

JOeSandbox Cloud BASIC



ID: 502545

Sample Name: Contract and PI
of 1500W.exe

Cookbook: default.jbs

Time: 03:17:29

Date: 14/10/2021

Version: 33.0.0 White Diamond


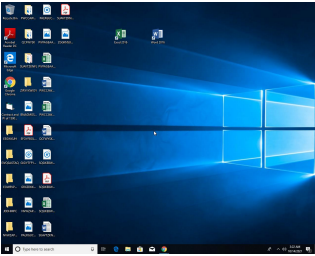
Table of Contents

Table of Contents	2
Windows Analysis Report Contract and PI of 1500W.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
System Summary:	4
Data Obfuscation:	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	6
Contacted Domains	7
Contacted IPs	7
General Information	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	7
IPs	7
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	8
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	9
Analysis Process: Contract and PI of 1500W.exe PID: 6180 Parent PID: 2804	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10

Windows Analysis Report Contract and PI of 1500W.exe

Overview

General Information

Sample Name:	Contract and PI of 1500W.exe
Analysis ID:	502545
MD5:	dbceab5b0f79168.
SHA1:	c5c25d75233ea8..
SHA256:	7d6174dce4980e..
Tags:	exe
Infos:	
Most interesting Screenshot:	
	

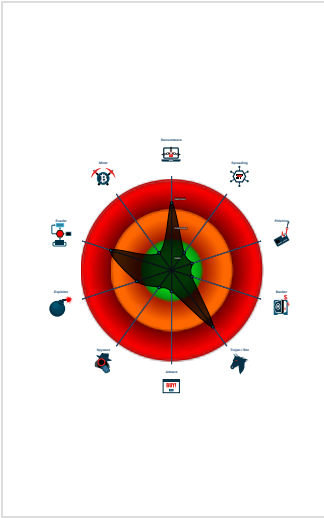
Detection

<div><div>MALICIOUS</div><div>SUSPICIOUS</div><div>CLEAN</div><div>UNKNOWN</div></div>	
<div>GuLoader</div>	
Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%


Signatures

Found malware configuration
Potential malicious icon found
Yara detected GuLoader
Found potential dummy code loops (...)
C2 URLs / IPs found in malware con...
Uses 32bit PE files
Found inlined nop instructions (likely...
Contains functionality to call native f...
Sample file is different than original ...
PE file contains strange resources
Contains functionality to read the PEB
Program does not show much activi...

Classification



Process Tree

▪ System is w10x64
•  Contract and PI of 1500W.exe (PID: 6180 cmdline: 'C:\Users\user\Desktop\Contract and PI of 1500W.exe' MD5: DBCEAB5B0F79168FFEA64F16BF7F1263)
▪ cleanup

Malware Configuration

Threatname: GuLoader

<pre>{ "Payload URL": "https://drive.google.com/uc?export=download" }</pre>

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.810237307.00000000020C 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

Networking:



C2 URLs / IPs found in malware configuration

System Summary:



Potential malicious icon found

Data Obfuscation:



Yara detected GuLoader

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	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Recovery Time Windows Available
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	Recovery Time Windows Available
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode 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	Operational Data Collection
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	System Information Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Recovery Time Windows Available

Behavior Graph



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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

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:	502545
Start date:	14.10.2021
Start time:	03:17:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 6s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Contract and PI of 1500W.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:	23
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:	mal72.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none">• Successful, ratio: 1% (good quality ratio 1%)• Quality average: 47%• Quality standard deviation: 8.2%
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):	6.277540298871474
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:	Contract and PI of 1500W.exe
File size:	135168
MD5:	dbceab5b0f79168ffea64f16bf7f1263
SHA1:	c5c25d75233ea8523111b1f964fbd482be973cd7
SHA256:	7d6174dce4980e71b083ae63d3b165b50b20855edb40ffa10a06a8e46e765cab
SHA512:	d13aa6e928f70d8051d0db5bd8e7a263567846b38f3817022db988f0d0230852579bd9c038f750a793dd5cc5cca14bf839c73a7cdb20bdc8a6b09caca76097f3
SSDEEP:	1536:gFA4c6Hdpd+KpVI+R9ATkcbu/nW9qUUWxexQ4vk8VcYGczNYGJM94oiGUASFUEv9:mc6HHdvpsSRbuRqA4/Zp9v3H
File Content Preview:	MZ.....@.....!..!Th is program cannot be run in DOS mode...\$.....#...B..B ...B..L^...B...`...B...d...B..Rich.B.....PE..L...d..O.....`.....h.....@.....B..

File Icon

	
Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401868
Entrypoint Section:	.text
Digitally signed:	false

General	
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4FFBD264 [Tue Jul 10 06:57:40 2012 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:	c727a98e677fb7bd25bb06d2a2d956f1

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x19de0	0x1a000	False	0.567514272837	data	6.73754725529	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1b000	0xaf0	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1c000	0x456a	0x5000	False	0.396240234375	data	4.60962667095	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: Contract and PI of 1500W.exe PID: 6180 Parent PID: 2804

General

Start time:	03:18:22
Start date:	14/10/2021
Path:	C:\Users\user\Desktop\Contract and PI of 1500W.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Contract and PI of 1500W.exe'
Imagebase:	0x400000
File size:	135168 bytes
MD5 hash:	DBCEAB5B0F79168FFEA64F16BF7F1263
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: 00000001.00000002.810237307.00000000020C0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

[Show Windows behavior](#)

Disassembly

Code Analysis