



ID: 451394
Sample Name:
nZdwtTEYoW.exe
Cookbook: default.jbs
Time: 15:49:08
Date: 20/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report nZdwtTEYoW.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 7
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
Code Manipulations 9
Statistics 9
System Behavior 10
Analysis Process: nZdwtTEYoW.exe PID: 4536 Parent PID: 5528 10
General 10
File Activities 10
Disassembly 10
Code Analysis 10

Copyright Joe Security LLC 2021

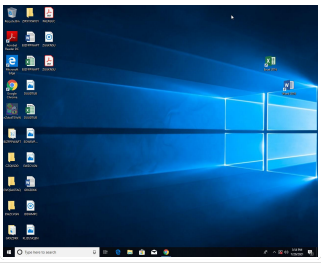
Windows Analysis Report nZdwtTEYoW.exe

Overview

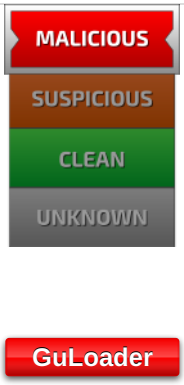
General Information

Sample Name:	nZdwtTEYoW.exe
Analysis ID:	451394
MD5:	c8feb9d53b567cd..
SHA1:	82a22cb59d46ba..
SHA256:	642a0df15a9b8e3.
Tags:	exe GuLoader
Infos:	

Most interesting Screenshot:



Detection



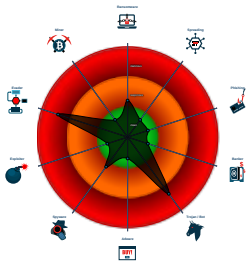
GuLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Found potential dummy code loops (…
- Machine Learning detection for samp…
- 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
- Creates a DirectInput object (often fo…

Classification



Process Tree

- **System is w10x64**
- nZdwtTEYoW.exe (PID: 4536 cmdline: 'C:\Users\user\Desktop\nZdwtTEYoW.exe' MD5: C8FEB9D53B567CD1BFB0E59CF7D26BC2)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=10PtVT-x7\"[OfT"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.762366853.000000000221 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Copyright Joe Security LLC 2021

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:



Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

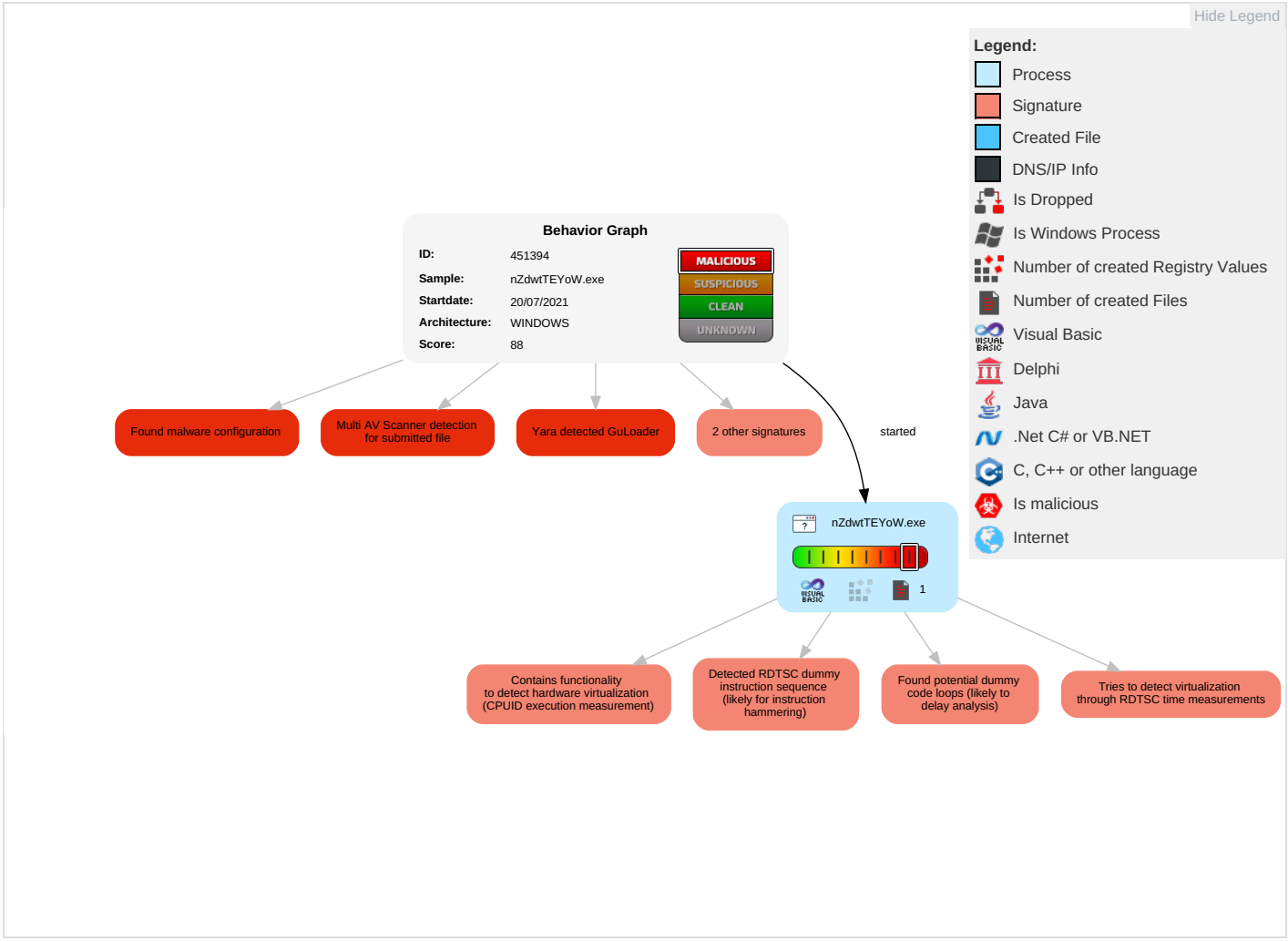


Found potential dummy code loops (likely to delay analysis)

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 4 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	Software Packing 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)	Process Injection 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)	Obfuscated Files or Information 2	NTDS	System Information Discovery 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

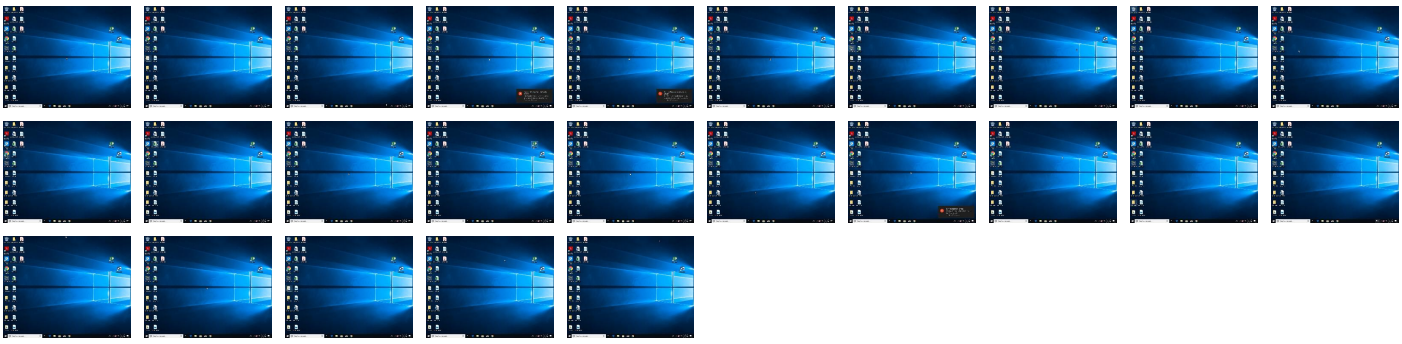
Behavior Graph



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
nZdwtTEYoW.exe	25%	Virustotal		Browse
nZdwtTEYoW.exe	13%	ReversingLabs	Win32.Trojan.Vebzenpak	
nZdwtTEYoW.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Copyright Joe Security LLC 2021

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:	451394
Start date:	20.07.2021
Start time:	15:49:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	nZdwtTEYoW.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:	26
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.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
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):	6.4666127843418355
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:	nZdwtTEYoW.exe
File size:	118784
MD5:	c8feb9d53b567cd1bfb0e59cf7d26bc2
SHA1:	82a22cb59d46bae21fa4877015e163eacc04a022
SHA256:	642a0df15a9b8e3124d638e755f0bdbacd0d1c3ff01b59b36213a190a5e5645a
SHA512:	da707134a7bfdcb66389f111bb363d1e7b7260bb718d6a999a23fc538e2065d8be766a713d8d20860e835eb21609bbbcb0d0b6c237124fa38bd2ada04acf157
SSDEEP:	1536:/bjX1R6rHR+Gz6YsFdVfKcLe0NMDfuoFVHYGokXYtvcOOfgrJZ+R6rHJXdb:jjX1yH1HErzwmoFtoZtkJgrCyHJXd
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....!.Q.....@.....(.....P....@.....

File Icon



Icon Hash:	b29a4a4a5a4a4a45

Static PE Info

General

Entrypoint:	0x401128
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:	0x510121E6 [Thu Jan 24 11:58:30 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:	5c4d602843f54570889588b32f7af650

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x13d90	0x14000	False	0.640209960938	data	6.90665747983	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x15000	0x115c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x17000	0x6d6a	0x7000	False	0.566301618304	data	5.78429982153	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
Maltese	Malta	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: nZdwtTEYoW.exe PID: 4536 Parent PID: 5528

General

Start time:	15:50:01
Start date:	20/07/2021
Path:	C:\Users\user\Desktop\nZdwtTEYoW.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\nZdwtTEYoW.exe'
Imagebase:	0x400000
File size:	118784 bytes
MD5 hash:	C8FEB9D53B567CD1BFB0E59CF7D26BC2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.762366853.0000000002210000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021