ID: 501915
Sample Name: Statement of Account.exe
Cookbook: default.jbs
Time: 12:07:41
Date: 13/10/2021
Version: 33.0.0 White Diamond

Table of Contents

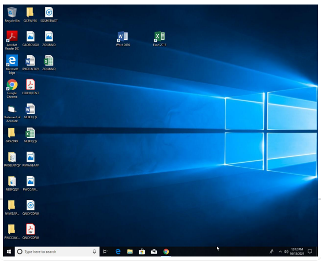
Windows Analysis Report Statement of Account.exe

Overview

General Information

Sample Name:	Statement of Account.exe
Analysis ID:	501915
MD5:	0fb63e5eb6af1af...
SHA1:	5e7e1db40c9104..
SHA256:	0b65815d462586..
Tags:	exe guloader
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

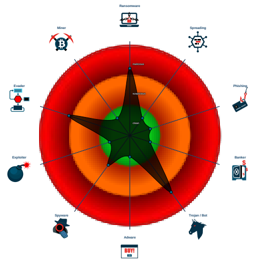
GuLoader

Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Potential malicious icon found
- Yara detected GuLoader
- 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 strange resources
- Contains functionality to read the PEB
- Uses code obfuscation techniques (…

Classification



Process Tree

- **System is w10x64**
- Statement of Account.exe (PID: 6644 cmdline: 'C:\Users\user\Desktop\Statement of Account.exe' MD5: 0FB63E5EB6AF1AFF086E3C2A2321F716)
- **cleanup**

Malware Configuration

Threatname: GuLoader

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

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.1200992906.0000000000740000.00000040.00000001.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

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Potential malicious icon found

Data Obfuscation:

Yara detected GuLoader

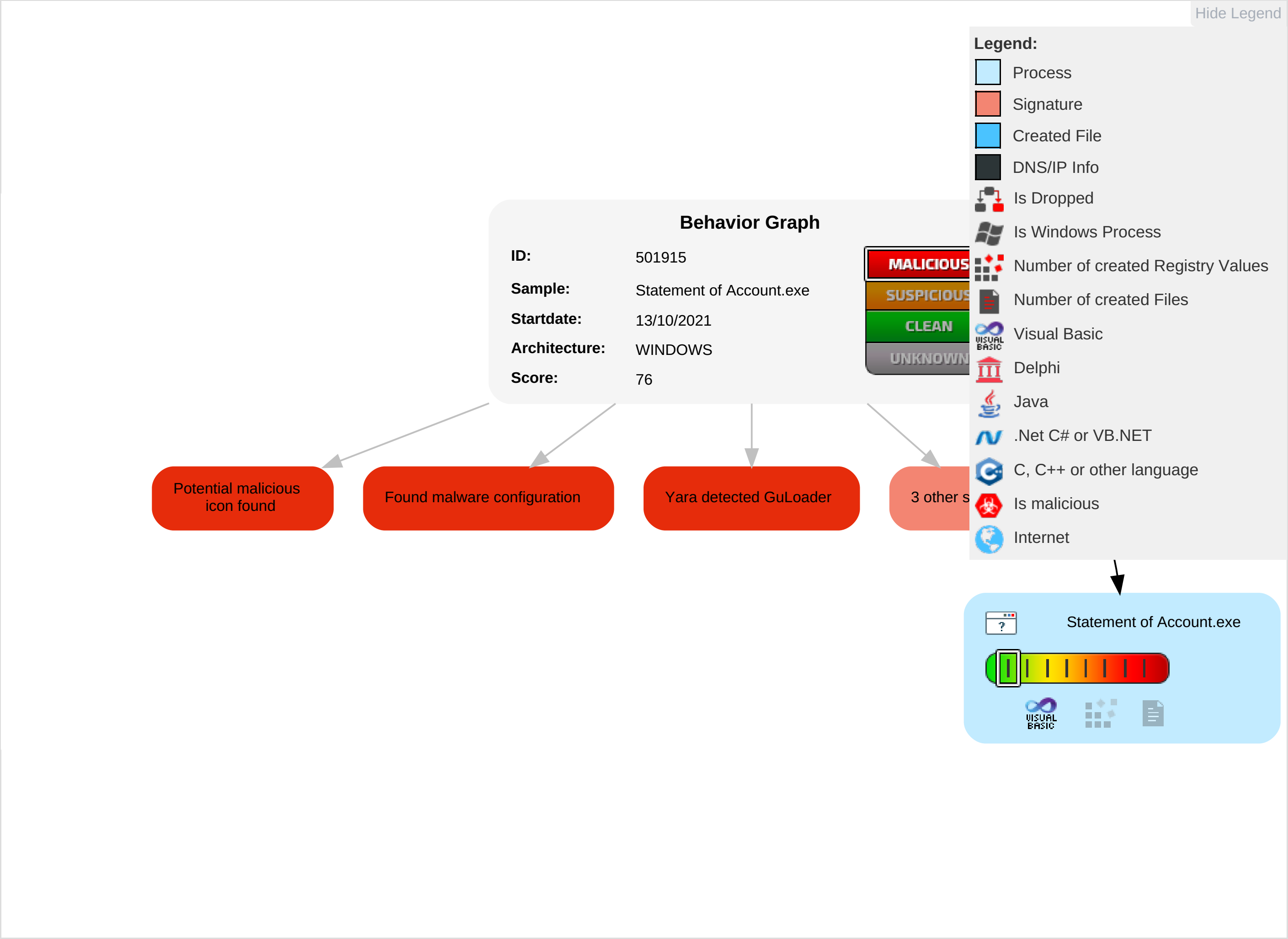
Anti Debugging:

