ID: 526595
Sample Name: Sales Order List.exe
Cookbook: default.jbs
Time: 19:29:31
Date: 22/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

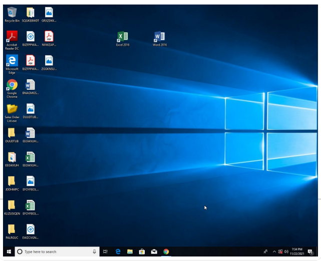
Windows Analysis Report Sales Order List.exe

Overview

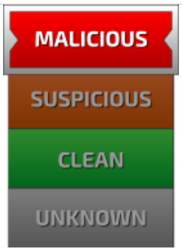
General Information

Sample Name:	Sales Order List.exe
Analysis ID:	526595
MD5:	80bad0903ee7ec..
SHA1:	35aecf6fe3ac24a..
SHA256:	260e6b75d7616e..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



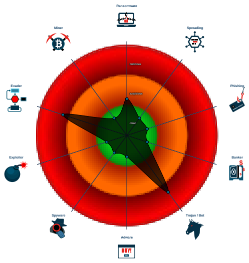
GuLoader

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Initial sample is a PE file and has a …
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Found potential dummy code loops (…
- Machine Learning detection for samp…
- Uses 32bit PE files
- Sample file is different than original …
- PE file contains strange resources
- Contains functionality to read the PEB

Classification



Process Tree

- **System is w10x64**
- Sales Order List.exe (PID: 2260 cmdline: "C:\Users\user\Desktop\Sales Order List.exe" MD5: 80BAD0903EE7EC98805678673720CFD9)
- **cleanup**

Malware Configuration

Threatname: GuLoader

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

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.821817884.00000000020F0000.00000040.00000001.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

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

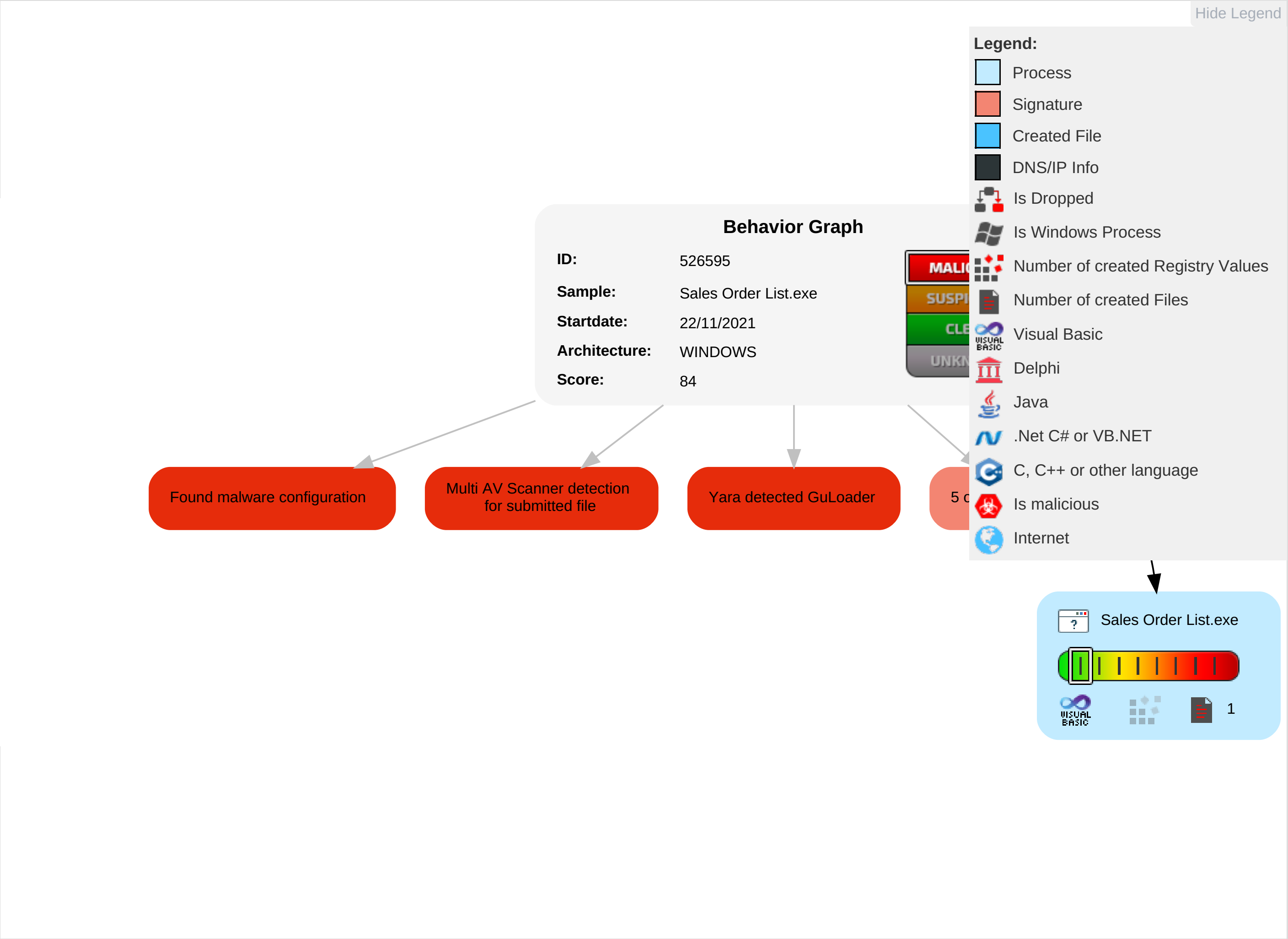
Anti Debugging:

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 S E
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	R T W A
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 A
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 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Behavior Graph



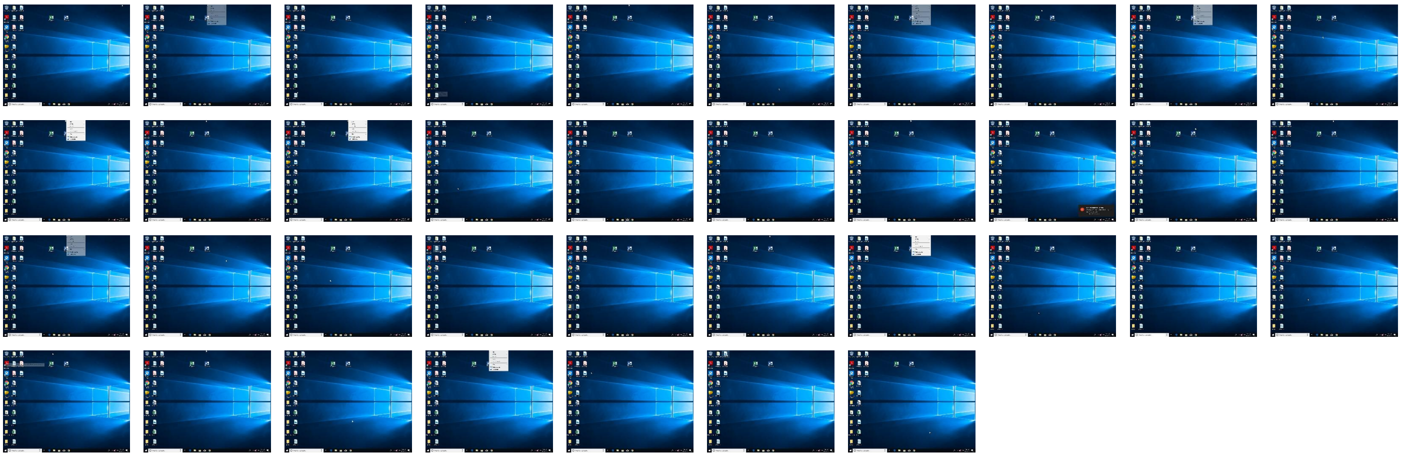
Behavior Graph

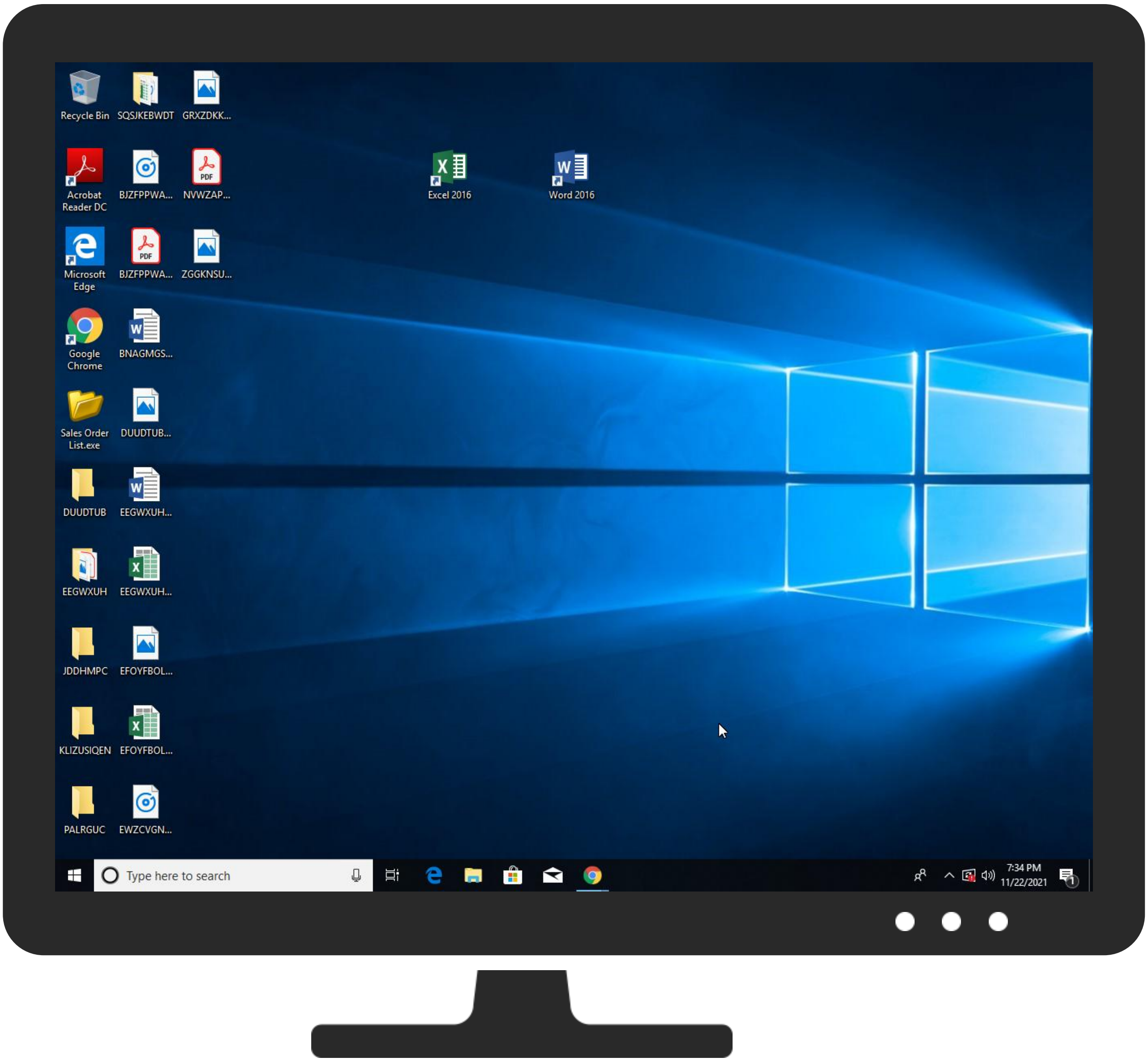
ID: 526595
Sample: Sales Order List.exe
Startdate: 22/11/2021
Architecture: WINDOWS
Score: 84

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
Sales Order List.exe	40%	ReversingLabs	Win32.Trojan.GuLoader	
Sales Order List.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://topqualityfreeware.com	0%	Avira URL Cloud	safe	
http://www.topqualityfreeware.com/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	526595
Start date:	22.11.2021
Start time:	19:29:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Sales Order List.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:	19
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:	mal84.troj.evad.winEXE@1/1@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 61% (good quality ratio 46.8%) • Quality average: 49.1% • Quality standard deviation: 35.6%
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

C:\Users\user\AppData\Local\Temp\~DF904D784913DB7A54.TMP	
Process:	C:\Users\user\Desktop\Sales Order List.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	4.01191323271951
Encrypted:	false
SSDEEP:	384:wcZ0tADSVlx6JQhynrV7Vr9wrCIM/ZUYVPzBAPN:wcZeADSV/6qhynrV7VxwrrMvqPN
MD5:	6C4C01A4316CD9338DE51EC175EBF11D
SHA1:	8C5D5B07E0ED6AAC72705F516E25BEAEA891EFA0
SHA-256:	95876F7C1242672418DB201C02D70276EE9CC4345394DEAD3500619A39DA28F0
SHA-512:	9F60729E865B0414DB4792F76465EDCE1595D22E884D01C07389A312474D1CE916E4CF73275D5AA0CB411D8EBB0617EF661CD10467AD838FD1B0B388C44823D
Malicious:	false
Reputation:	low
Preview:	......................>.. ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.002958856412811
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:	Sales Order List.exe
File size:	192512
MD5:	80bad0903ee7ec98805678673720cfd9
SHA1:	35aecf6fe3ac24adaf16c04b787e90ac4c845eb0

General

SHA256:	260e6b75d7616efd29c05151f1ce95bbab1aaf8703f86f62 c4d9bc6d308a56b8
SHA512:	9a88b4ea27bbc8b83c0722c715c12b3667d6138d27d2fa bb315a8a8c4ddcb020962625d1aa75c56d7e2082bbded7 ffaa3512b482f1a4ba138d1877a55e848e9b
SSDEEP:	3072:trejCYyLGrRxfFNEv6QN744ndRkHDwLVly5Mrc0y vhXeJ:treiGrRNFMjN6jIVCMrcbeJ
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$........i............ ....*..............Rich....................PE..L......G................. 0..........L........@....@........

File Icon

Icon Hash:	0ceefedec6f67c0c

Static PE Info

General

Entrypoint:	0x40134c
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:	0x47ABAEC7 [Fri Feb 8 01:22:15 2008 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:	f27a613fda76c14f4eab7dc0085d799e

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x22f6c	0x23000	False	0.367292131696	data	5.18350124338	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x24000	0x13f0	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x26000	0x90bd	0xa000	False	0.346240234375	data	4.35051738239	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

Language of compilation system	Country where language is spoken	Map
English	United States	
Turkmen	Turkmenistan	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: Sales Order List.exe PID: 2260 Parent PID: 5012

General

Start time:	19:30:31
Start date:	22/11/2021
Path:	C:\Users\user\Desktop\Sales Order List.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Sales Order List.exe"
Imagebase:	0x400000
File size:	192512 bytes
MD5 hash:	80BAD0903EE7EC98805678673720CFD9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.821817884.00000000020F0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Disassembly

Code Analysis