

ID: 482886
Sample Name: NOA_-_CMA_CGM_ARRIVAL_NOTICE.lzh
Cookbook: default.jbs
Time: 09:50:53
Date: 14/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report NOA_-_CMA_CGM_ARRIVAL_NOTICE.lzh 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Overview 3
Sigma Overview 3
Jbx Signature Overview 3
AV Detection: 4
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 4
Thumbnails 4
Antivirus, Machine Learning and Genetic Malware Detection 5
Initial Sample 5
Dropped Files 6
Unpacked PE Files 6
Domains 6
URLs 6
Domains and IPs 6
Contacted Domains 6
Contacted IPs 6
General Information 6
Simulations 7
Behavior and APIs 7
Joe Sandbox View / Context 7
IPs 7
Domains 7
ASN 7
JA3 Fingerprints 7
Dropped Files 7
Created / dropped Files 7
Static File Info 8
General 8
File Icon 8
Network Behavior 8
Code Manipulations 8
Statistics 8
Behavior 8
System Behavior 8
Analysis Process: unarchiver.exe PID: 2172 Parent PID: 1576 8
General 8
File Activities 9
File Created 9
File Written 9
File Read 9
Analysis Process: 7za.exe PID: 5036 Parent PID: 2172 9
General 9
Disassembly 9
Code Analysis 9

Copyright Joe Security LLC 2021

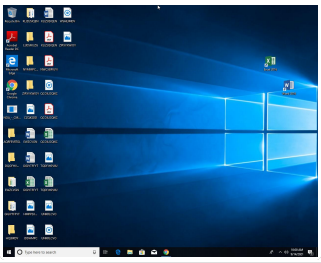
Windows Analysis Report NOA_-_CMA_CGM_ARRIVAL…

Overview

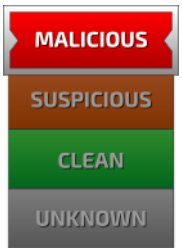
General Information

Sample Name:	NOA_-_CMA_CGM_ARRIVAL_NOTICE.lzh
Analysis ID:	482886
MD5:	b71a9e47912352..
SHA1:	5aae421b9bc63d..
SHA256:	1908c35415f99b5.
Infos:	

Most interesting Screenshot:



Detection

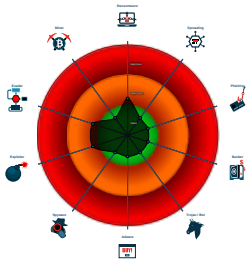


Score:	48
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Found inlined nop instructions (likely…
- Creates a process in suspended mo…
- Detected potential crypto function

Classification



Process Tree

- **System is w10x64**
- unarchiver.exe (PID: 2172 cmdline: 'C:\Windows\SysWOW64\unarchiver.exe' 'C:\Users\user\Desktop\NOA_-_CMA_CGM_ARRIVAL_NOTICE.lzh' MD5: DB55139D9DD29F24AE8EA8F0E5606901)
  - 7za.exe (PID: 5036 cmdline: 'C:\Windows\System32\7za.exe' x -pinfected -y -o'C:\Users\user\AppData\Local\Temp\zdsmcxok.014' 'C:\Users\user\Desktop\NOA_-_CMA_CGM_ARRIVAL_NOTICE.lzh' MD5: 77E556CDFDC5C592F5C46DB4127C6F4C)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

Copyright Joe Security LLC 2021

AV Detection:

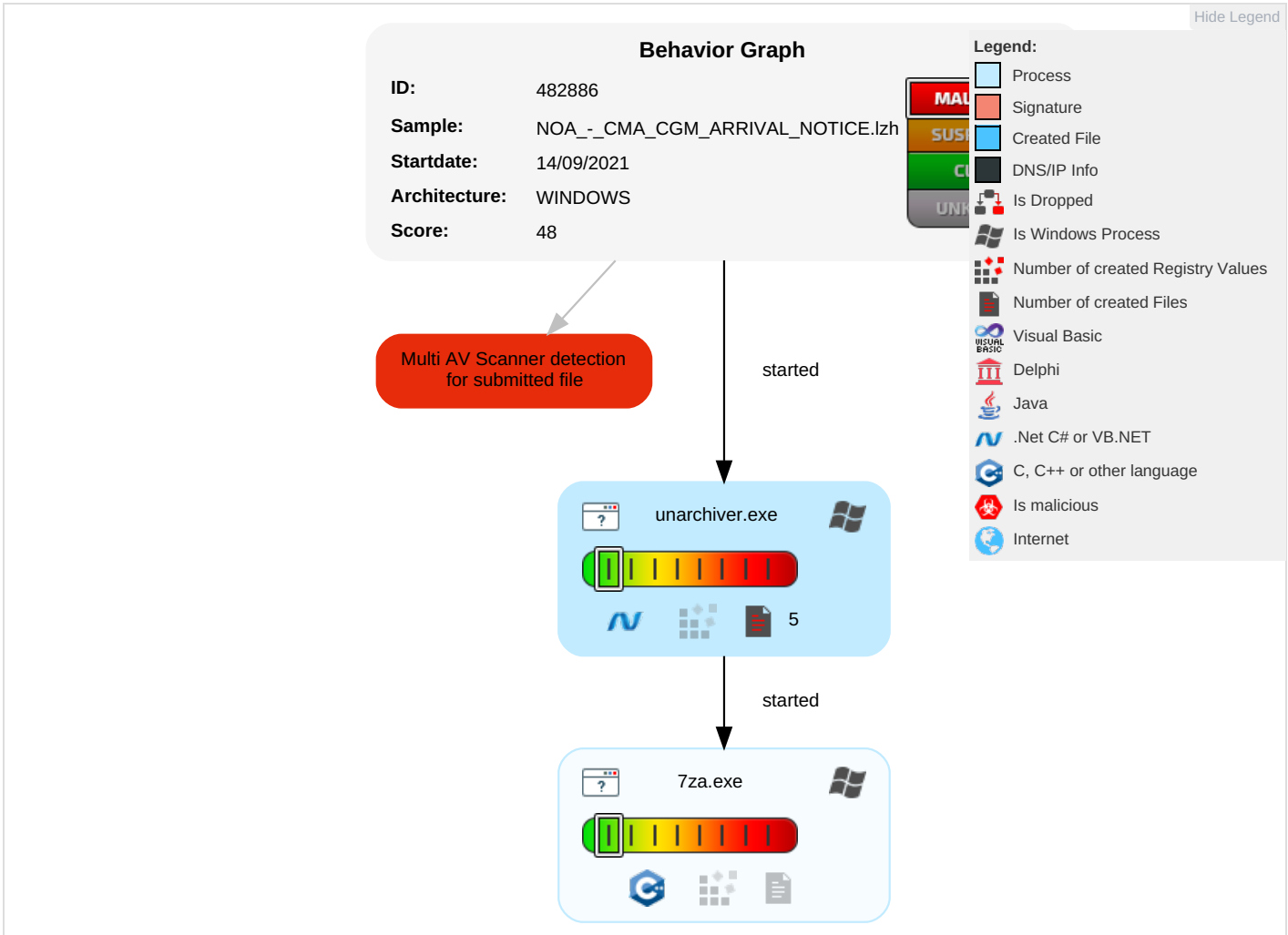


Multi AV Scanner detection for submitted file

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	In
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 2	Disable or Modify Tools 1	OS Credential Dumping	Process Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M Sy Pa
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D Lo
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D

Behavior Graph

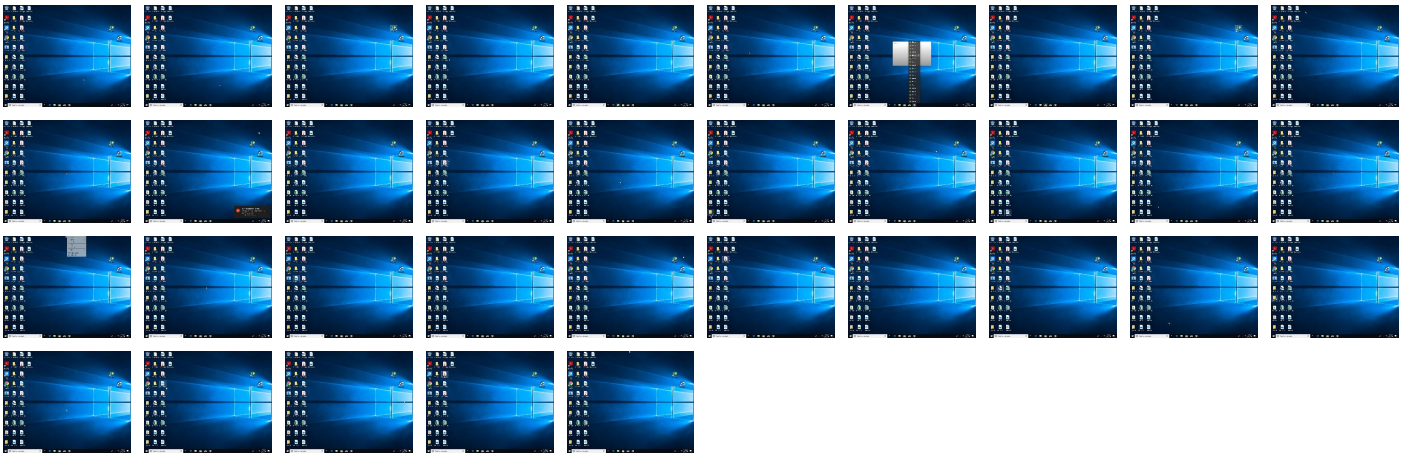


Screenshots

Thumbnails

Copyright Joe Security LLC 2021

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.lzh	14%	Virustotal		Browse
NOA_-_CMA_CGM_ARRIVAL_NOTICE.lzh	40%	ReversingLabs	Win32.Backdoor.Androm	

Copyright Joe Security LLC 2021

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:	33.0.0 White Diamond
Analysis ID:	482886
Start date:	14.09.2021
Start time:	09:50:53
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NOA_-_CMA_CGM_ARRIVAL_NOTICE.lzh
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
Run name:	Suspected Instruction Hammering Hide Perf
Number of analysed new started processes analysed:	37
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:	mal48.winLZH@3/1@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Copyright Joe Security LLC 2021

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .lzh
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\103b5ifs.cxq\unarchiver.log	
Process:	C:\Windows\SysWOW64\unarchiver.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	164
Entropy (8bit):	5.281035011969486
Encrypted:	false
SSDEEP:	3:t9tIoC1OUfuWDUWJRWrfj6MwkZJsmo6OKUsttIoDoF8UWWDUkh4E2J5xAIhKh+Ry:moDU1NJAbj6qsD9oDu1923fu
MD5:	46A89269107BA94195D3A2A20DFFAA9A
SHA1:	532B3843A26A4B771791FD3852C7655674475A08
SHA-256:	2B3BB182ED50A9ED2B11634E5302EEA3DE5DD87C0ED0224F10159640950457CB
SHA-512:	042A8AC300009739B2F2FA258095A128B96AE6ECE6B04E6107E75B0889A6DC5F5AD8CCBB97228DBE6C18F4BB7C45ED9B4241C3B070412302D3B3F588DACB9D1
Malicious:	false
Reputation:	low
Preview:	09/14/2021 9:51 AM: Unpack: C:\Users\user\Desktop\NOA_-_CMA_CGM_ARRIVAL_NOTICE.lzh..09/14/2021 9:51 AM: Tmp dir: C:\Users\user\AppData\Local\Temp\zdsmcxok.014..

Static File Info

General

File type:	LHa (2.x) archive data [lh5], with "NOA_-_CMA_CGM_ARRIVAL_NOTICE.exe"
Entropy (8bit):	7.983327494950816
TrID:	• LHARC/LZARK compressed archive (6/4) 100.00%
File name:	NOA_-_CMA_CGM_ARRIVAL_NOTICE.lzh
File size:	107136
MD5:	b71a9e479123528ba6f7b8642b924d0e
SHA1:	5aae421b9bc63d5982f5ef0e19abdfb85cb1688b
SHA256:	1908c35415f99b55e81ea5dd70da0ebbd3e341cd4d2cf77a418c09235be590d5
SHA512:	ba6f16107c9a944ca2c62b419ff29933caad97650f4482102f92c364d95d52282710a2882723785373035e79828e56f98aee69f0f280b81c9cecbe103e7dbcde
SSDEEP:	3072:dVlHrjorhU1+isBSk4x1DdS3sdP2hxhBpimq:9r8U+94x1Z2s1qxPY
File Content Preview:	6.-lh5-H....0....-S . NOA_-_CMA_CGM_ARRIVAL_NOTICE.exe..^.....]..x.....2.Z....R..Z*T..R....f.....P..2j.IEU..HQU$.....}.....=.....y...{..|.'.;.....@....#m.3<E.....=.....5...e..|..k..U....x.N...%..i..B..AC.5c@i ..".....6..c...j. t.....

File Icon



Icon Hash:	00828e8e8686b000

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: unarchiver.exe PID: 2172 Parent PID: 1576

General

Start time:	09:51:55
Start date:	14/09/2021
Path:	C:\Windows\SysWOW64\unarchiver.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\SysWOW64\unarchiver.exe' 'C:\Users\user\Desktop\NOA_-_CMA_CGM_ARRIVAL_NOTICE.lzh'

Imagebase:	0xe20000
File size:	10240 bytes
MD5 hash:	DB55139D9DD29F24AE8EA8F0E5606901
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: 7za.exe PID: 5036 Parent PID: 2172

General

Start time:	09:51:56
Start date:	14/09/2021
Path:	C:\Windows\SysWOW64\7za.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\7za.exe' x -pinfected -y -o'C:\Users\user\AppData\Local\Temp\zdsmcxok.014' 'C:\Users\user\Desktop\NOA_-_CMA_CGM_ARRIVAL_NOTICE.lzh'
Imagebase:	0x230000
File size:	289792 bytes
MD5 hash:	77E556CDFDC5C592F5C46DB4127C6F4C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021