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	Re Se Ef
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	Input Capture 1	Security Software Discovery 1 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)	Deobfuscate/Decode Files or Information 1	NTDS	System Information Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

Behavior Graph



Hide Legend

Legend:

- 🟦 Process
- 🟥 Signature
- 🟦 Created File
- ⬛ DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

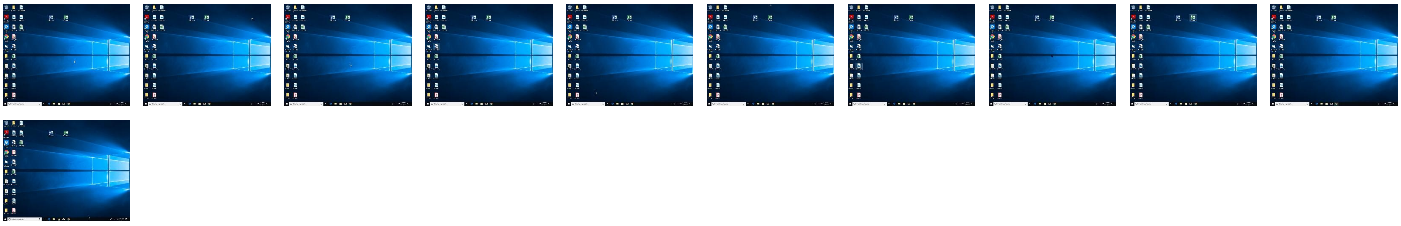
Behavior Graph

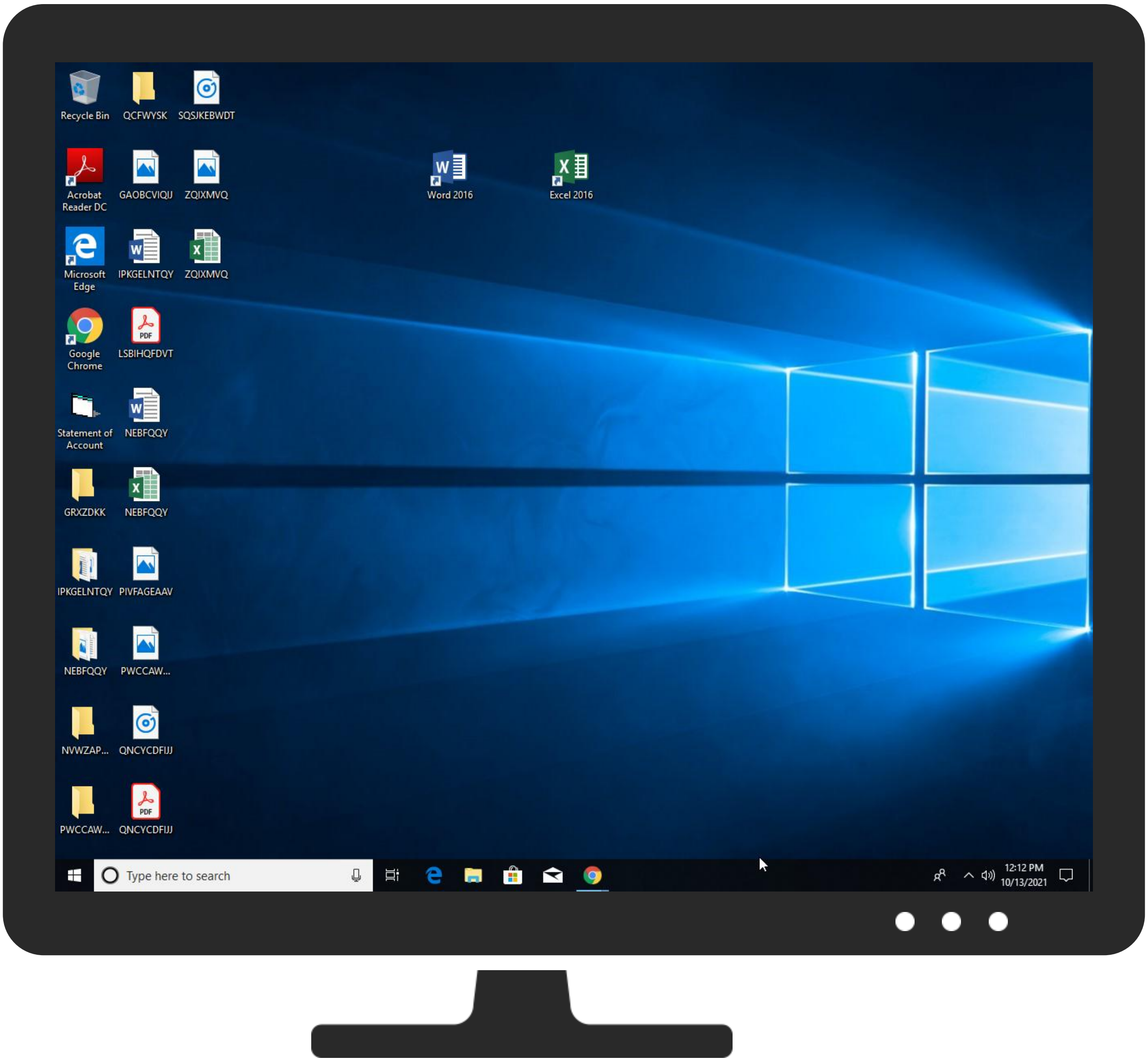
ID:	501915
Sample:	Statement of Account.exe
Startdate:	13/10/2021
Architecture:	WINDOWS
Score:	76

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
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

Name	IP	Active	Malicious	Antivirus Detection	Reputation
windowsupdate.s.llnwi.net	178.79.242.128	true	false		unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	501915
Start date:	13.10.2021
Start time:	12:07:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 36s
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:	15
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:	mal76.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.6% (good quality ratio 0.6%) • Quality average: 47% • Quality standard deviation: 8.2%
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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
windowsupdate.s.llnwi.net	jh6KzwrXQp.exe	Get hash	malicious	Browse	• 178.79.242.0
	heX1kOkwqy.exe	Get hash	malicious	Browse	• 178.79.242.0
	mixsix_20211013-084409.exe	Get hash	malicious	Browse	• 178.79.242.0
	2rd Quater Order Quotation.zip.xls	Get hash	malicious	Browse	• 178.79.242.128
	DOC REC EIPT.html	Get hash	malicious	Browse	• 178.79.242.128
	Efe-8 GPP Project Steel Pipe Tender.exe	Get hash	malicious	Browse	• 178.79.242.128
	emil.franchi@global.com #Ud83d#Udce0 VGX47BBSBJ44838.HTM	Get hash	malicious	Browse	• 178.79.242.128
	DHL Lieferschein,pdf.exe	Get hash	malicious	Browse	• 178.79.242.128
	Payment_MT103.exe	Get hash	malicious	Browse	• 178.79.242.0
	Doc-CS3.exe	Get hash	malicious	Browse	• 178.79.242.128
	SecuriteInfo.com.Suspicious.Win32.Save.a.28039.exe	Get hash	malicious	Browse	• 178.79.242.0
	oG3zl54AA5.exe	Get hash	malicious	Browse	• 178.79.242.128
	dNIT8STqLN.exe	Get hash	malicious	Browse	• 178.79.242.128
	Revised Quotation F657.exe	Get hash	malicious	Browse	• 178.79.242.0
	Quotation Request.pdf.exe	Get hash	malicious	Browse	• 178.79.242.0
	Proof of payment.jpg.exe	Get hash	malicious	Browse	• 178.79.242.128
	vk5MXd2Rxm.msi	Get hash	malicious	Browse	• 178.79.242.0
	jjBv8SpZXm.exe	Get hash	malicious	Browse	• 178.79.242.128
	COPIA DE PAGO.exe	Get hash	malicious	Browse	• 178.79.242.0
	Dekont.exe	Get hash	malicious	Browse	• 178.79.242.0

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

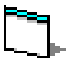
General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.361190831487217
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:	Statement of Account.exe

General

File size:	135168
MD5:	0fb63e5eb6af1aff086e3c2a2321f716
SHA1:	5e7e1db40c9104297c3b05b26c97a788eb92401b
SHA256:	0b65815d4625868701778980 72a1500ec014a390eb466e a0dd716567ada4109a
SHA512:	4dfd892dec9c4182005f668b201063085c6868085c2f556 791c5654516ce9a4be9c7a7c887e0da182f7cfb29c5690c f45638fb6749bf49e7ba74929d82c35a82
SSDEEP:	1536:5sYs89TfPXmlAo30SC66Biy2bbMSekC7dY5Kwc hyuGWawkANvv0LLhQ4sZiDNmMN:5JXS0SC6aiyCYU Kw7T3hBd
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$........#...B...B ...B..L^...B...`...B...d...B..Rich.B..........PE..L....u.W.......... ..........`......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:	0x578A7516 [Sat Jul 16 17:55:34 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	0x19ef0	0x1a000	False	0.567673903245	data	6.83550763896	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	0.396142578125	data	4.61030929614	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: 6644 Parent PID: 5940

General

Start time:	12:08:43
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:	0FB63E5EB6AF1AFF086E3C2A2321F716
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	- Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.1200992906.0000000000740000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis