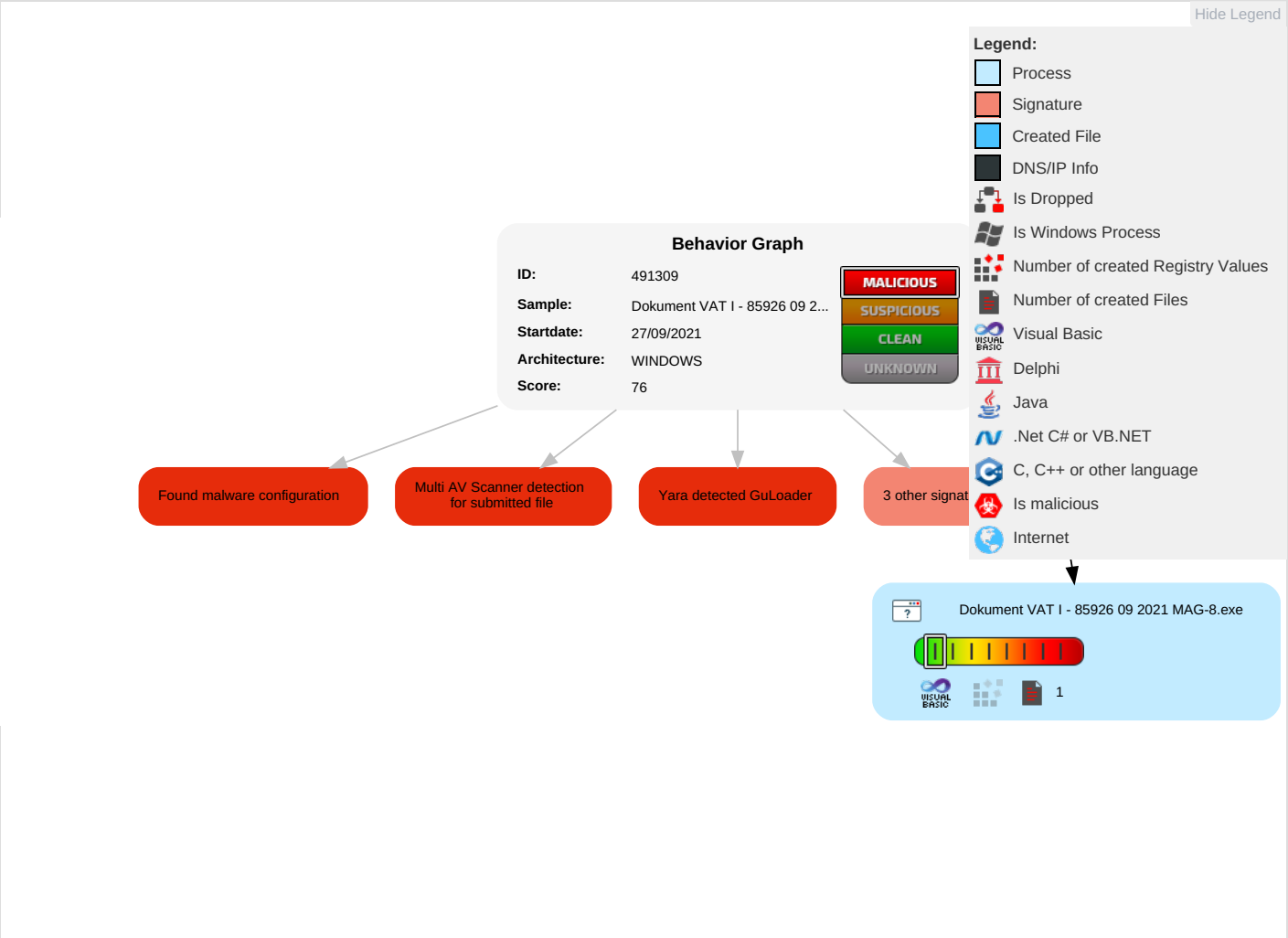


Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Recovery
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	Input Capture 1	Security Software Discovery 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Recovery
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	Recovery
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	Recovery
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Recovery

Behavior Graph





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Dokument VAT I - 85926 09 2021 MAG-8.exe	21%	Virustotal		Browse

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:	491309
Start date:	27.09.2021
Start time:	13:06:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Dokument VAT I - 85926 09 2021 MAG-8.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:	24
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:	mal76.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none">• Successful, ratio: 29.8% (good quality ratio 19.2%)• Quality average: 35.3%• Quality standard deviation: 33.4%
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):	5.702812730672399
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:	Dokument VAT I - 85926 09 2021 MAG-8.exe
File size:	90112
MD5:	0a2f51e6d3650f115c1b5484afbfd3a7
SHA1:	6283d55e065802036f0e5da958bfd458a7999c09
SHA256:	e49ff3e9ecbbe320e8cd29470d13b72643674b66e75ab5e824dda36eef6bf05e
SHA512:	4dbbba19dd4965cff3e7c9406dc37ce105beccab3cfd466eda57a734a15d3f7786b7a651f36df41a673ec53263d540de3a5aa8065a7a3e561b2d289828cf4ce7
SSDEEP:	1536:tDaUkPdJVa7kUSYdtAXrLHDLMAuP7I8ddUPrjr:t+TPdBaQUSB/3lm7oPrH
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode...\$......i.....*.....Rich.....PE..L....nR..... 0... ..@...@.....

File Icon

	
Icon Hash:	821ca88c8e8c8c00

Static PE Info

General	
Entrypoint:	0x4012c8
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:	0x526E8EE7 [Mon Oct 28 16:20:55 2013 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:	e73b8c032c82c64991ebe487a7ffcd43

Entrypoint Preview

Data Directories

Sections


Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x126ec	0x13000	False	0.513324938322	data	6.19701564833	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x14000	0xcf4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x15000	0x560	0x1000	False	0.13232421875	data	1.43718241534	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
Chinese	Taiwan	

Network Behavior

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

System Behavior

Analysis Process: Dokument VAT I - 85926 09 2021 MAG-8.exe PID: 6420 Parent PID: 5044

General

Start time:	13:07:50
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\Dokument VAT I - 85926 09 2021 MAG-8.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Dokument VAT I - 85926 09 2021 MAG-8.exe'
Imagebase:	0x400000
File size:	90112 bytes
MD5 hash:	0A2F51E6D3650F115C1B5484AFBDF3A7
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: 00000001.00000002.815595666.0000000021E0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis