ID: 491950
Sample Name: Hesap Hareketleri 28-09-2021.exe
Cookbook: default.jbs
Time: 08:03:16
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

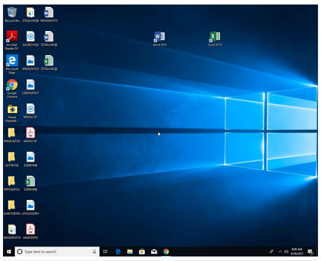
Windows Analysis Report Hesap Hareketleri 28-09-2021…

Overview

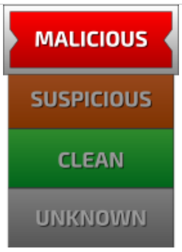
General Information

Sample Name:	Hesap Hareketleri 28-09-2021.exe
Analysis ID:	491950
MD5:	2fca7a3e51417ee.
SHA1:	931518250bed6c..
SHA256:	bffbffc2b1be1547..
Tags:	exe geo TUR
Infos:	

Most interesting Screenshot:



Detection



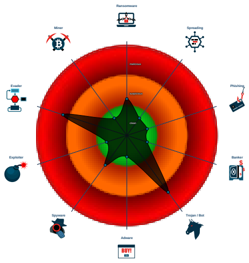
GuLoader

Score:	80
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 (…
- Machine Learning detection for samp…
- Creates a DirectInput object (often fo…
- Uses 32bit PE files
- Sample file is different than original …
- PE file contains an invalid checksum
- PE file contains strange resources
- Contains functionality to read the PEB
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- Hesap Hareketleri 28-09-2021.exe (PID: 6572 cmdline: 'C:\Users\user\Desktop\Hesap Hareketleri 28-09-2021.exe' MD5: 2FCA7A3E51417EE2E8AEFAFEDE0847D9)
- **cleanup**

Malware Configuration

Threatname: GuLoader

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

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.867469822.000000000071 0000.00000040.00000001.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

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

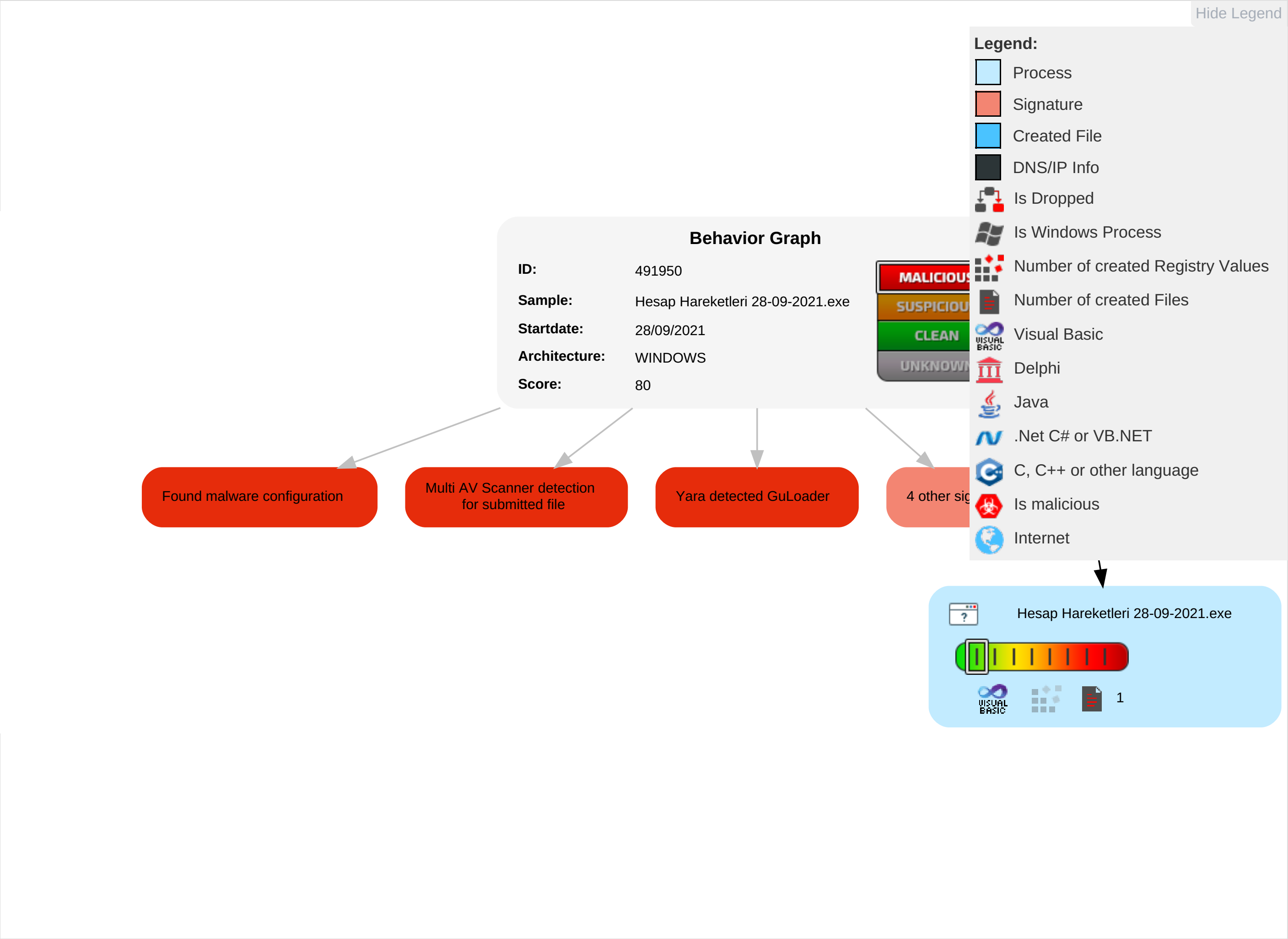
Anti Debugging:

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	Re Se Ef
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	Re Tr W Au
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	Re W W Au
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	Ol De Cl Ba
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	

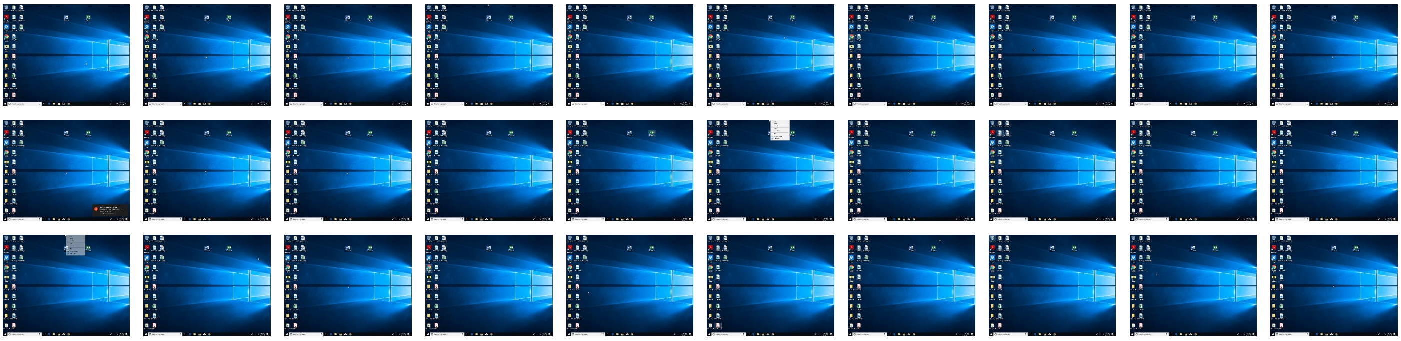
Behavior Graph

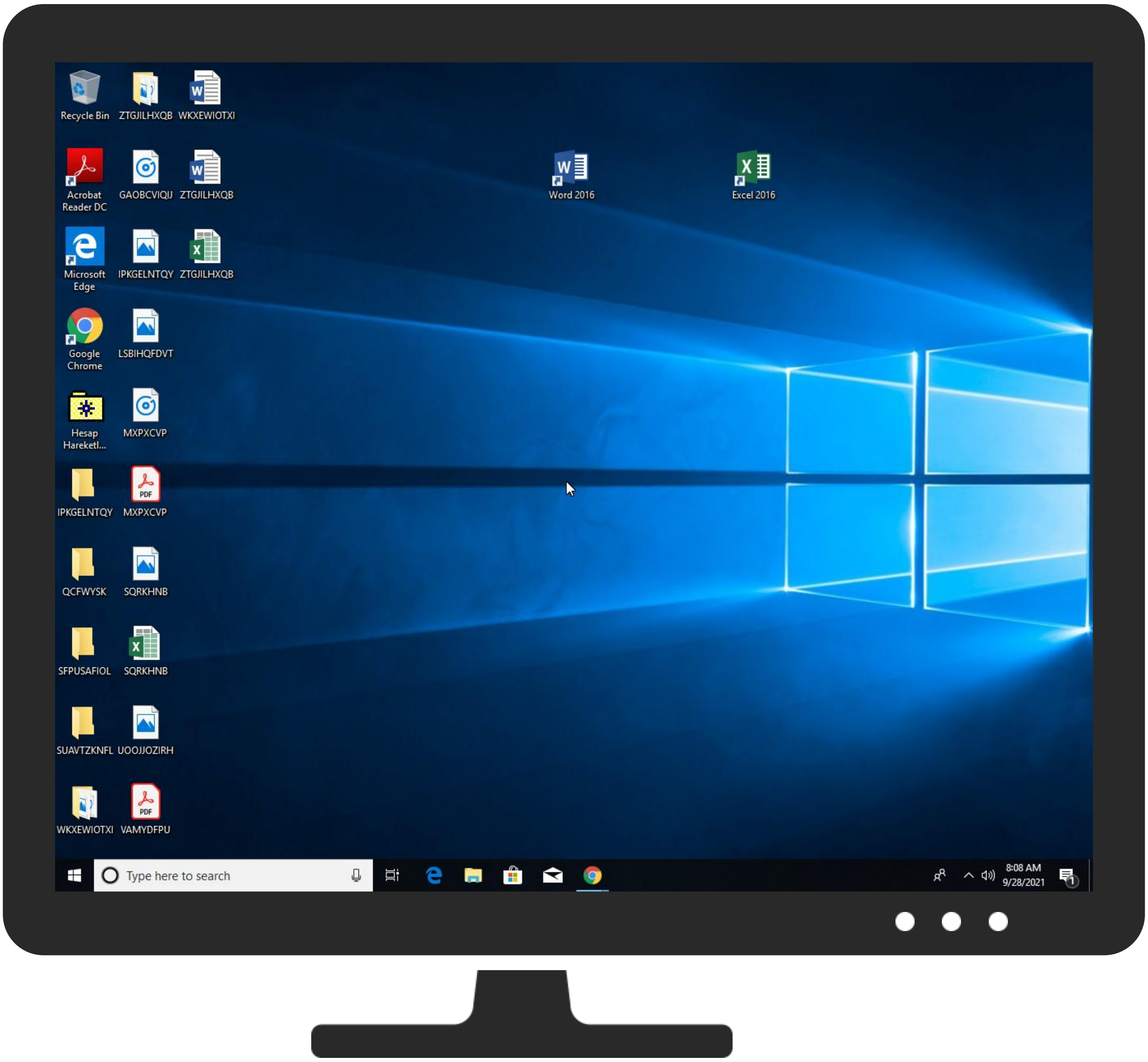


Screenshots

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
Hesap Hareketleri 28-09-2021.exe	27%	ReversingLabs	Win32.Trojan.Generic	
Hesap Hareketleri 28-09-2021.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:	491950
Start date:	28.09.2021
Start time:	08:03:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Hesap Hareketleri 28-09-2021.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:	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.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 23.4% (good quality ratio 7.5%) • Quality average: 20.1% • Quality standard deviation: 32.5%
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):	5.7538699249737375
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:	Hesap Hareketleri 28-09-2021.exe
File size:	90112
MD5:	2fca7a3e51417ee2e8aefafede0847d9
SHA1:	931518250bed6cd21b6cab529ed3ad9ead83cdcf
SHA256:	bffbffc2b1be154742fb81ecea14cb779b8fd81581ffce2855cf588f21a8020f
SHA512:	4d56a20cc61aa096fbd1e181ce72a79d237d90b7e20078 ed0e3c767dfead51a5b1d150307ca911fbaffac206ef3679 c99e9dc93dd37b3f5f419a55bb683220a
SSDEEP:	1536:tM0wFjVxFXrMGm0tEM5eoz/s74HEgKhs:tM0wFjV7XrXltPXs7SJgs
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$........i.....................*..............Rich....................PE..L...A6.L.................0... ....@....@........

File Icon

Icon Hash:	821ca88c8e8c8c00

Static PE Info

General

Entrypoint:	0x4012c8

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:	0x4C923641 [Thu Sep 16 15:22:41 2010 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	0x12aec	0x13000	False	0.519377055921	data	6.24667059185	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	0x540	0x1000	False	0.1298828125	data	1.4104134768	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: Hesap Hareketleri 28-09-2021.exe PID: 6572 Parent PID: 3888

General

Start time:	08:04:14
Start date:	28/09/2021
Path:	C:\Users\user\Desktop\Hesap Hareketleri 28-09-2021.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Hesap Hareketleri 28-09-2021.exe'
Imagebase:	0x400000
File size:	90112 bytes
MD5 hash:	2FCA7A3E51417EE2E8AEFAFEDE0847D9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.867469822.0000000000710000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis