

JOeSandbox Cloud BASIC



ID: 502024

Sample Name: Statement of
Account.exe

Cookbook: default.jbs

Time: 14:27:11

Date: 13/10/2021

Version: 33.0.0 White Diamond




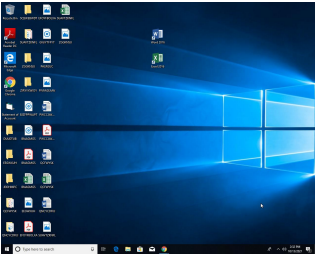
Table of Contents

Table of Contents	2
Windows Analysis Report Statement of Account.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	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: Statement of Account.exe PID: 5984 Parent PID: 6140	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10

Windows Analysis Report Statement of Account.exe

Overview

General Information

Sample Name:	Statement of Account.exe
Analysis ID:	502024
MD5:	1232806812f946a.
SHA1:	f9a820627667403.
SHA256:	86907475c81bc4..
Tags:	<div>exe guloader</div>
Infos:	<div>  </div>
Most interesting Screenshot:	
	

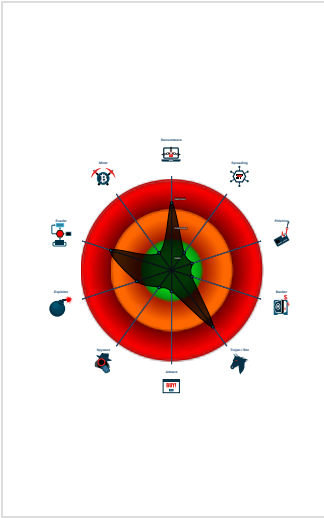
Detection

<div><div>MALICIOUS</div><div>SUSPICIOUS</div><div>CLEAN</div><div>UNKNOWN</div></div>	
<div>GuLoader</div>	
Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%


Signatures

Found malware configuration
Potential malicious icon found
Multi AV Scanner detection for subm...
Yara detected GuLoader
C2 URLs / IPs found in malware con...
Found potential dummy code loops (...)
Machine Learning detection for samp...
Uses 32bit PE files
Found inlined nop instructions (likely...
Sample file is different than original ...
PE file contains strange resources
Contains functionality to read the PEB

Classification



Process Tree

▪ System is w10x64
•  Statement of Account.exe (PID: 5984 cmdline: 'C:\Users\user\Desktop\Statement of Account.exe' MD5: 1232806812F946A2AFABC5F5FE489DE5)
▪ 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
00000000.00000002.783365997.0000000004BF0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

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
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	Data from Removable Media	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)	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	Recovery
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	System Information Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Recovery
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 4	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	Recovery

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

Source	Detection	Scanner	Label	Link
Statement of Account.exe	22%	ReversingLabs	Win32.Trojan.Mucc	
Statement of Account.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:	502024
Start date:	13.10.2021
Start time:	14:27:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Statement of Account.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:	27
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:	mal84.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none">• Successful, ratio: 0.9% (good quality ratio 0.7%)• Quality average: 37.6%• Quality standard deviation: 20.2%
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):	6.343524499435611
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:	Statement of Account.exe
File size:	135168
MD5:	1232806812f946a2afabc5f5fe489de5
SHA1:	f9a820627667403e90b3a387de0b644f8f0ddc31
SHA256:	86907475c81bc4700fc465c758592c51e905feed8aecdc0c10ccb6a8c650218a
SHA512:	14e655a40e696c7fedc58754e4263c512a2d0d0b922dae5c3e84594b3c639b0995e7b57ac10af97c69098e9bc9e42f336999fbafb44bb79470f4d568f690c4e
SSDEEP:	1536:BO7nxt7IPeC+EPGqwK+L1zDfCyuOiye7cuA+gg+5fTMZ9cBjyG3VqbfuYpZN88M+:U7dK2CneTx3Cyi31SQLGZq
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....9X.....`.....h.....@.....B..

File Icon

	
Icon Hash:	20047c7c70f0e004

Static PE Info

General	
Entrypoint:	0x401868
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:	0x5839B8B9 [Sat Nov 26 16:30:49 2016 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	0x19dd0	0x1a000	False	0.568171574519	data	6.81553512761	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	0x4562	0x5000	False	0.39609375	data	4.60717950331	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: Statement of Account.exe PID: 5984 Parent PID: 6140

General

Start time:	14:28:13
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\Statement of Account.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Statement of Account.exe'
Imagebase:	0x400000
File size:	135168 bytes
MD5 hash:	1232806812F946A2AFABC5F5FE489DE5
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: 00000000.00000002.783365997.0000000004BF0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis