ID: 532136
Sample Name:
Transferencia_29_11_2021
17.03.39.exe
Cookbook: default.jbs
Time: 18:59:22
Date: 01/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Copyright Joe Security LLC 2021

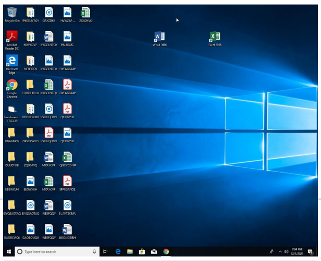
Windows Analysis Report Transferencia_29_11_2021 17…

Overview

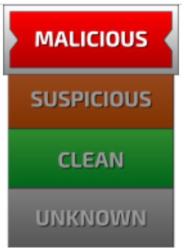
General Information

Sample Name:	Transferencia_29_11_2021 17.03.39.exe
Analysis ID:	532136
MD5:	a70cf8fdf5c68e4…
SHA1:	4a974930db6254..
SHA256:	dd7883497ba8fc4.
Tags:	exe signed
Infos:	

Most interesting Screenshot:



Detection



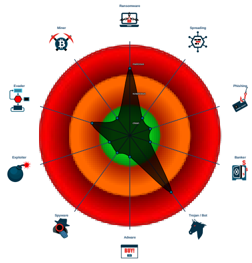
GuLoader

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Potential malicious icon found
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- PE / OLE file has an invalid certificate
- Contains functionality to call native f…
- Sample file is different than original …
- PE file contains strange resources
- Contains functionality to read the PEB
- Uses code obfuscation techniques (…
- Contains functionality for execution …

Classification



Process Tree

- **System is w10x64**
- Transferencia_29_11_2021 17.03.39.exe (PID: 6856 cmdline: "C:\Users\user\Desktop\Transferencia_29_11_2021 17.03.39.exe" MD5: A70CF8FDF5C68E414BAD4494A44F272A)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1V_BC3orZyo_Cje"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.882678032.00000000020F0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Copyright Joe Security LLC 2021

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Potential malicious icon found

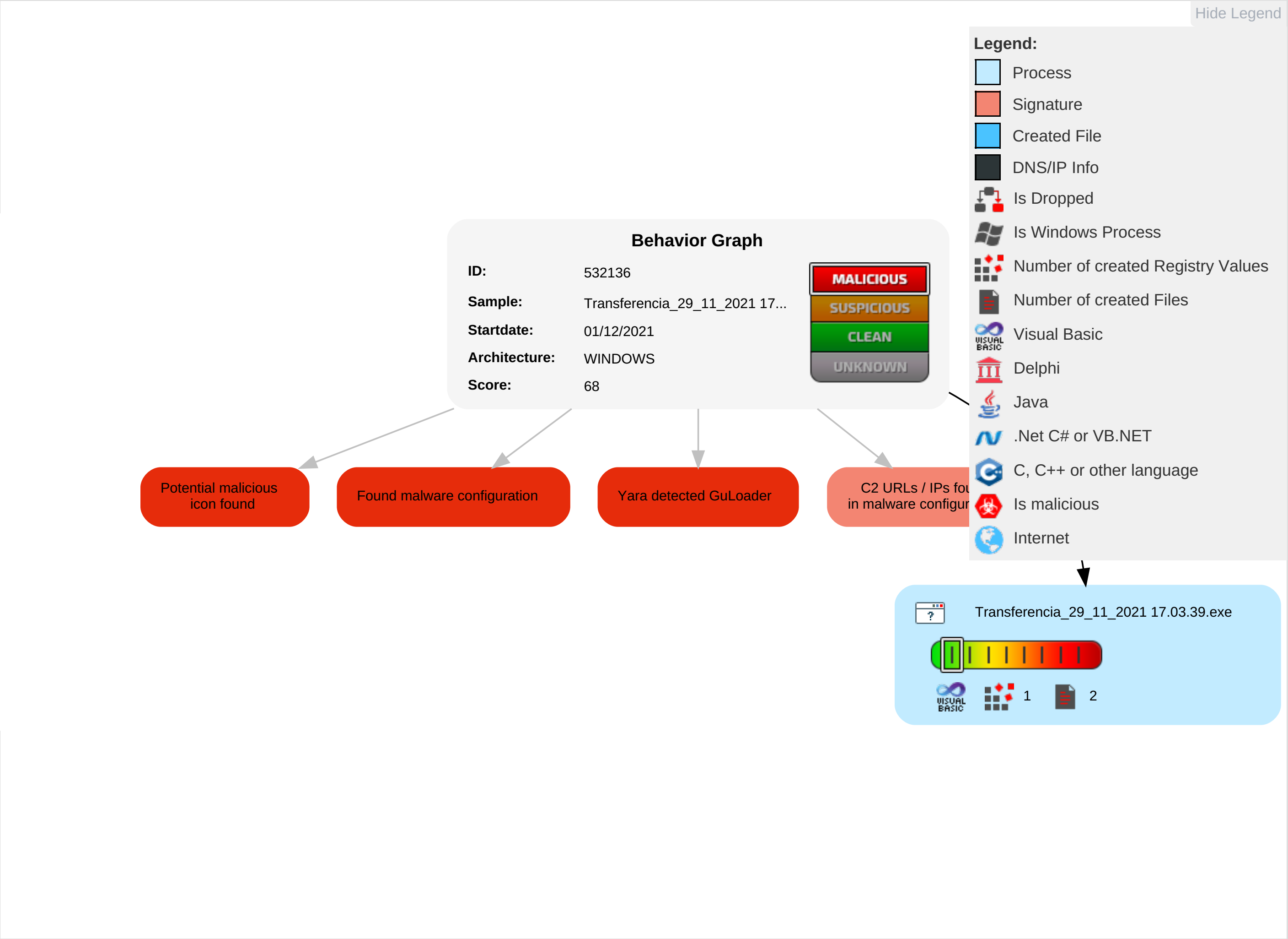
Data Obfuscation:

Yara detected GuLoader

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	Masquerading 1	OS Credential Dumping	Security Software 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	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	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	System Information Discovery 1	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



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

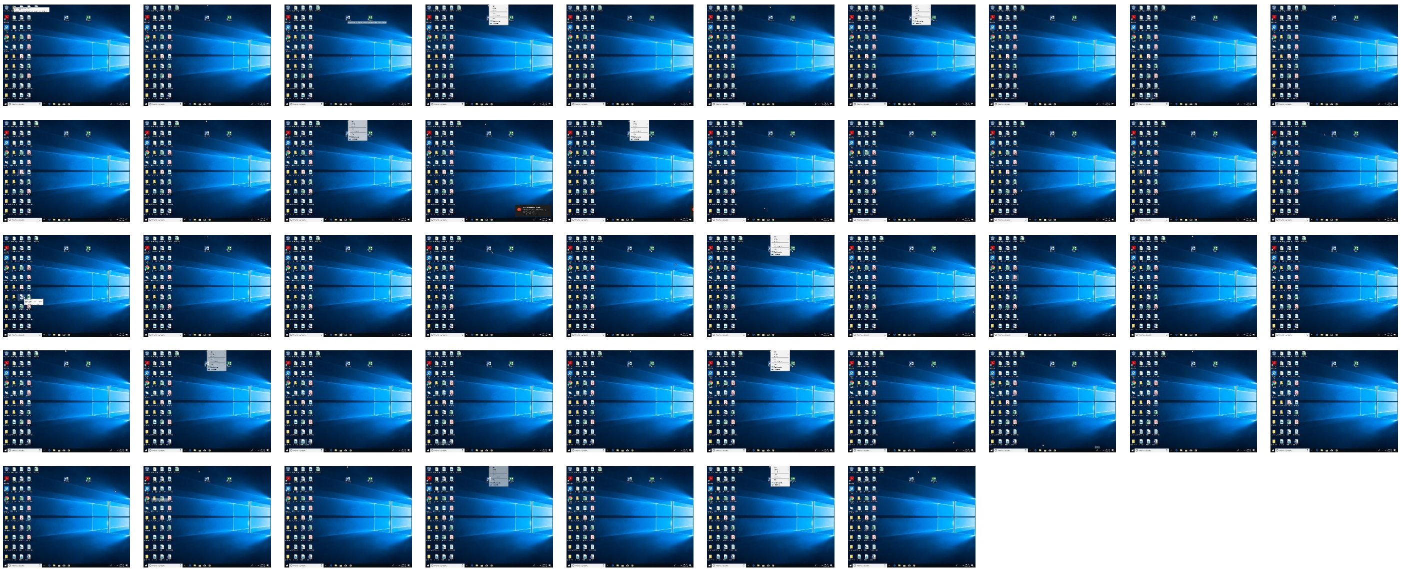
ID:	532136
Sample:	Transferencia_29_11_2021 17...
Startdate:	01/12/2021
Architecture:	WINDOWS
Score:	68

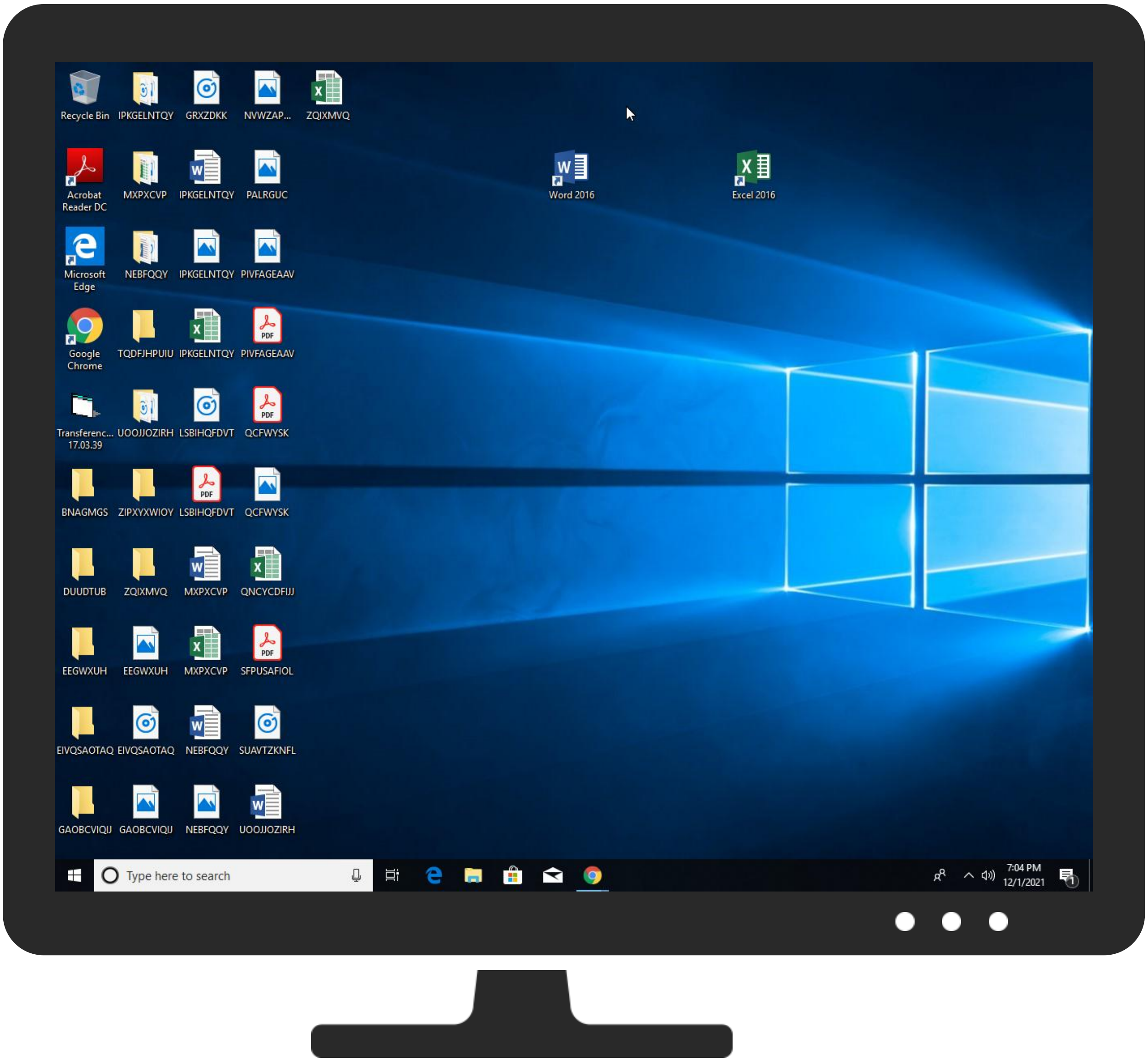
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Potential malicious icon found
Found malware configuration
Yara detected GuLoader
C2 URLs / IPs fou in malware configur
Transferencia_29_11_2021 17.03.39.exe
VISUAL BASIC
1
2

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
Transferencia_29_11_2021 17.03.39.exe	9%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.Transferencia_29_11_2021 17.03.39.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1140082		Download File
0.2.Transferencia_29_11_2021 17.03.39.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1140082		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Copyright Joe Security LLC 2021

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532136
Start date:	01.12.2021
Start time:	18:59:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Transferencia_29_11_2021 17.03.39.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:	20
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:	mal68.rans.troj.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 53.3% (good quality ratio 17.2%) • Quality average: 19.8% • Quality standard deviation: 31.1%
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

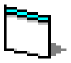
No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.216110090959714
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:	Transferencia_29_11_2021 17.03.39.exe
File size:	152688
MD5:	a70cf8fdf5c68e414bad4494a44f272a
SHA1:	4a974930db625492a8aa3f046759db6f3f057129
SHA256:	dd7883497ba8fc4a8fac606d4f3cec70b6d42c0017e320f9becb071d899c6c30
SHA512:	7279f30ac01665f31e4dd4ff11fb85954d9109953e1d3b04 1971cba8973e6b640eca8794223a5be3762d1911889ba1 2fc8b84c952b49f002f98f1e79ba6eb273
SSDEEP:	1536:4JE6l7m717UopmGeFgk1hG6dvlWOCQe1FpVfBRnOmk:KE6l7mh/UFgk1hG6GOC/lf2mk
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......O.......................D.......=.......Rich............PE..L....7.K.....................0............... ....@................

File Icon



Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401888
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:	0x4B9437E6 [Sun Mar 7 23:33:58 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:	b209c8634733456633136bfedc71877a

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=ansvarslsere@Episcotister1.BON, CN=INDDRIVNING, OU=sporuloid, O=atomkraftvrks, L=Capsheaf, S=Appointed, C=CD
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 12/1/2021 3:06:33 AM 12/1/2022 3:06:33 AM
Subject Chain	• E=ansvarslsere@Episcotister1.BON, CN=INDDRIVNING, OU=sporuloid, O=atomkraftvrks, L=Capsheaf, S=Appointed, C=CD
Version:	3
Thumbprint MD5:	29DB6066933764E6DBF96BB776031AF3
Thumbprint SHA-1:	7F5DF2711E99DDB2A16381EF8330D115FB1C72B2
Thumbprint SHA-256:	B038217303FB0C77E03FB5D245BB31AF36E8932DBBB944A0599B9F5ECB20D07C
Serial:	00

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x20ac4	0x21000	False	0.366751006155	data	5.29953521895	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x22000	0x122c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x24000	0x960	0x1000	False	0.175048828125	data	2.0387904916	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
Chinese	Taiwan	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: Transferencia_29_11_2021 17.03.39.exe PID: 6856 Parent PID: 6076

General

Start time:	19:00:26
Start date:	01/12/2021
Path:	C:\Users\user\Desktop\Transferencia_29_11_2021 17.03.39.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Transferencia_29_11_2021 17.03.39.exe"
Imagebase:	0x400000
File size:	152688 bytes
MD5 hash:	A70CF8FDF5C68E414BAD4494A44F272A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.882678032.00000000020F0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis

Copyright Joe Security LLC

Joe Sandbox Cloud Basic 34.0.0 Boulder Opal