Joe Sandbox Cloud BASIC

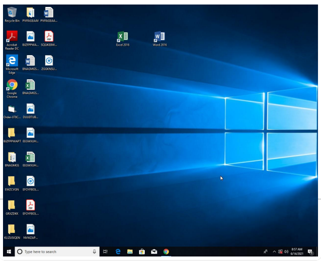
ID: 433965
Sample Name: Order-078CNLTD.exe
Cookbook: default.jbs
Time: 08:52:46
Date: 14/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

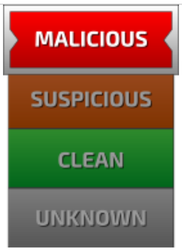
Analysis Report Order-078CNLTD.exe

Overview

General Information

Sample Name:	Order-078CNLTD.exe
Analysis ID:	433965
MD5:	db7cc0b29cf38b5..
SHA1:	8e5c1a3ca8e4b5..
SHA256:	aa70c51a1df950f..
Tags:	exe
Infos:	
Most interesting Screenshot:	

Detection



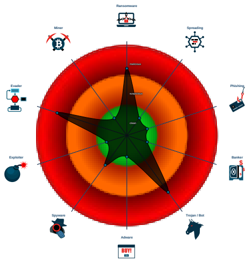
GuLoader

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Potential malicious icon found
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Found potential dummy code loops (…
- Initial sample is a PE file and has a …
- Tries to detect virtualization through…
- Abnormal high CPU Usage
- Contains functionality for execution …

Classification



Process Tree

- **System is w10x64**
- Order-078CNLTD.exe (PID: 5800 cmdline: 'C:\Users\user\Desktop\Order-078CNLTD.exe' MD5: DB7CC0B29CF38B5ED2A176C0043B2A58)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://andreameixueiro.com/TODAY_tRiyv97.bin"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.738009135.000000000210 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Potential malicious icon found

Initial sample is a PE file and has a suspicious name

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

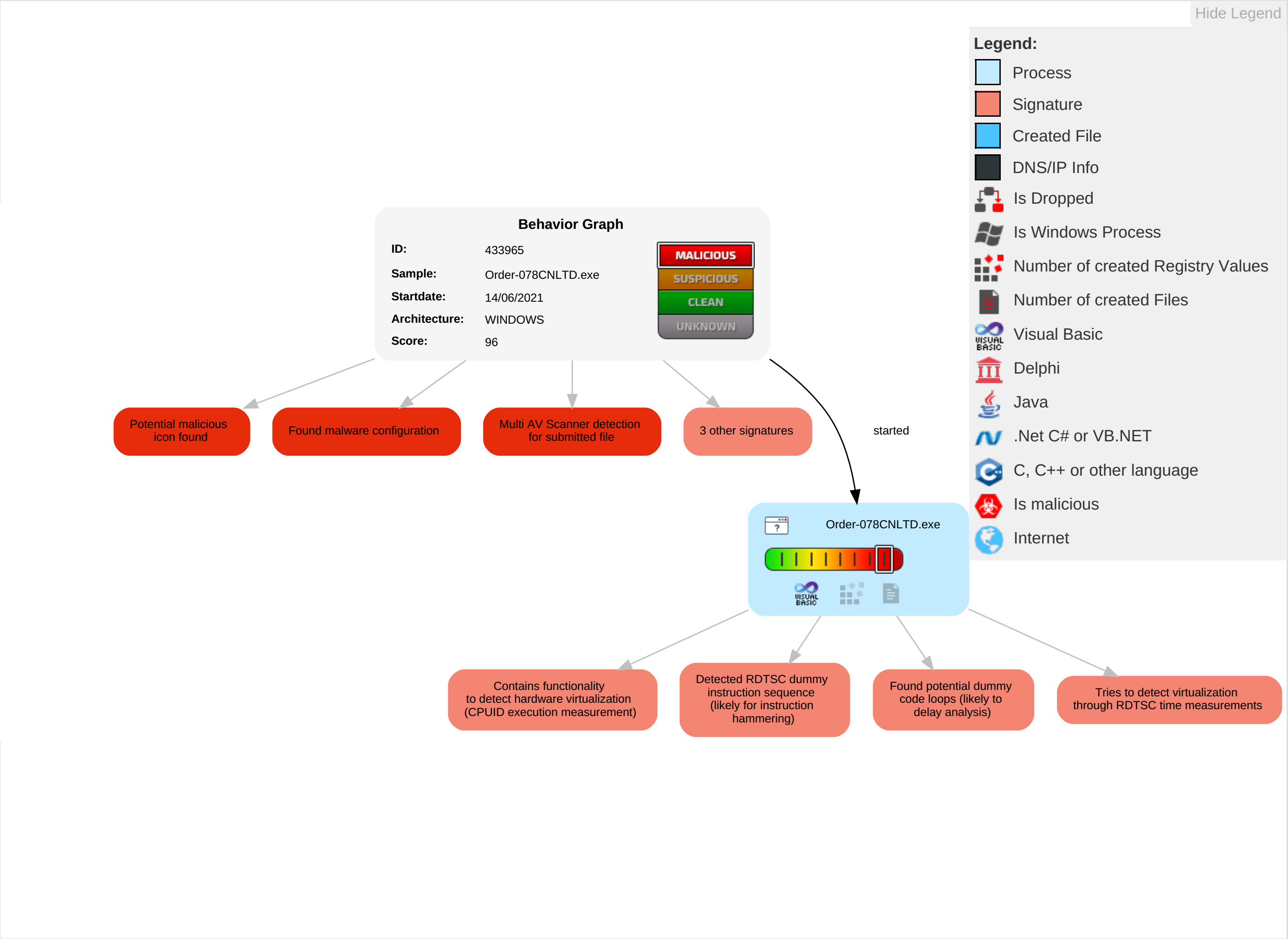
Anti Debugging:

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	R S E
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 4 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 3 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

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

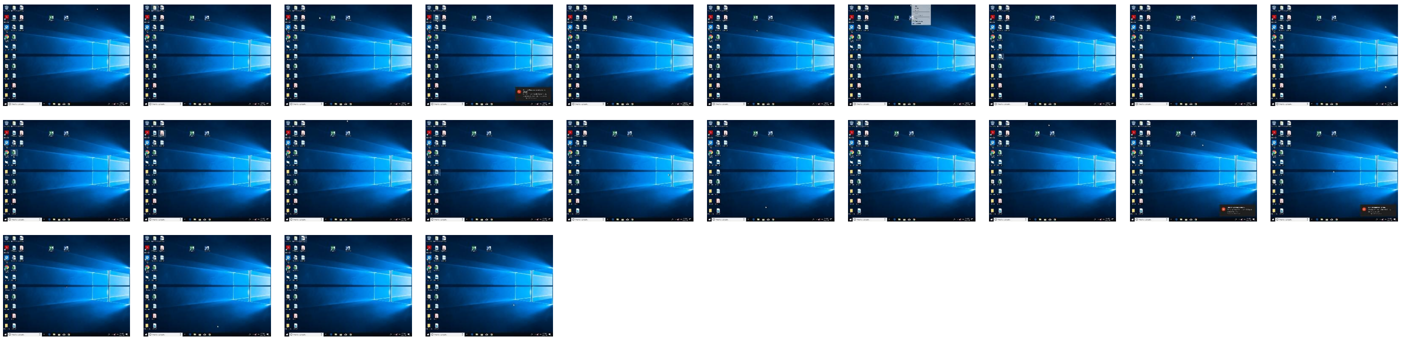
ID:	433965
Sample:	Order-078CNLTD.exe
Startdate:	14/06/2021
Architecture:	WINDOWS
Score:	96

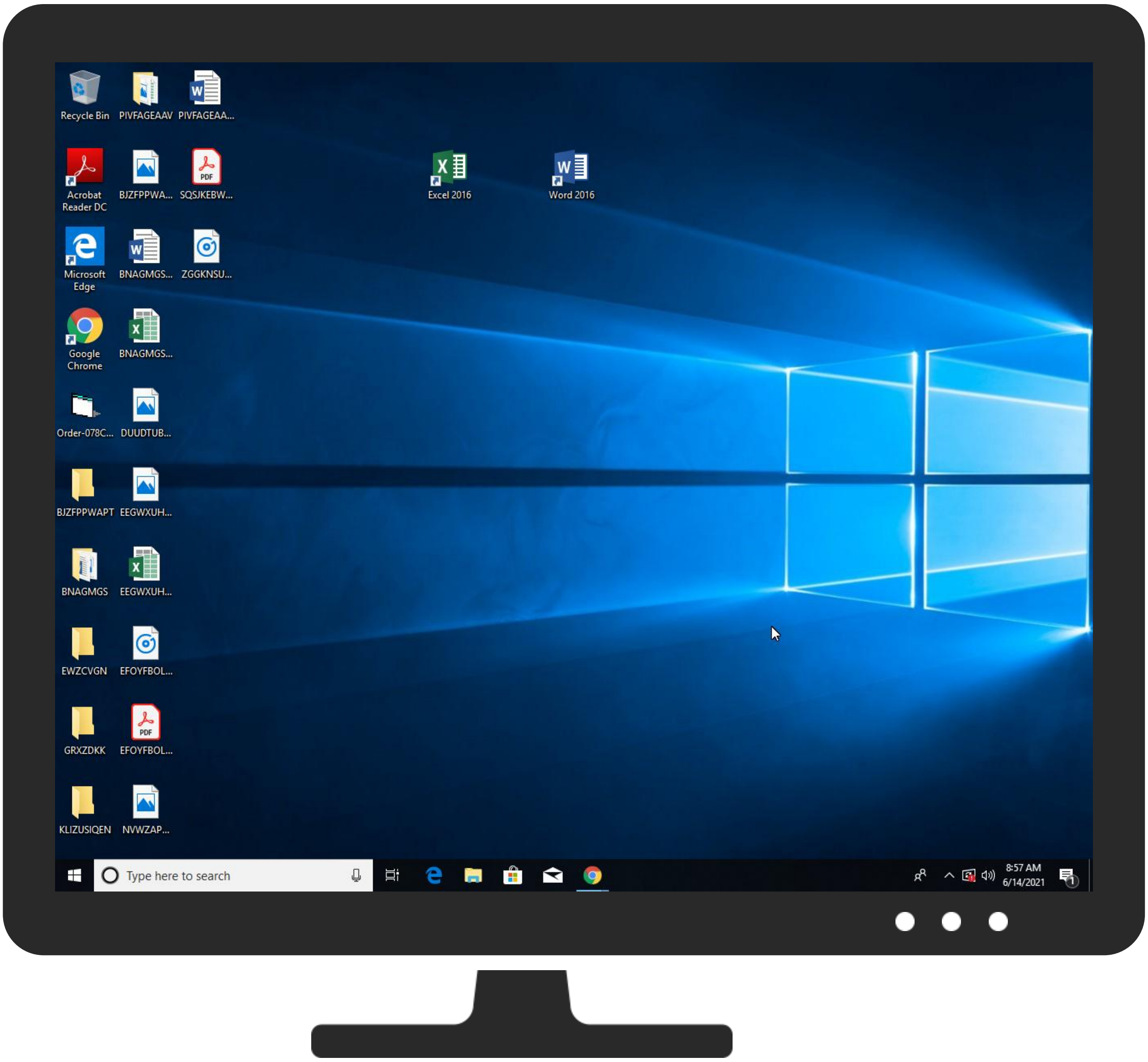
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Potential malicious icon found
Found malware configuration
Multi AV Scanner detection for submitted file
3 other signatures
started
Order-078CNLTD.exe
VISUAL BASIC
Contains functionality to detect hardware virtualization (CPUID execution measurement)
Detected RDTSC dummy instruction sequence (likely for instruction hammering)
Found potential dummy code loops (likely to delay analysis)
Tries to detect virtualization through RDTSC time measurements

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
Order-078CNLTD.exe	70%	Virustotal		Browse
Order-078CNLTD.exe	29%	Metadefender		Browse
Order-078CNLTD.exe	86%	ReversingLabs	Win32.Infostealer.Fareit	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://andreameixueiro.com/TODAY_tRiyv97.bin	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://andreameixueiro.com/TODAY_tRiyv97.bin	true	- Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433965
Start date:	14.06.2021
Start time:	08:52:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Order-078CNLTD.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:	29
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:	mal96.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.2%) • Quality average: 52% • Quality standard deviation: 5.7%
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

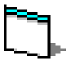
No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.742264491721508
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:	Order-078CNLTD.exe
File size:	294912
MD5:	db7cc0b29cf38b5ed2a176c0043b2a58
SHA1:	8e5c1a3ca8e4b5cd7c43cd7f0acbc40a09cefbef
SHA256:	aa70c51a1df950f7b8406f4599a7e3bb89bc61fec570fc0e3a53826d42cbf13c
SHA512:	ed42d70c69df510f2e832af1ea72d9579486b433cc478e1a10265e02a453cc031696f7f74b2530c42826852e4eb3a88ccd37359fec59843a2e5dc2f8e10549e3
SSDEEP:	3072:VO64I415+Uznrw1JmTgxViFJqryHbQbZ:Q64I4HHz0oym7
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......u...1...1...1.......0...~...0.......0...Rich1...........PE..L...B.NY................P... ....`....@................

File Icon



Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401f04
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:	0x594ECB42 [Sat Jun 24 20:27:46 2017 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:	fd5523c2b03dc52202311eff5bcab494

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x44f44	0x45000	False	0.212437726449	data	4.83296274478	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x46000	0xab4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x47000	0x9f4	0x1000	False	0.1806640625	data	2.21609318156	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: Order-078CNLTD.exe PID: 5800 Parent PID: 5580

General

Start time:	08:53:38
Start date:	14/06/2021
Path:	C:\Users\user\Desktop\Order-078CNLTD.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Order-078CNLTD.exe'
Imagebase:	0x400000
File size:	294912 bytes
MD5 hash:	DB7CC0B29CF38B5ED2A176C0043B2A58
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.738009135.0000000002100000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis