

ID: 432593
Sample Name:
d81yNmZHaE.exe
Cookbook: default.jbs
Time: 15:19:00
Date: 10/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report d81yNmZHaE.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
Initial Sample 3
Memory Dumps 3
Unpacked PEs 3
Sigma Overview 4
Signature Overview 4
AV Detection: 4
Networking: 4
System Summary: 4
Data Obfuscation: 4
Malware Analysis System Evasion: 4
Anti Debugging: 4
Mitre Att&ck Matrix 4
Behavior Graph 5
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
Entrypoint Preview 9
Data Directories 9
Sections 9
Resources 9
Imports 9
Version Infos 9
Possible Origin 9
Network Behavior 9
Code Manipulations 9
Statistics 10
System Behavior 10
Analysis Process: d81yNmZHaE.exe PID: 5416 Parent PID: 5696 10
General 10
Disassembly 10
Code Analysis 10

Copyright Joe Security LLC 2021

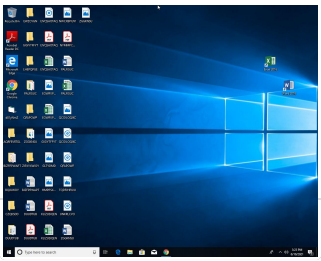
Analysis Report d81yNmZHaE.exe

Overview

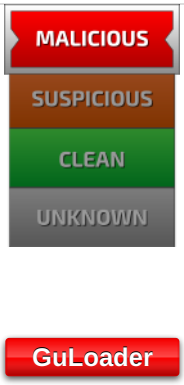
General Information

Sample Name:	d81yNmZHaE.exe
Analysis ID:	432593
MD5:	74b1969d9f41c94.
SHA1:	54935d5f7a59384.
SHA256:	f50e2cbd23d058c..
Tags:	exe GuLoader
Infos:	

Most interesting Screenshot:



Detection



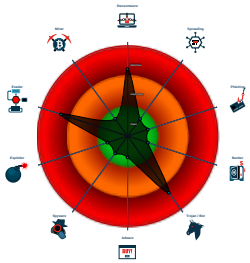
GuLoader

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Potential malicious icon found
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- Found potential dummy code loops (…
- Tries to detect virtualization through…
- Abnormal high CPU Usage
- Contains functionality for execution …
- Contains functionality to call native f…
- Contains functionality to read the PEB

Classification



Process Tree

- **System is w10x64**
- d81yNmZHaE.exe (PID: 5416 cmdline: 'C:\Users\user\Desktop\d81yNmZHaE.exe' MD5: 74B1969D9F41C94A1A07431B65BBF390)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://genitoriborgosatollo.it/main/client_sOcehs220.bin, http://amandaduquenoy."
}
```

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
d81yNmZHaE.exe	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.234240857.000000000401000.00000020.00020000.sdmp	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	
00000000.00000002.760283199.000000000401000.00000020.00020000.sdmp	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

Unpacked PEs

Copyright Joe Security LLC 2021

Source	Rule	Description	Author	Strings
0.0.d81yNmZHaE.exe.400000.0.unpack	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	
0.2.d81yNmZHaE.exe.400000.0.unpack	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

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

System Summary:



Potential malicious icon found

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)

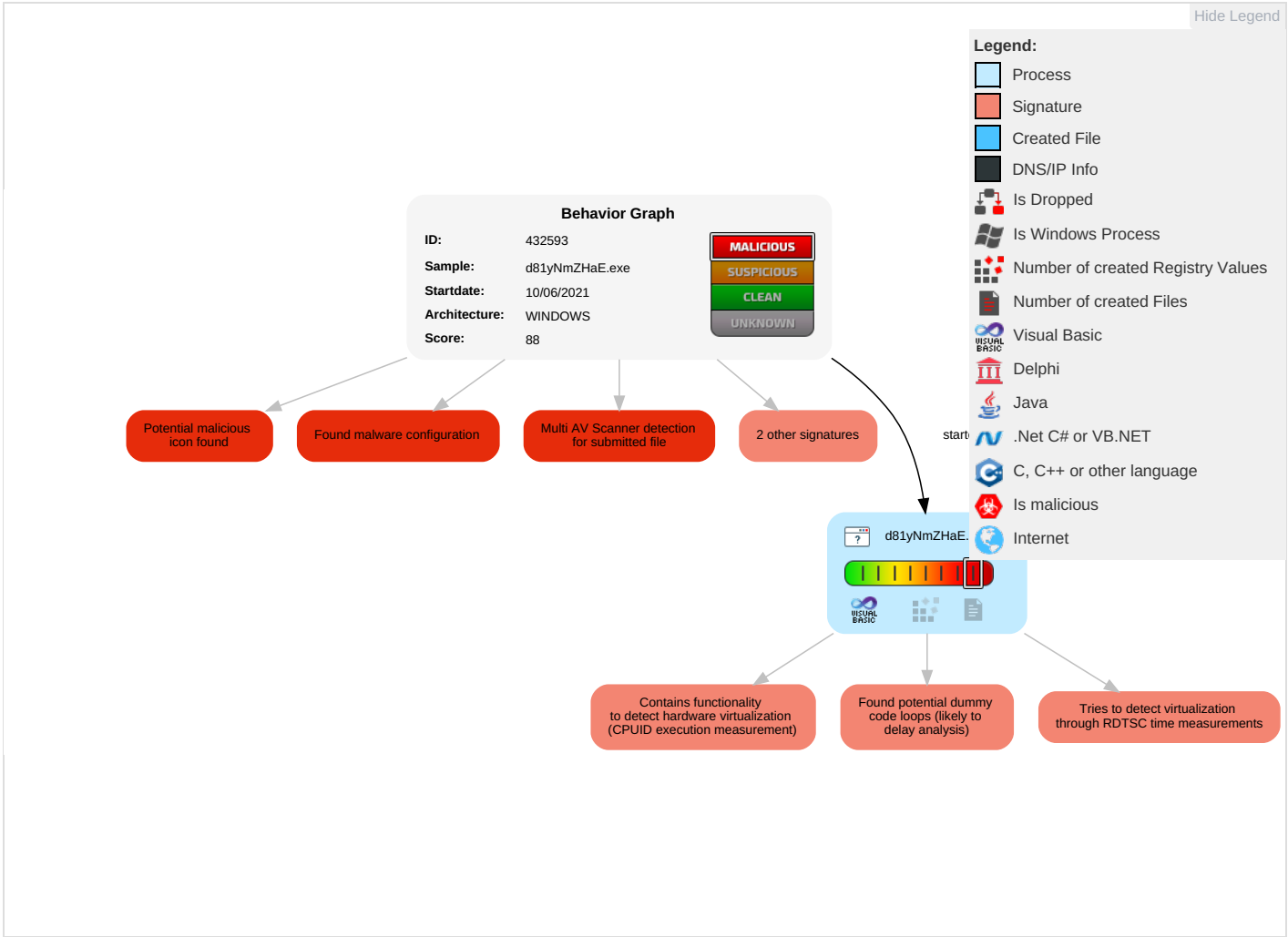
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R Se El
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	R 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	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	R W W Au

Copyright Joe Security LLC 2021

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
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	O D C B
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

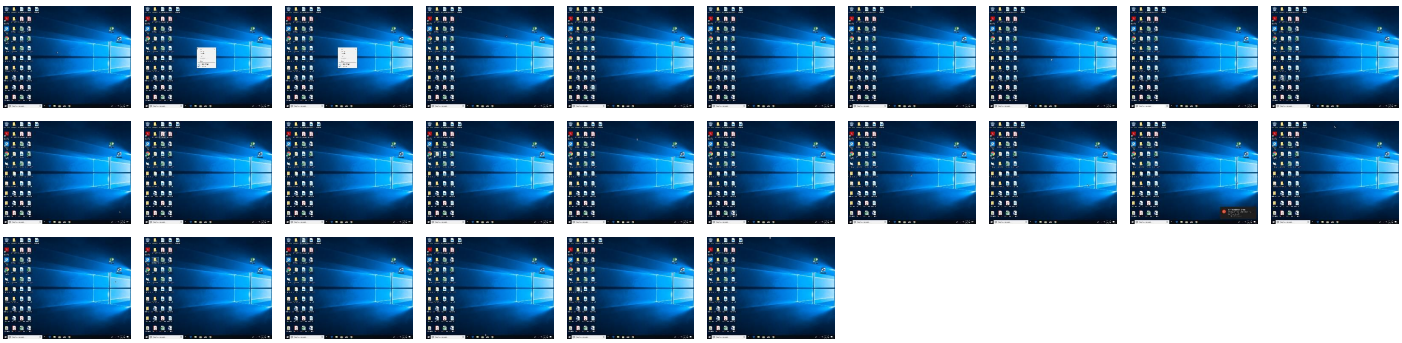
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Copyright Joe Security LLC 2021



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
d81yNmZHaE.exe	33%	Virustotal		Browse
d81yNmZHaE.exe	39%	ReversingLabs	Win32.Trojan.Jaik	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://genitoriborgosatollo.it/main/client_sOcehs220.bin, amandaduquenoy.	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://genitoriborgosatollo.it/main/client_sOcehs220.bin, amandaduquenoy.	true	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	432593
Start date:	10.06.2021
Start time:	15:19:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	d81yNmZHaE.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:	28
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:	mal88.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.4% (good quality ratio 0.3%) • Quality average: 11.5% • Quality standard deviation: 20.6%
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):	5.567506613853901
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:	d81yNmZHaE.exe
File size:	147456
MD5:	74b1969d9f41c94a1a07431b65bbf390
SHA1:	54935d5f7a59384ba8d1b26e25bbbc394e91922a
SHA256:	f50e2cbd23d058c6f0b1b147c1ee77ccd969b9f895375aed3c42ccbab0bbbe15
SHA512:	1f20e36948015e46dc30cc1b1aa7e03cb0c8586e045bfe02d0794b3306cb1ddbbf43b62c737d8a90b2db5ff5f85de9fa96af97e4e978f223fa9dc6a37ba9ad7c
SSDEEP:	1536:vMaIFFEMgx3vnWE7Hpm6IJNTcXmXSt4lYEQe3pyzBEkWKS:ExFQvWy8lxc14lwe3pyzyjKS
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...N.DU.....0..... ....@.....

File Icon



Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401c10
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:	0x5544D64E [Sat May 2 13:51:10 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:	9b8686288ab82fdbf8ede30bc55c83b7

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x20148	0x21000	False	0.350423177083	data	5.81715288276	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x22000	0x1250	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x24000	0x938	0x1000	False	0.16943359375	data	2.00254326763	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: d81yNmZHaE.exe PID: 5416 Parent PID: 5696

General

Start time:	15:19:54
Start date:	10/06/2021
Path:	C:\Users\user\Desktop\d81yNmZHaE.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\d81yNmZHaE.exe'
Imagebase:	0x400000
File size:	147456 bytes
MD5 hash:	74B1969D9F41C94A1A07431B65BBF390
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000000.00000000.234240857.0000000000401000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000000.00000002.760283199.0000000000401000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021