

JoeSandbox Cloud BASIC



**ID:** 434868

**Sample Name:**

OrdineFornitore\_Nr\_2021\_OV\_445..exe

**Cookbook:** default.jbs

**Time:** 15:58:28

**Date:** 15/06/2021

**Version:** 32.0.0 Black Diamond


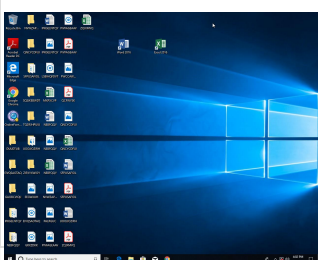
## Table of Contents

Table of Contents	2
Windows Analysis Report OrdineFornitore_Nr_2021_OV_445..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
Signature Overview	3
AV Detection:	4
Networking:	4
Data Obfuscation:	4
Malware Analysis System Evasion:	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	8
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
Authenticode Signature	9
Entrypoint Preview	9
Data Directories	9
Sections	9
Resources	9
Imports	9
Version Infos	9
Possible Origin	9
Network Behavior	10
Code Manipulations	10
Statistics	10
System Behavior	10
Analysis Process: OrdineFornitore_Nr_2021_OV_445..exe PID: 6896 Parent PID: 6012	10
General	10
File Activities	10
Disassembly	10
Code Analysis	10



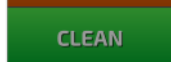


# Windows Analysis Report OrdineFornitore\_Nr\_2021\_OV...

## Overview

### General Information

Sample Name:	OrdineFornitore_Nr_2021_OV_445..exe
Analysis ID:	434868
MD5:	ca5dbe288ef27fd..
SHA1:	2de17b7906332d..
SHA256:	582ef41b5d92451..
Infos:	
Most interesting Screenshot:	

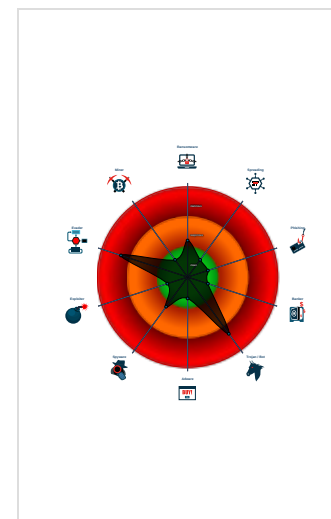
### Detection

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


### Signatures

Found malware configuration
Multi AV Scanner detection for subm...
Yara detected GuLoader
C2 URLs / IPs found in malware con...
Contains functionality to detect hard...
Found potential dummy code loops (...)
Machine Learning detection for samp...
Tries to detect virtualization through...
Abnormal high CPU Usage
Contains functionality for execution ...
Contains functionality to call native f...
Contains functionality to query CPU ...

### Classification



## Process Tree

- System is w10x64
-  OrdineFornitore\_Nr\_2021\_OV\_445..exe (PID: 6896 cmdline: 'C:\Users\user\Desktop\OrdineFornitore\_Nr\_2021\_OV\_445..exe' MD5: CA5DBE288EF27FD1A4BB491A3119285F)
- cleanup

## Malware Configuration

### Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1xUEBGrPLI038P_OFJ8CjCR9Fp-zTgH1u"
}
```

## Yara Overview

### Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.1011030674.000000000022 40000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

## Sigma Overview

No Sigma rule has matched

## 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

## Data Obfuscation:



Yara detected GuLoader

## Malware Analysis System Evasion:



Contains functionality to detect hardware virtualization (CPUID execution measurement)

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	Recovery
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 3 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	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
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	Recovery
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 2 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Recovery

## Behavior Graph

## Screenshots

## Thumbnails

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

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
OrdineFornitore_Nr_2021_OV_445..exe	16%	Virustotal		<a href="#">Browse</a>
OrdineFornitore_Nr_2021_OV_445..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:	32.0.0 Black Diamond
Analysis ID:	434868
Start date:	15.06.2021
Start time:	15:58:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	OrdineFornitore_Nr_2021_OV_445..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:	16
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"><li>• HCA enabled</li><li>• EGA enabled</li><li>• HDC enabled</li><li>• AMSI enabled</li></ul>
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.troj.evad.winEXE@1/0@0/0
EGA Information:	<ul style="list-style-type: none"><li>• Successful, ratio: 100%</li></ul>
HDC Information:	<ul style="list-style-type: none"><li>• Successful, ratio: 20.6% (good quality ratio 8.8%)</li><li>• Quality average: 20.7%</li><li>• Quality standard deviation: 28.3%</li></ul>
HCA Information:	Failed
Cookbook Comments:	<ul style="list-style-type: none"><li>• Adjust boot time</li><li>• Enable AMSI</li><li>• Found application associated with file extension: .exe</li><li>• Override analysis time to 240s for sample files taking high CPU consumption</li></ul>
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):	6.220371339599688
TrID:	<ul style="list-style-type: none"><li>Win32 Executable (generic) a (10002005/4) 99.15%</li><li>Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81%</li><li>Generic Win/DOS Executable (2004/3) 0.02%</li><li>DOS Executable Generic (2002/1) 0.02%</li><li>Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%</li></ul>
File name:	OrdineFornitore_Nr_2021_OV_445..exe
File size:	165640
MD5:	ca5dbe288ef27fd1a4bb491a3119285f
SHA1:	2de17b7906332db8828e87afd8f24aea93a9db25
SHA256:	582ef41b5d92451e2ca69cba6f821731d077fae38931556f2e2e3e09c577311d
SHA512:	8b062f9bb759bab77ed1274049461b71a59c91895423acca74b20afcbfe51ba6b2a6d74ff0309cb0e8dd81e923f484e70774bf2a9c69b4cda6550f68437f0712
SSDEEP:	3072:ZC1lQdla63sGvSI14DcKB8cp2UgILGvHQX:sWlaLpJLj
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...4S.J..... .....@.....

### File Icon



Icon Hash: e8f0b2caa69e98a8

### Static PE Info



<b>General</b>	
Entrypoint:	0x401890
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4AFE5334 [Sat Nov 14 06:50:28 2009 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:	4cd0d92faa0bc2c54919bd9657da5865

**Authenticode Signature**

Signature Valid:	false
Signature Issuer:	E=Pentadrachm@Troller.tr, CN=smykkeskrin, OU=POLYURETAN, O=VANDBRERENS, L=Microcolorimetric, S=nationalliberales, C=GF
Signature Validation Error:	<b>A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider</b>
Error Number:	-2146762487
Not Before, Not After	<ul style="list-style-type: none"><li>6/15/2021 1:59:30 PM 6/15/2022 1:59:30 PM</li></ul>
Subject Chain	<ul style="list-style-type: none"><li>E=Pentadrachm@Troller.tr, CN=smykkeskrin, OU=POLYURETAN, O=VANDBRERENS, L=Microcolorimetric, S=nationalliberales, C=GF</li></ul>
Version:	3
Thumbprint MD5:	06AF2709916BCE0CF03CF59BA855DE36
Thumbprint SHA-1:	AB72123C786FF25DC7F4258DB4A20D3CA00FBFB8
Thumbprint SHA-256:	C3815096127C1922171F6EF636BBECFBE8418FE97148EC9A27CB6B4FE180836A
Serial:	00

**Entrypoint Preview**

**Data Directories**

**Sections**


Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1eda8	0x1f000	False	0.502488659274	data	6.34204533529	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x20000	0x1220	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x22000	0x6d0a	0x7000	False	0.611921037946	data	6.03995475111	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
Kazakh	Kazakhstan	

## Network Behavior

No network behavior found

## Code Manipulations

## Statistics

## System Behavior

Analysis Process: OrdineFornitore\_Nr\_2021\_OV\_445..exe PID: 6896 Parent PID: 6012

### General

Start time:	15:59:26
Start date:	15/06/2021
Path:	C:\Users\user\Desktop\OrdineFornitore_Nr_2021_OV_445..exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\OrdineFornitore_Nr_2021_OV_445..exe'
Imagebase:	0x400000
File size:	165640 bytes
MD5 hash:	CA5DBE288EF27FD1A4BB491A3119285F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	<ul style="list-style-type: none"><li>Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.1011030674.0000000002240000.00000040.00000001.sdmp, Author: Joe Security</li></ul>
Reputation:	low

### File Activities

Show Windows behavior

## Disassembly

### Code Analysis