

JoeSandbox Cloud BASIC



**ID:** 482590

**Sample Name:** NOA\_-  
\_CMA\_CGM\_ARRIVAL\_NOTICE  
.exe

**Cookbook:** default.jbs

**Time:** 22:41:49

**Date:** 13/09/2021

**Version:** 33.0.0 White Diamond

## Table of Contents

Table of Contents	2
Windows Analysis Report NOA_-_CMA_CGM_ARRIVAL_NOTICE.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	4
AV Detection:	4
Networking:	4
System Summary:	4
Data Obfuscation:	4
Malware Analysis System Evasion:	4
Anti Debugging:	4
Stealing of Sensitive Information:	4
Mitre Att&ck Matrix	4
Behavior Graph	5
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	8
Static PE Info	9
General	9
Entrypoint Preview	9
Data Directories	9
Sections	9
Resources	9
Imports	9
Version Infos	9
Possible Origin	9
Network Behavior	9
Code Manipulations	9
Statistics	10
Behavior	10
System Behavior	10
Analysis Process: NOA_-_CMA_CGM_ARRIVAL_NOTICE.exe PID: 5520 Parent PID: 1408	10
General	10
Registry Activities	10
Key Created	10
Key Value Created	10
Analysis Process: NOA_-_CMA_CGM_ARRIVAL_NOTICE.exe PID: 3080 Parent PID: 5520	10
General	10
Disassembly	11
Code Analysis	11

# Windows Analysis Report NOA\_-\_CMA\_CGM\_ARRIVAL...

## Overview

General Information

Sample Name:

NOA\_-\_CMA\_CGM\_ARRIVAL\_NOTICE.exe

Analysis ID:

482590

MD5:

e8bceea59b2074...

SHA1:

8b62bf811b03fe2...

SHA256:

0b4684d82509a6...

Tags:

exe

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

GuLoader

Score:

92

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Found malware configuration

Multi AV Scanner detection for subm...

GuLoader behavior detected

Yara detected GuLoader

Hides threads from debuggers

Initial sample is a PE file and has a ...

Tries to detect Any.run

C2 URLs / IPs found in malware con...

Tries to detect sandboxes and other...

Uses 32bit PE files

Sample file is different than original ...

PE file contains an invalid checksum

Classification

Process Tree

System is w10x64

NOA\_-\_CMA\_CGM\_ARRIVAL\_NOTICE.exe (PID: 5520 cmdline: 'C:\Users\user\Desktop\NOA\_-\_CMA\_CGM\_ARRIVAL\_NOTICE.exe' MD5: E8BCEEA59B2074BD08BF68AB55ECDF3E)

NOA\_-\_CMA\_CGM\_ARRIVAL\_NOTICE.exe (PID: 3080 cmdline: 'C:\Users\user\Desktop\NOA\_-\_CMA\_CGM\_ARRIVAL\_NOTICE.exe' MD5: E8BCEEA59B2074BD08BF68AB55ECDF3E)

cleanup

## Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://www.paulassinkarchitect.nl/bin_fDiyu115.bin"
}
```

## Yara Overview

Source	Rule	Description	Author	Strings
00000017.00000002.783554447.0000000000056 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000001.00000002.544066668.00000000024E 0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	


## Sigma Overview

No Sigma rule has matched

Copyright Joe Security LLC 2021

Page 3 of 11

## Jbx 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:



Initial sample is a PE file and has a suspicious name

### Data Obfuscation:



Yara detected GuLoader

### Malware Analysis System Evasion:



Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

### Anti Debugging:



Hides threads from debuggers

### Stealing of Sensitive Information:

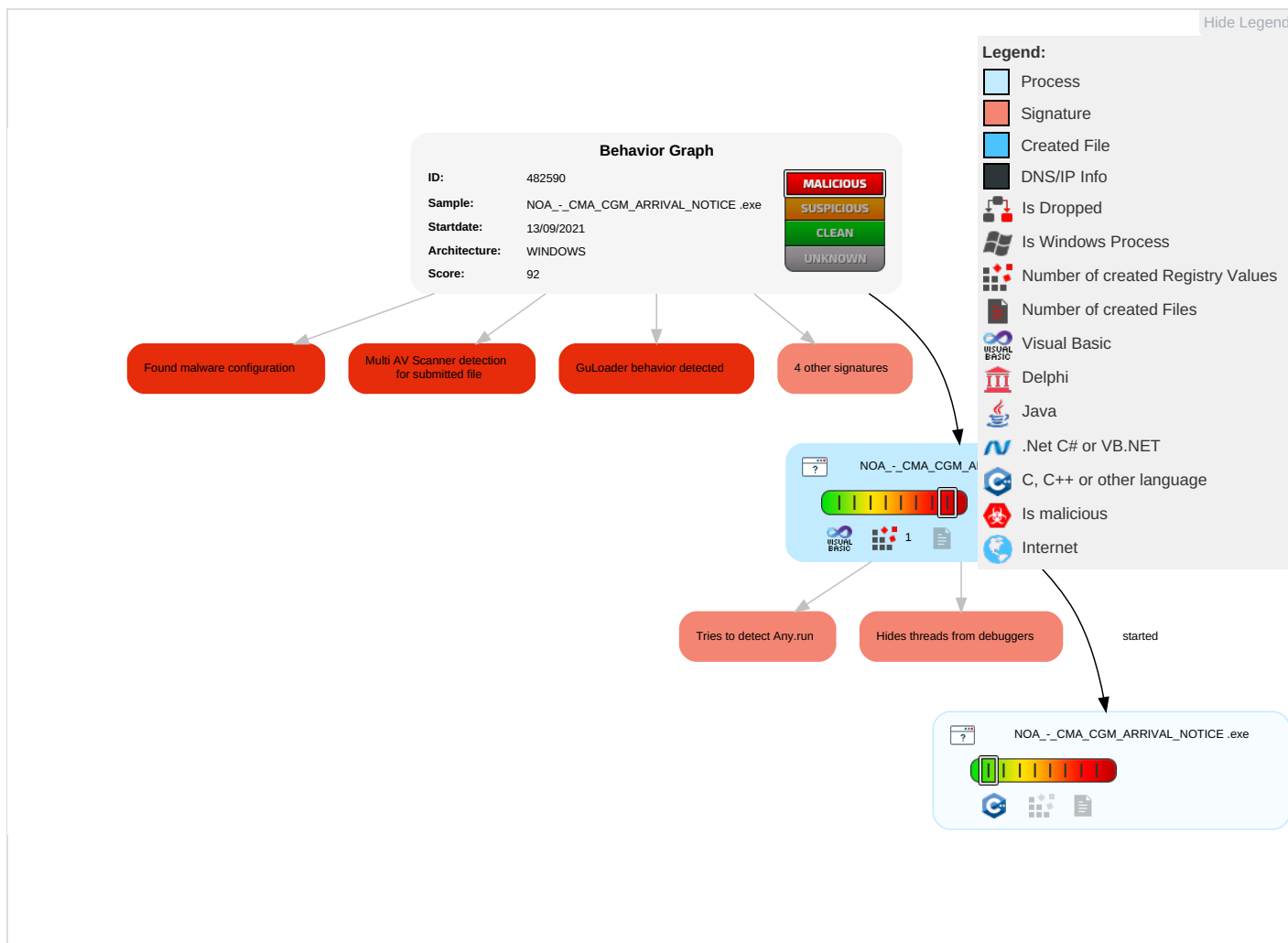


GuLoader behavior detected

## Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection <span>1</span> <span>2</span>	Virtualization/Sandbox Evasion <span>2</span> <span>1</span>	OS Credential Dumping	Security Software Discovery <span>3</span> <span>2</span> <span>1</span>	Remote Services	Archive Collected Data <span>1</span>	Exfiltration Over Other Network Medium	Encrypted Channel <span>1</span>	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection <span>1</span> <span>2</span>	LSASS Memory	Virtualization/Sandbox Evasion <span>2</span> <span>1</span>	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol <span>1</span>	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information <span>1</span>	Security Account Manager	Process Discovery <span>1</span>	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery <span>2</span>	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap

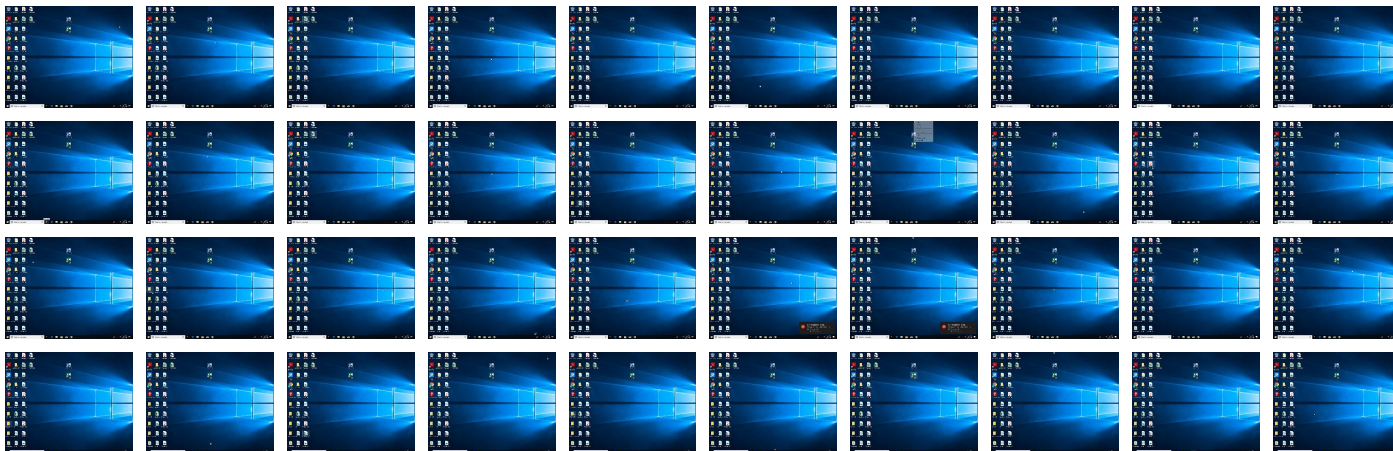
## Behavior Graph



## 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
NOA_-_CMA_CGM_ARRIVAL_NOTICE .exe	25%	Virustotal		<a href="#">Browse</a>
NOA_-_CMA_CGM_ARRIVAL_NOTICE .exe	18%	ReversingLabs	Win32.Trojan.Mucc	

### Dropped Files

No Antivirus matches

### Unpacked PE Files

No Antivirus matches

### Domains

No Antivirus matches

### URLs

Source	Detection	Scanner	Label	Link
<a href="http://https://www.paulassinkarchitect.nl/bin_fDiyu115.bin">http://https://www.paulassinkarchitect.nl/bin_fDiyu115.bin</a>	0%	Avira URL Cloud	safe	

## Domains and IPs

### Contacted Domains

No contacted domains info

### Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.paulassinkarchitect.nl/bin_fDiyu115.bin	true	<ul style="list-style-type: none"><li>Avira URL Cloud: safe</li></ul>	unknown

### Contacted IPs

No contacted IP infos

## General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	482590
Start date:	13.09.2021
Start time:	22:41:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NOA_-_CMA_CGM_ARRIVAL_NOTICE.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:	25
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:	mal92.troj.evad.winEXE@3/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none"><li>Successful, ratio: 24.1% (good quality ratio 15.1%)</li><li>Quality average: 29.8%</li><li>Quality standard deviation: 27.1%</li></ul>
HCA Information:	<ul style="list-style-type: none"><li>Successful, ratio: 88%</li><li>Number of executed functions: 0</li><li>Number of non-executed functions: 0</li></ul>
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):	4.255614019053077
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:	NOA_ - _CMA_ CGM_ ARRIVAL_ NOTICE .exe
File size:	466944
MD5:	e8bceea59b2074bd08bf68ab55ecdff3e
SHA1:	8b62bf811b03fe25924ef6ff4d4afd89c902f7cd
SHA256:	0b4684d82509a6e7e0c1cb63174bf68d182ccff75a3d19f16821127605d636b8
SHA512:	405f00ffa49ecb3131f0a16afa2b4488c8580c2c8161a0bd4384b9218c9dc74a21812fe6a86f49c16f08959b4743d9f19bb07f7524ce63e6ed339ab01679add1
SSDEEP:	12288:8HLEuNNNNN6NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNGvNNNNNNNasgTJ4KJ1Z:8HY2csg9h1Z
File Content Preview:	MZ.....@.....!..!Th is program cannot be run in DOS mode....\$......6...W...W...W...K...W...u...W...q...W...Rich.W.....PE ..L...f=L.....P.....H.....`....@

File Icon



	
Icon Hash:	70f0a231b3b2f071

## Static PE Info

### General

Entrypoint:	0x401448
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:	0x4C3D6691 [Wed Jul 14 07:26:09 2010 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:	01b006fd37878659f6f60ca0efdc2460

### Entrypoint Preview

### Data Directories

### Sections


Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x44f28	0x45000	False	0.271176545516	data	4.83437034271	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x46000	0x148c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x48000	0x2a156	0x2b000	False	0.161876589753	data	3.15995554576	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

## Behavior



Click to jump to process

## System Behavior

Analysis Process: NOA\_-\_CMA\_CGM\_ARRIVAL\_NOTICE.exe PID: 5520 Parent PID: 1408

### General

Start time:	22:42:54
Start date:	13/09/2021
Path:	C:\Users\user\Desktop\NOA_-_CMA_CGM_ARRIVAL_NOTICE.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NOA_-_CMA_CGM_ARRIVAL_NOTICE.exe'
Imagebase:	0x400000
File size:	466944 bytes
MD5 hash:	E8BCEE59B2074BD08BF68AB55ECDF3E
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: 00000001.00000002.544066668.00000000024E0000.00000040.00000001.sdmp, Author: Joe Security</li></ul>
Reputation:	low

### Registry Activities

Show Windows behavior

### Key Created

### Key Value Created

Analysis Process: NOA\_-\_CMA\_CGM\_ARRIVAL\_NOTICE.exe PID: 3080 Parent PID: 5520

### General

Start time:	22:45:05
Start date:	13/09/2021
Path:	C:\Users\user\Desktop\NOA_-_CMA_CGM_ARRIVAL_NOTICE.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NOA_-_CMA_CGM_ARRIVAL_NOTICE.exe'
Imagebase:	0x400000
File size:	466944 bytes
MD5 hash:	E8BCEE59B2074BD08BF68AB55ECDF3E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	<ul style="list-style-type: none"><li>Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000017.00000002.783554447.0000000000560000.00000040.00000001.sdmp, Author: Joe Security</li></ul>
Reputation:	low

## Disassembly

## Code Analysis