

JOeSandbox Cloud BASIC



**ID:** 528460

**Sample Name:** ORDINE + DDT

A.M.F SpA.exe

**Cookbook:** default.jbs

**Time:** 10:37:18

**Date:** 25/11/2021

**Version:** 34.0.0 Boulder Opal

## Table of Contents

Table of Contents	2
Windows Analysis Report ORDINE + DDT A.M.F SpA.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
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 URLs	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	9
Static PE Info	9
General	9
Authenticode Signature	9
Entrypoint Preview	9
Data Directories	9
Sections	9
Resources	10
Imports	10
Version Infos	10
Possible Origin	10
Network Behavior	10
Code Manipulations	10
Statistics	10
System Behavior	10
Analysis Process: ORDINE + DDT A.M.F SpA.exe PID: 6416 Parent PID: 4944	10
General	10
File Activities	11
Disassembly	11
Code Analysis	11

# Windows Analysis Report ORDINE + DDT A.M.F SpA.exe

## Overview

### General Information

Sample Name:

ORDINE + DDT A.M.F SpA.exe

Analysis ID:

528460

MD5:

f5423b7a8987604.

SHA1:

24c550c47d2609..

SHA256:




68a31512334944..

Tags:

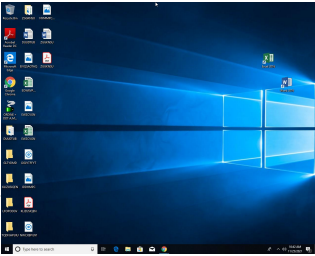
exe

guloader

Infos:

Most interesting Screenshot:



### Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

GuLoader

Score:

76

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

### Signatures

Found malware configuration

Multi AV Scanner detection for subm...

Yara detected GuLoader

Tries to detect virtualization through...

C2 URLs / IPs found in malware con...

Found potential dummy code loops (...)

Uses 32bit PE files

Sample file is different than original ...

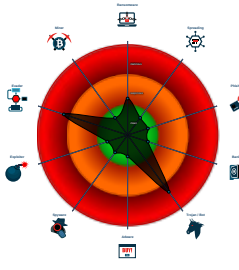
PE file contains strange resources

Contains functionality to read the PEB


Uses code obfuscation techniques (...)

Detected potential crypto function

### Classification



## Process Tree

- System is w10x64
-  ORDINE + DDT A.M.F SpA.exe (PID: 6416 cmdline: "C:\Users\user\Desktop\ORDINE + DDT A.M.F SpA.exe" MD5: F5423B7A89876044078CBB68DB883AF8)
- cleanup

## Malware Configuration

Threatname: GuLoader

```
{  "Payload URL": "https://fabricraft.co.za/Farmant_hhVNwJna195.bin"}
```

## Yara Overview

### Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.770096860.000000000213 0000.00000040.00000001.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

## Networking:



C2 URLs / IPs found in malware configuration

## 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)

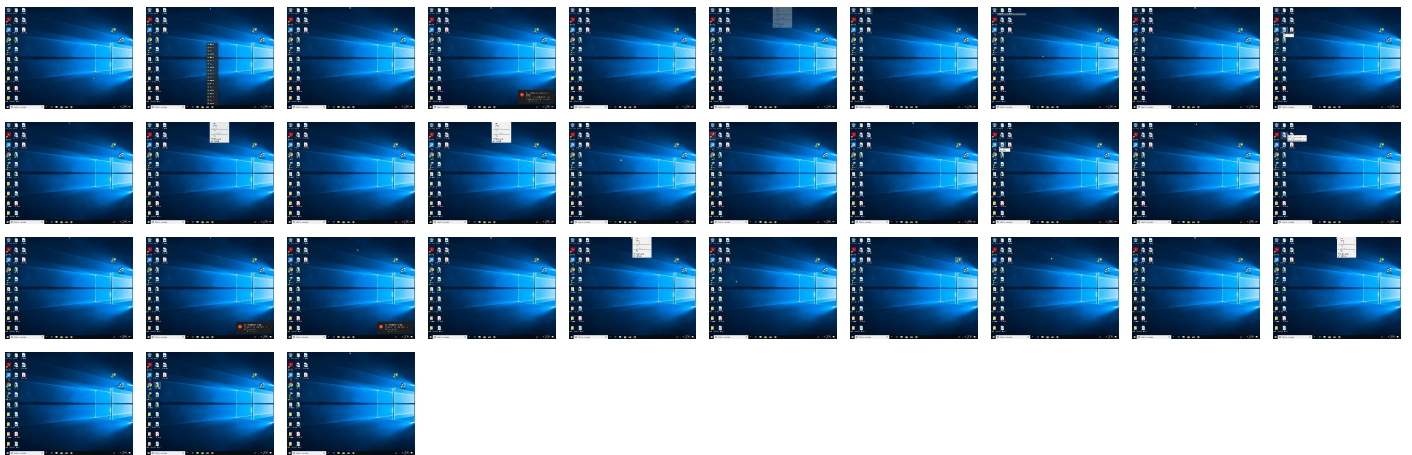
## Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Recovery
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	Recovery Time Windows
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 Time Windows
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	Operational Capability
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	Recovery Time Windows

## 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
ORDINE + DDT A.M.F SpA.exe	22%	Virustotal		<a href="#">Browse</a>

### 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 URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://fabricraft.co.za/Farmant_hhVNWJna195.bin	false		high

### Contacted IPs

No contacted IP infos

## General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528460
Start date:	25.11.2021
Start time:	10:37:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ORDINE + DDT A.M.F SpA.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:	24
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:	mal76.troj.evad.winEXE@1/1@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none"><li>• Successful, ratio: 0.7% (good quality ratio 0.2%)</li><li>• Quality average: 20.2%</li><li>• Quality standard deviation: 32.4%</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

C:\Users\user\AppData\Local\Temp\~DF61EBE6BB9760AAB6.TMP	
Process:	C:\Users\user\Desktop\ORDINE + DDT A.M.F SpA.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	1.5460794479699351
Encrypted:	false
SSDEEP:	96:kOtJyg4D7OKBqQOtJyg4D1DDPwYDPXxJXf6nZV4XoB:1KD7OKAJKD1DDPwYDPXxJXf6nZV4XoB
MD5:	A10173F2BC7809BD9C218B204F91B9B5
SHA1:	CCC33C4FF5908D771A921E81FA6DEC9E83BF9399
SHA-256:	9D569DF219A76092E36A090729EF451275255D21A7B7FA9BEEA8431DF88906D8
SHA-512:	F2FB87D14882D23D9F49F4AE31D179CE083C0D7F2C87755C68600CDBB8A48E06E02DBFD0FCF42BB7611590FDF03EB4FDA0B5FBB530A1DB4AAB5487099A495FDB
Malicious:	false
Reputation:	low
Preview:	.....>..... ..... ..... .....

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.174630404591659
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, flfi, cel) (7/3) 0.00%</li></ul>
File name:	ORDINE + DDT A.M.F SpA.exe
File size:	164928



<b>General</b>	
MD5:	f5423b7a89876044078cbb68db883af8
SHA1:	24c550c47d26090f298fea030d7fb890c94737a5
SHA256:	68a315123349444d30fed12643a7be20eb003531a4b95d0db800fb765449037d
SHA512:	a1e0da217c0a383878405f53b7318316d87fa7483831429ef50973a526bf160baa855ac2b7853dfe95b15265aee3bba9044ad04ee4319ab41cb2fdb1cd2cf166
SSDEEP:	3072:9cqN5FpupBqUudn4Qw6cOOxQnLC6hpA7VHACd:xN5mpBHAYxQnLn4D
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode.....\$......7b..s...s. ..s.....r...<!.v..E%.r...Richs.....PE..L..... O..... ..`.....@.....0....@

<b>File Icon</b>	
	
Icon Hash:	e5c1e079b0dcdc3c

<b>Static PE Info</b>	
<b>General</b>	
Entrypoint:	0x401640
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:	0x4FF98A07 [Sun Jul 8 13:24:23 2012 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:	90425c3cfb1918f16a4ffb8047a25e88

<b>Authenticode Signature</b>	
Signature Valid:	false
Signature Issuer:	E=Halvmilitr5@Pasan.Out, CN=yeara, OU=Hnisses, O=Frstestyrmndenes, L=langhalms, S=Targon, C=TH
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>11/24/2021 10:31:27 PM 11/24/2022 10:31:27 PM</li></ul>
Subject Chain	<ul style="list-style-type: none"><li>E=Halvmilitr5@Pasan.Out, CN=yeara, OU=Hnisses, O=Frstestyrmndenes, L=langhalms, S=Targon, C=TH</li></ul>
Version:	3
Thumbprint MD5:	1675B0681F6E08F88C72FD3302E50FD9
Thumbprint SHA-1:	DDEB96699987B30C7A4E263EC2B1CE4BED20032D
Thumbprint SHA-256:	490EABAB012CB43983C62C20A02D579B84FABA9ADF4734E32E4330690D5139D1
Serial:	00

<b>Entrypoint Preview</b>
---------------------------

<b>Data Directories</b>
-------------------------

<b>Sections</b>
-----------------

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x21bcc	0x22000	False	0.385268267463	data	6.40485948077	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x23000	0x20b4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x26000	0x22a4	0x3000	False	0.194580078125	data	3.74537367217	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	
Chinese	Taiwan	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: ORDINE + DDT A.M.F SpA.exe PID: 6416 Parent PID: 4944

General

Start time:	10:38:35
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\ORDINE + DDT A.M.F SpA.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\ORDINE + DDT A.M.F SpA.exe"
Imagebase:	0x400000
File size:	164928 bytes
MD5 hash:	F5423B7A89876044078CBB68DB883AF8
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: 00000000.00000002.770096860.0000000002130000.00000040.00000001.sdmp, Author: Joe Security</li></ul>
Reputation:	low

[File Activities](#)

Show Windows behavior

Disassembly

Code Analysis