Case Study: Forensic Investigation of a Phishing Attack on Kybereo University

Esomchi Eze

Investigative Report
Attacks, Defence and Protection
03.03.2025
Information and Communication Technology

Contents

1 Introduction

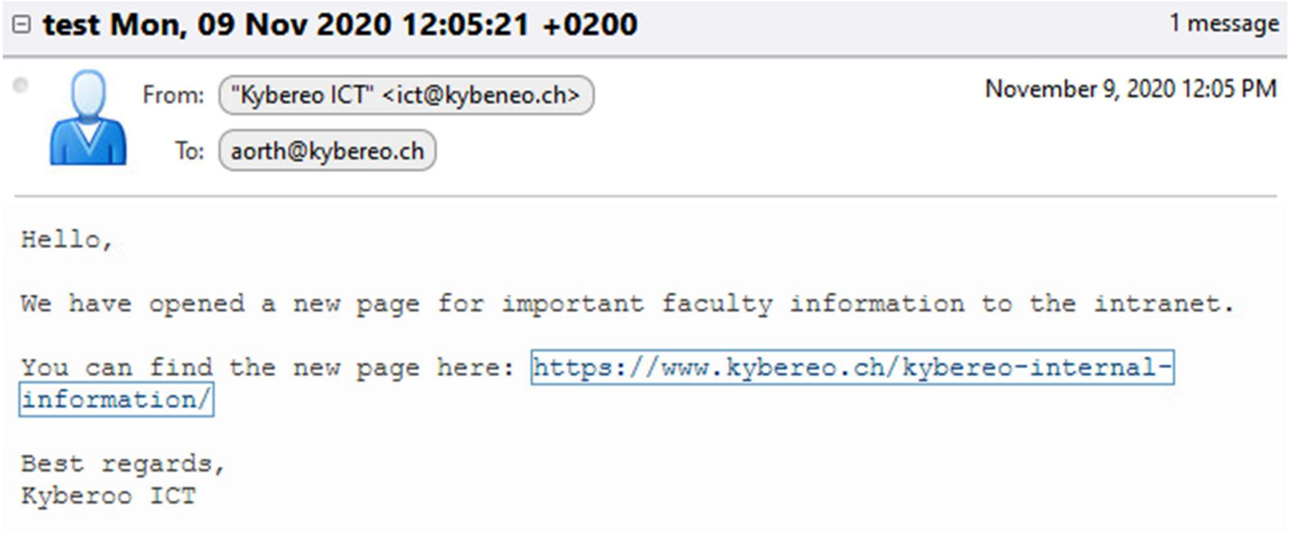
Cyber-attacks are a growing threat, and phishing is one of the most common methods used by hackers to steal information. This report investigates a phishing attack on the University of Kybereo.

The goal of this report is to analyse the attack, find out how it happened, and understand its impact. By using digital forensic techniques, we will identify the phishing email, track where stolen login details went, and examine security weaknesses that made the attack possible.

This report will also provide an explanation of the attack process, security risks, and ways to prevent similar attacks in the future

2 Phishing Attack Investigation.

2.1 Is the message a phishing email?



test Mon, 09 Nov 2020 12:05:21 +0200 1 message

From: "Kybereo ICT" <ict@kybeneo.ch> November 9, 2020 12:05 PM

To: aorth@kybereo.ch

```
Hello,

We have opened a new page for important faculty information to the intranet.

You can find the new page here: https://www.kybereo.ch/kybereo-internal-
information/

Best regards,
Kyberoo ICT
```

Figure 1- Email

This email is a **phishing attempt** due to the following reasons:

- **Suspicious Sender Domain**: The real domain should be **@kybereo.ch**, but the phishing email uses **@kybeneo.ch**.
- **Lack of Personalization**: A legitimate email would say, *“Dear Amelie Orth,”* rather than just *“Hello.”*
- **Malicious Link**: The email urges the recipient to click on a hyperlink (**https://www.kybereo.ch/kybereo-internal-information/**).

- **Spelling and Grammar Errors**: The sentence structure is awkward and unnatural. For example, *"We have opened a new page for important faculty information to the intranet."* sounds incorrect, whereas a legitimate IT email would say, *"We have launched a new faculty information page on the intranet."*
- **Unusual Request**: The email asks the recipient to log in through an external link instead of directing them to the official university portal.
- The contact information has a spelling error. It should be "Kybereo" and not "Kyberoo".

2.2 Where the phishing site mentioned in the email is located?

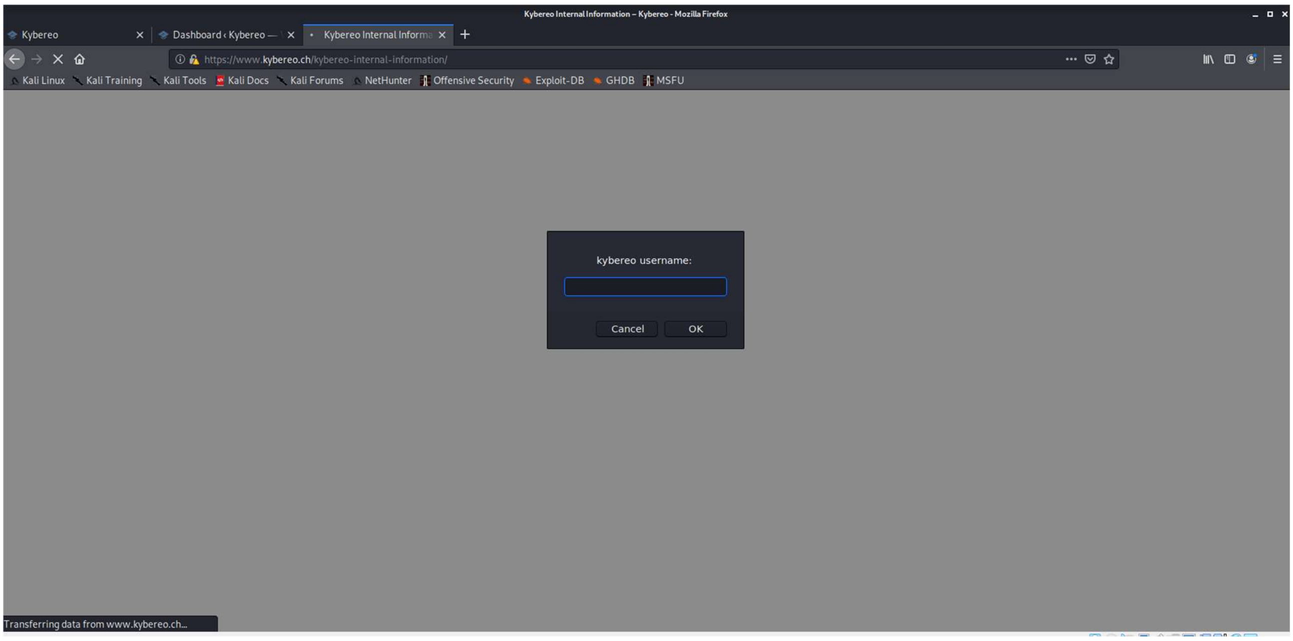


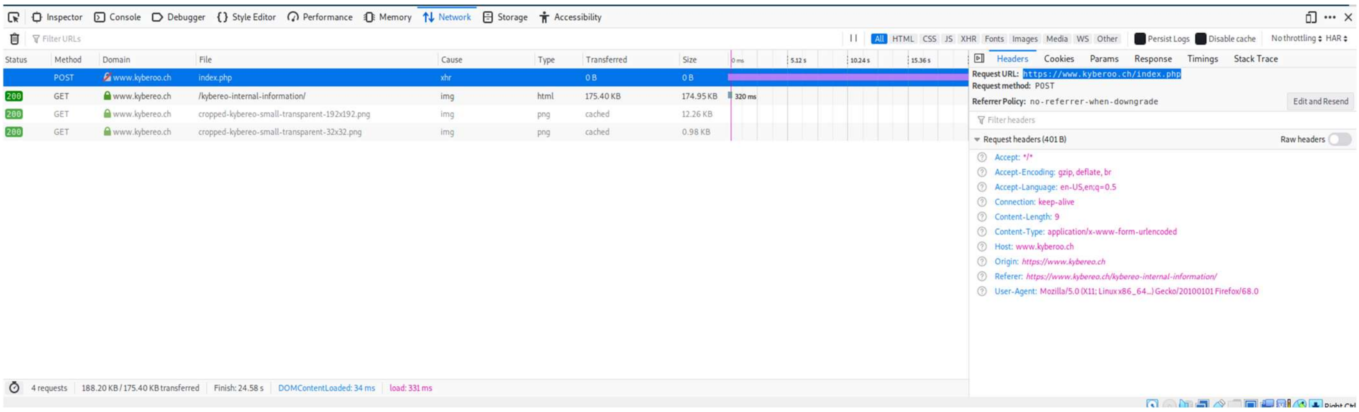
Figure 2- Phising site

The site in the phishing email is located at **https://www.kybereo.ch/kybereo-internal-information/**

Although it may seem real at first glance, several indicators suggest that it is fake. Signs of possible phishing include:

- The sign in box asking for "kybereo username"
- The phishing site is likely hosted on the real **kybereo.ch** domain through a breach or as a fake replica
- The site contains a fake login page designed likely designed to steal usernames and passwords.

2.3 Where the user credentials from the phishing site end up?



Status	Method	Domain	File	Cause	Type	Transferred	Size	0 ms 5.12 s 10.24 s 15.36 s
	POST	www.kyberoo.ch	index.php	xhr		0 B	0 B	
200	GET	www.kybereo.ch	/kybereo-internal-information/	img	html	175.40 KB	174.95 KB	320 ms
200	GET	www.kybereo.ch	cropped-kybereo-small-transparent-192x192.png	img	png	cached	12.26 KB	
200	GET	www.kybereo.ch	cropped-kybereo-small-transparent-32x32.png	img	png	cached	0.98 KB	

4 requests | 188.20 KB / 175.40 KB transferred | Finish: 24.58 s | DOMContentLoaded: 34 ms | load: 331 ms

Request URL: https://www.kyberoo.ch/index.php
Request method: POST
Referrer Policy: no-referrer-when-downgrade

Request headers (401 B)

Accept: */*
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Content-Length: 9
Content-Type: application/x-www-form-urlencoded
Host: www.kyberoo.ch
Origin: https://www.kybereo.ch
Referer: https://www.kybereo.ch/kybereo-internal-information/
User-Agent: Mozilla/5.0 (X11; Linux x86_64...) Gecko/20100101 Firefox/68.0

Figure 3- User Credentials Location

During my investigation, I inspected the phishing site using the Network tab in Developer Tools. I observed that when a user submits their login credentials, the site sends a POST request to `https://www.kyberoo.ch/index.php` using an XMLHttpRequest (XHR). Additionally:

- The phishing site captures user input and transmits it silently.

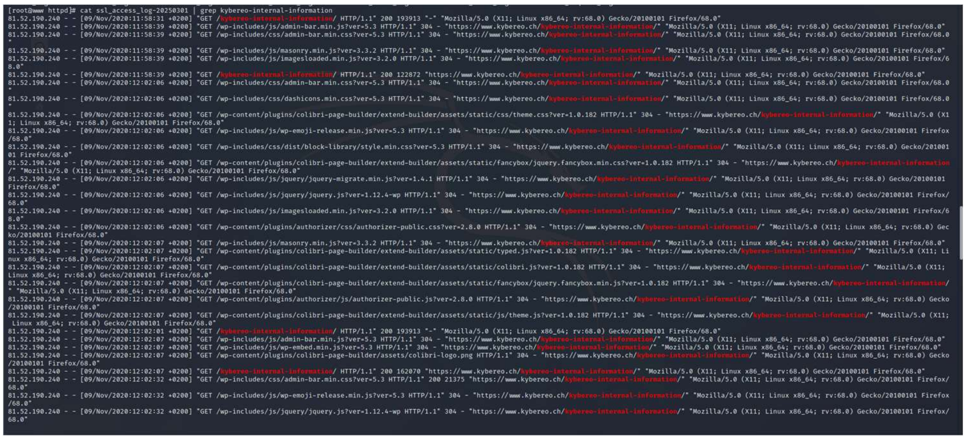
- The POST request sends two key parameters:

a (username)

b (password)

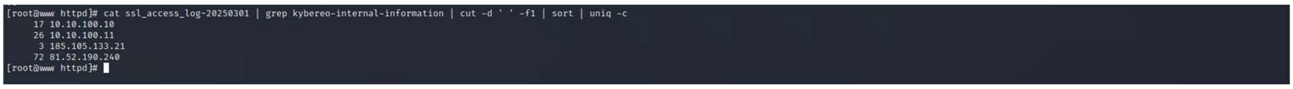
2.4 How many users have visited the phishing site?

Checking the logs of the website, we can continue investigating suspicious activity.



```
[root@www httpd]# cat ssl_access_log-20250301 | grep kybereo-internal-information
81.52.190.240 - - [09/Nov/2020:11:58:31 +0200] "GET /kybereo-internal-information/ HTTP/1.1" 200 193913 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
81.52.190.240 - - [09/Nov/2020:11:58:39 +0200] "GET /wp-includes/js/admin-bar.min.js?ver=5.3 HTTP/1.1" 304 - "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
81.52.190.240 - - [09/Nov/2020:11:58:39 +0200] "GET /wp-includes/css/admin-bar.min.css?ver=5.3 HTTP/1.1" 304 - "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
"
81.52.190.240 - - [09/Nov/2020:11:58:39 +0200] "GET /wp-includes/js/masonry.min.js?ver=3.3.2 HTTP/1.1" 304 - "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
81.52.190.240 - - [09/Nov/2020:11:58:39 +0200] "GET /wp-includes/js/imagesloaded.min.js?ver=3.2.0 HTTP/1.1" 304 - "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/6
8.0"
81.52.190.240 - - [09/Nov/2020:11:58:39 +0200] "GET /kybereo-internal-information/ HTTP/1.1" 200 122872 "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
81.52.190.240 - - [09/Nov/2020:12:02:06 +0200] "GET /wp-includes/css/admin-bar.min.css?ver=5.3 HTTP/1.1" 304 - "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
"
81.52.190.240 - - [09/Nov/2020:12:02:06 +0200] "GET /wp-includes/css/dashicons.min.css?ver=5.3 HTTP/1.1" 304 - "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
"
81.52.190.240 - - [09/Nov/2020:12:02:06 +0200] "GET /wp-content/plugins/colibri-page-builder/extend-builder/assets/static/css/theme.css?ver=1.0.182 HTTP/1.1" 304 - "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X1
1; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
81.52.190.240 - - [09/Nov/2020:12:02:06 +0200] "GET /wp-includes/js/wp-emoji-release.min.js?ver=5.3 HTTP/1.1" 304 - "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox
/68.0"
81.52.190.240 - - [09/Nov/2020:12:02:06 +0200] "GET /wp-includes/css/dist/block-library/style.min.css?ver=5.3 HTTP/1.1" 304 - "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/201001
01 Firefox/68.0"
81.52.190.240 - - [09/Nov/2020:12:02:06 +0200] "GET /wp-content/plugins/colibri-page-builder/extend-builder/assets/static/fancybox/jquery.fancybox.min.css?ver=1.0.182 HTTP/1.1" 304 - "https://www.kybereo.ch/kybereo-internal-information
/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
81.52.190.240 - - [09/Nov/2020:12:02:06 +0200] "GET /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1 HTTP/1.1" 304 - "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0"
81.52.190.240 - - [09/Nov/2020:12:02:06 +0200] "GET /wp-includes/js/jquery/jquery.js?ver=1.12.4-wp HTTP/1.1" 304 - "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/
68.0"
81.52.190.240 - - [09/Nov/2020:12:02:06 +0200] "GET /wp-includes/js/imagesloaded.min.js?ver=3.2.0 HTTP/1.1" 304 - "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/6
8.0"
81.52.190.240 - - [09/Nov/2020:12:02:06 +0200] "GET /wp-content/plugins/authorizer/css/authorizer-public.css?ver=2.8.0 HTTP/1.1" 304 - "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gec
ko/20100101 Firefox/68.0"
81.52.190.240 - - [09/Nov/2020:12:02:07 +0200] "GET /wp-includes/js/masonry.min.js?ver=3.3.2 HTTP/1.1" 304 - "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
81.52.190.240 - - [09/Nov/2020:12:02:07 +0200] "GET /wp-content/plugins/colibri-page-builder/extend-builder/assets/static/typed.js?ver=1.0.182 HTTP/1.1" 304 - "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X11; Li
nux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
81.52.190.240 - - [09/Nov/2020:12:02:07 +0200] "GET /wp-content/plugins/colibri-page-builder/extend-builder/assets/static/colibri.js?ver=1.0.182 HTTP/1.1" 304 - "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X11;
Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
81.52.190.240 - - [09/Nov/2020:12:02:07 +0200] "GET /wp-content/plugins/colibri-page-builder/extend-builder/assets/static/fancybox/jquery.fancybox.min.js?ver=1.0.182 HTTP/1.1" 304 - "https://www.kybereo.ch/kybereo-internal-information/
" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
81.52.190.240 - - [09/Nov/2020:12:02:07 +0200] "GET /wp-content/plugins/authorizer/js/authorizer-public.js?ver=2.8.0 HTTP/1.1" 304 - "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko
/20100101 Firefox/68.0"
81.52.190.240 - - [09/Nov/2020:12:02:07 +0200] "GET /wp-content/plugins/colibri-page-builder/extend-builder/assets/static/js/theme.js?ver=1.0.182 HTTP/1.1" 304 - "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X11;
 Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
81.52.190.240 - - [09/Nov/2020:12:02:01 +0200] "GET /kybereo-internal-information/ HTTP/1.1" 200 193913 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
81.52.190.240 - - [09/Nov/2020:12:02:07 +0200] "GET /wp-includes/js/admin-bar.min.js?ver=5.3 HTTP/1.1" 304 - "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
81.52.190.240 - - [09/Nov/2020:12:02:07 +0200] "GET /wp-includes/js/wp-embed.min.js?ver=5.3 HTTP/1.1" 304 - "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
81.52.190.240 - - [09/Nov/2020:12:02:07 +0200] "GET /wp-content/plugins/colibri-page-builder/assets/colibri-logo.png HTTP/1.1" 304 - "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko
/20100101 Firefox/68.0"
81.52.190.240 - - [09/Nov/2020:12:02:07 +0200] "GET /kybereo-internal-information/ HTTP/1.1" 200 162070 "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
81.52.190.240 - - [09/Nov/2020:12:02:32 +0200] "GET /wp-includes/css/admin-bar.min.css?ver=5.3 HTTP/1.1" 200 21375 "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/
68.0"
81.52.190.240 - - [09/Nov/2020:12:02:32 +0200] "GET /wp-includes/js/wp-emoji-release.min.js?ver=5.3 HTTP/1.1" 304 - "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox
/68.0"
81.52.190.240 - - [09/Nov/2020:12:02:32 +0200] "GET /wp-includes/js/jquery/jquery.js?ver=1.12.4-wp HTTP/1.1" 304 - "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/
68.0"
```

Figure 4- Website logs



```
[root@www httpd]# cat ssl_access_log-20250301 | grep kybereo-internal-information | cut -d ' ' -f1 | sort | uniq -c
     17 10.10.100.10
     26 10.10.100.11
      3 185.105.133.21
     72 81.52.190.240
[root@www httpd]# 
```

Figure 5- Website Visitors

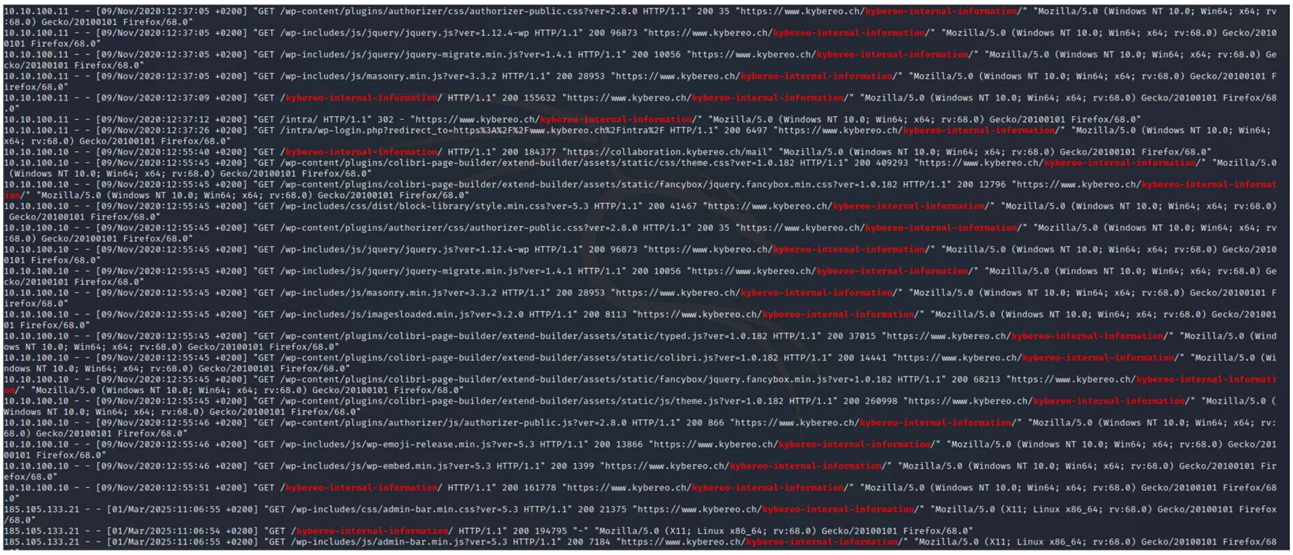
Logs show 4 unique visitors to the site with ip addresses (10.10.100.10, 10.10.100.11, 185.105.133.21, 81.52.198.240).

2.5 How has the attacker carried out his criminal actions?

The logs suggest that someone made attempts to gather information about the website kybereo.ch.

The command **'cat ssl_access_log-20250301 | grep kybereo-internal-information'** shows the attacker was searching for sensitive information that is displayed in the logs.

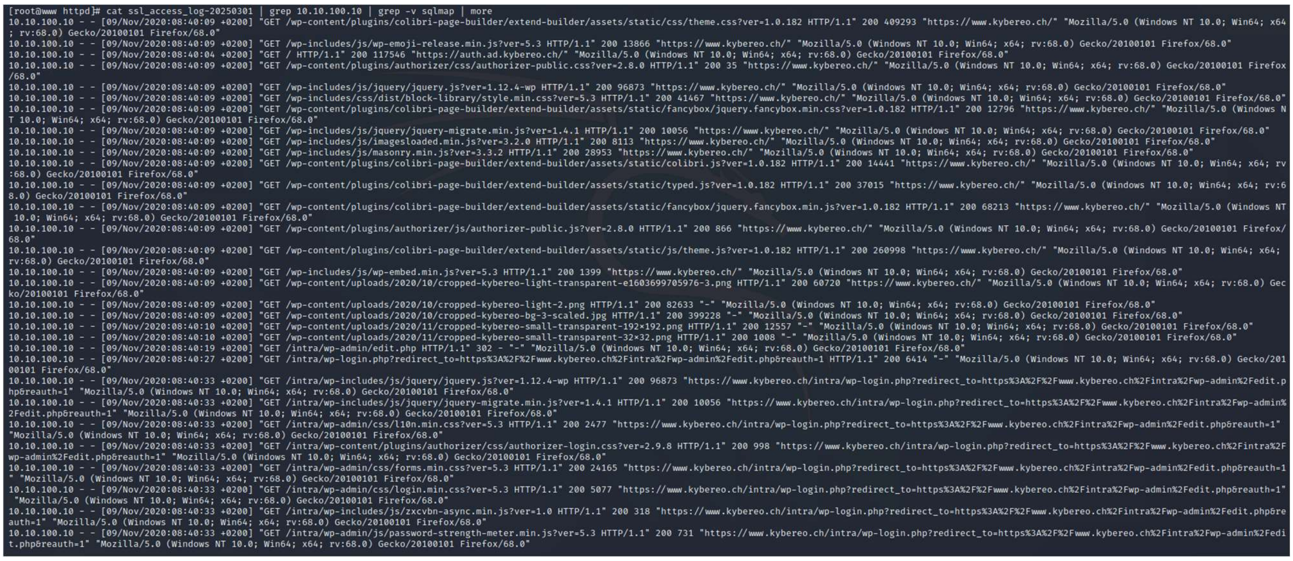
Multiple Ips were able to gain access to this sensitive information but 81.52.190.240 visited about 72 times



```
10.10.100.11 - - [09/Nov/2020:12:37:05 +0200] "GET /wp-content/plugins/authorizer/css/authorizer-public.css?ver=2.8.0 HTTP/1.1" 200 35 "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv
:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.11 - - [09/Nov/2020:12:37:05 +0200] "GET /wp-includes/js/jquery/jquery.js?ver=1.12.4-wp HTTP/1.1" 200 96873 "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/2010
0101 Firefox/68.0"
10.10.100.11 - - [09/Nov/2020:12:37:05 +0200] "GET /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1 HTTP/1.1" 200 10056 "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Ge
cko/20100101 Firefox/68.0"
10.10.100.11 - - [09/Nov/2020:12:37:05 +0200] "GET /wp-includes/js/masonry.min.js?ver=3.3.2 HTTP/1.1" 200 28953 "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 F
irefox/68.0"
10.10.100.11 - - [09/Nov/2020:12:37:09 +0200] "GET /kybereo-internal-information/ HTTP/1.1" 200 155632 "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68
.0"
10.10.100.11 - - [09/Nov/2020:12:37:12 +0200] "GET /intra/ HTTP/1.1" 302 - "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.11 - - [09/Nov/2020:12:37:26 +0200] "GET /intra/wp-login.php?redirect_to=https%3A%2F%2Fwww.kybereo.ch%2Fintra%2F HTTP/1.1" 200 6497 "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (Windows NT 10.0; Win64;
x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:12:55:40 +0200] "GET /kybereo-internal-information/ HTTP/1.1" 200 184377 "https://collaboration.kybereo.ch/mail" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:12:55:45 +0200] "GET /wp-content/plugins/colibri-page-builder/extend-builder/assets/static/css/theme.css?ver=1.0.182 HTTP/1.1" 200 409293 "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0
 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:12:55:45 +0200] "GET /wp-content/plugins/colibri-page-builder/extend-builder/assets/static/fancybox/jquery.fancybox.min.css?ver=1.0.182 HTTP/1.1" 200 12796 "https://www.kybereo.ch/kybereo-internal-informat
ion/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:12:55:45 +0200] "GET /wp-includes/css/dist/block-library/style.min.css?ver=5.3 HTTP/1.1" 200 41467 "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0)
 Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:12:55:45 +0200] "GET /wp-content/plugins/authorizer/css/authorizer-public.css?ver=2.8.0 HTTP/1.1" 200 35 "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv
:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:12:55:45 +0200] "GET /wp-includes/js/jquery/jquery.js?ver=1.12.4-wp HTTP/1.1" 200 96873 "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/2010
0101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:12:55:45 +0200] "GET /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1 HTTP/1.1" 200 10056 "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Ge
cko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:12:55:45 +0200] "GET /wp-includes/js/masonry.min.js?ver=3.3.2 HTTP/1.1" 200 28953 "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 F
irefox/68.0"
10.10.100.10 - - [09/Nov/2020:12:55:45 +0200] "GET /wp-includes/js/imagesloaded.min.js?ver=3.2.0 HTTP/1.1" 200 8113 "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/201001
01 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:12:55:45 +0200] "GET /wp-content/plugins/colibri-page-builder/extend-builder/assets/static/typed.js?ver=1.0.182 HTTP/1.1" 200 37015 "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (Wind
ows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:12:55:45 +0200] "GET /wp-content/plugins/colibri-page-builder/extend-builder/assets/static/colibri.js?ver=1.0.182 HTTP/1.1" 200 14441 "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (Wi
ndows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:12:55:45 +0200] "GET /wp-content/plugins/colibri-page-builder/extend-builder/assets/static/fancybox/jquery.fancybox.min.js?ver=1.0.182 HTTP/1.1" 200 68213 "https://www.kybereo.ch/kybereo-internal-informati
on/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:12:55:45 +0200] "GET /wp-content/plugins/colibri-page-builder/extend-builder/assets/static/js/theme.js?ver=1.0.182 HTTP/1.1" 200 260998 "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (
Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:12:55:46 +0200] "GET /wp-content/plugins/authorizer/js/authorizer-public.js?ver=2.8.0 HTTP/1.1" 200 866 "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:
68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:12:55:46 +0200] "GET /wp-includes/js/wp-emoji-release.min.js?ver=5.3 HTTP/1.1" 200 13866 "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/201
00101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:12:55:46 +0200] "GET /wp-includes/js/wp-embed.min.js?ver=5.3 HTTP/1.1" 200 1399 "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Fir
efox/68.0"
10.10.100.10 - - [09/Nov/2020:12:55:51 +0200] "GET /kybereo-internal-information/ HTTP/1.1" 200 161778 "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68
.0"
185.105.133.21 - - [01/Mar/2025:11:06:55 +0200] "GET /wp-includes/css/admin-bar.min.css?ver=5.3 HTTP/1.1" 200 21375 "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox
/68.0"
185.105.133.21 - - [01/Mar/2025:11:06:54 +0200] "GET /kybereo-internal-information/ HTTP/1.1" 200 194795 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0"
185.105.133.21 - - [01/Mar/2025:11:06:55 +0200] "GET /wp-includes/js/admin-bar.min.js?ver=5.3 HTTP/1.1" 200 7184 "https://www.kybereo.ch/kybereo-internal-information/" "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68
```

Figure 6- Site Logs

2.6 What has enabled the attacker's criminal actions?



```
[root@www httpd]# cat ssl_access_log-20250301 | grep 10.10.100.10 | grep -v sqlmap | more
10.10.100.10 - - [09/Nov/2020:08:40:09 +0200] "GET /wp-content/plugins/colibri-page-builder/extend-builder/assets/static/css/theme.css?ver=1.0.182 HTTP/1.1" 200 409293 "https://www.kybereo.ch/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64
; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:09 +0200] "GET /wp-includes/js/wp-emoji-release.min.js?ver=5.3 HTTP/1.1" 200 13866 "https://www.kybereo.ch/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:04 +0200] "GET / HTTP/1.1" 200 117546 "https://auth.ad.kybereo.ch/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:09 +0200] "GET /wp-content/plugins/authorizer/css/authorizer-public.css?ver=2.8.0 HTTP/1.1" 200 35 "https://www.kybereo.ch/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox
/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:09 +0200] "GET /wp-includes/js/jquery/jquery.js?ver=1.12.4-wp HTTP/1.1" 200 96873 "https://www.kybereo.ch/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:09 +0200] "GET /wp-includes/css/dist/block-library/style.min.css?ver=5.3 HTTP/1.1" 200 41467 "https://www.kybereo.ch/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:09 +0200] "GET /wp-content/plugins/colibri-page-builder/extend-builder/assets/static/fancybox/jquery.fancybox.min.css?ver=1.0.182 HTTP/1.1" 200 12796 "https://www.kybereo.ch/" "Mozilla/5.0 (Windows N
T 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:09 +0200] "GET /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1 HTTP/1.1" 200 10056 "https://www.kybereo.ch/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:09 +0200] "GET /wp-includes/js/imagesloaded.min.js?ver=3.2.0 HTTP/1.1" 200 8113 "https://www.kybereo.ch/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:09 +0200] "GET /wp-includes/js/masonry.min.js?ver=3.3.2 HTTP/1.1" 200 28953 "https://www.kybereo.ch/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:09 +0200] "GET /wp-content/plugins/colibri-page-builder/extend-builder/assets/static/colibri.js?ver=1.0.182 HTTP/1.1" 200 14441 "https://www.kybereo.ch/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv
:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:09 +0200] "GET /wp-content/plugins/colibri-page-builder/extend-builder/assets/static/typed.js?ver=1.0.182 HTTP/1.1" 200 37015 "https://www.kybereo.ch/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:6
8.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:09 +0200] "GET /wp-content/plugins/colibri-page-builder/extend-builder/assets/static/fancybox/jquery.fancybox.min.js?ver=1.0.182 HTTP/1.1" 200 68213 "https://www.kybereo.ch/" "Mozilla/5.0 (Windows NT
 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:09 +0200] "GET /wp-content/plugins/authorizer/js/authorizer-public.js?ver=2.8.0 HTTP/1.1" 200 866 "https://www.kybereo.ch/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/
68.0"
10.10.100.10 - - [09/Nov/2020:08:40:09 +0200] "GET /wp-content/plugins/colibri-page-builder/extend-builder/assets/static/js/theme.js?ver=1.0.182 HTTP/1.1" 200 260998 "https://www.kybereo.ch/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:09 +0200] "GET /wp-includes/js/wp-embed.min.js?ver=5.3 HTTP/1.1" 200 1399 "https://www.kybereo.ch/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:09 +0200] "GET /wp-content/uploads/2020/10/cropped-kybereo-light-transparent-e1603699705976-3.png HTTP/1.1" 200 60720 "https://www.kybereo.ch/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gec
ko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:09 +0200] "GET /wp-content/uploads/2020/10/cropped-kybereo-light-2.png HTTP/1.1" 200 82633 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:09 +0200] "GET /wp-content/uploads/2020/10/cropped-kybereo-bg-3-scaled.jpg HTTP/1.1" 200 399228 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:10 +0200] "GET /wp-content/uploads/2020/11/cropped-kybereo-small-transparent-192×192.png HTTP/1.1" 200 12557 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:10 +0200] "GET /wp-content/uploads/2020/11/cropped-kybereo-small-transparent-32×32.png HTTP/1.1" 200 1008 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:19 +0200] "GET /intra/wp-admin/edit.php HTTP/1.1" 302 - "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:27 +0200] "GET /intra/wp-login.php?redirect_to=https%3A%2F%2Fwww.kybereo.ch%2Fintra%2Fwp-admin%2Fedit.php&reauth=1 HTTP/1.1" 200 6414 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/201
00101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:33 +0200] "GET /intra/wp-includes/js/jquery/jquery.js?ver=1.12.4-wp HTTP/1.1" 200 96873 "https://www.kybereo.ch/intra/wp-login.php?redirect_to=https%3A%2F%2Fwww.kybereo.ch%2Fintra%2Fwp-admin%2Fedit.p
hp&reauth=1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:33 +0200] "GET /intra/wp-includes/js/jquery/jquery-migrate.min.js?ver=1.4.1 HTTP/1.1" 200 10056 "https://www.kybereo.ch/intra/wp-login.php?redirect_to=https%3A%2F%2Fwww.kybereo.ch%2Fintra%2Fwp-admin%
2Fedit.php&reauth=1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:33 +0200] "GET /intra/wp-admin/css/l10n.min.css?ver=5.3 HTTP/1.1" 200 2477 "https://www.kybereo.ch/intra/wp-login.php?redirect_to=https%3A%2F%2Fwww.kybereo.ch%2Fintra%2Fwp-admin%2Fedit.php&reauth=1"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:33 +0200] "GET /intra/wp-content/plugins/authorizer/css/authorizer-login.css?ver=2.9.8 HTTP/1.1" 200 998 "https://www.kybereo.ch/intra/wp-login.php?redirect_to=https%3A%2F%2Fwww.kybereo.ch%2Fintra%2F
wp-admin%2Fedit.php&reauth=1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:33 +0200] "GET /intra/wp-admin/css/forms.min.css?ver=5.3 HTTP/1.1" 200 24165 "https://www.kybereo.ch/intra/wp-login.php?redirect_to=https%3A%2F%2Fwww.kybereo.ch%2Fintra%2Fwp-admin%2Fedit.php&reauth=1
" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:33 +0200] "GET /intra/wp-admin/css/login.min.css?ver=5.3 HTTP/1.1" 200 5077 "https://www.kybereo.ch/intra/wp-login.php?redirect_to=https%3A%2F%2Fwww.kybereo.ch%2Fintra%2Fwp-admin%2Fedit.php&reauth=1"
 "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:33 +0200] "GET /intra/wp-includes/js/zxcvbn-async.min.js?ver=1.0 HTTP/1.1" 200 318 "https://www.kybereo.ch/intra/wp-login.php?redirect_to=https%3A%2F%2Fwww.kybereo.ch%2Fintra%2Fwp-admin%2Fedit.php&re
auth=1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:08:40:33 +0200] "GET /intra/wp-admin/js/password-strength-meter.min.js?ver=5.3 HTTP/1.1" 200 731 "https://www.kybereo.ch/intra/wp-login.php?redirect_to=https%3A%2F%2Fwww.kybereo.ch%2Fintra%2Fwp-admin%2Fedi
t.php&reauth=1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
```

Figure 7- IP 10.10.100.10 logs

The attack was possible due to a **SQL injection vulnerability** in the **Safe Search plugin**. This may have allowed the attacker to interact with the database in unintended ways. Logs from **IP 10.10.100.10** show:

- Multiple requests to **kybereo.ch**, indicating **reconnaissance**.
- Access attempts to **/intra/wp-admin/edit.php** and **/wp-login.php**.
- Interaction with **Colibri Page Builder** and **Authorizer plugins**, which could have been targeted.

2.7 Investigation working path

Examining the Phishing Email

- The investigation started with analysing a phishing email received by an employee.
- I noticed a subtle spelling mistake in the sender’s domain (kybeneo.ch instead of kybereo.ch).
- The email contained urgent language, encouraging the recipient to click a suspicious link.

Examining the suspicious website

- The link led to a phishing site at https://www.kybereo.ch/kybereo-internal-information/ designed to mimic the real kybereo.ch.
- I carefully examined the page and found a fake login form meant to steal usernames and passwords.

Tracking destination of Stolen Data

- I entered test credentials into the phishing page and monitored network traffic.
- The login details were sent to https://www.kyberoo.ch/index.php, confirming the data theft attempt.

Gathering Log Data

- I accessed the web server logs to check for unusual activity.
- Using log filtering, I identified multiple suspicious requests targeting sensitive pages.
- One IP address (10.10.100.10) stood out due to repeated access attempts.

Identifying Reconnaissance Activity

- The attacker's IP was actively scanning the website for weaknesses.
- There were also repeated access attempts to internal resources, suggesting an effort to escalate privileges.

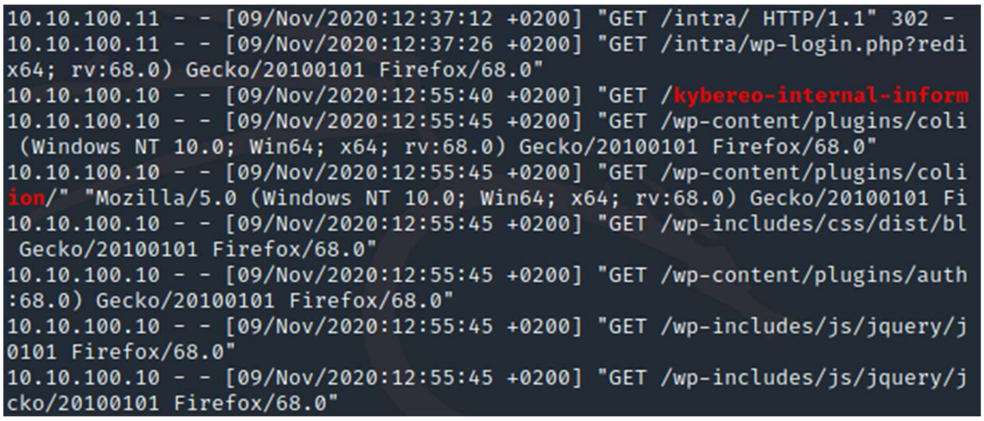
Investigating Security Weaknesses

- I checked which vulnerabilities the attacker may have exploited.
- The Safe Search plugin was found to be vulnerable to SQL injection.
- The Colibri Page Builder plugin had past security flaws that could have been exploited.

Confirming the Attack Path

- The phishing email was meant to trick an employee into entering credentials on a fake login page.
- The stolen credentials would then be used to access the WordPress admin panel.

2.8 Attacker’s modus operandi (Attack path)



```
10.10.100.11 - - [09/Nov/2020:12:37:12 +0200] "GET /intra/ HTTP/1.1" 302 -
10.10.100.11 - - [09/Nov/2020:12:37:26 +0200] "GET /intra/wp-login.php?redi
x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:12:55:40 +0200] "GET /kybereo-internal-inform
10.10.100.10 - - [09/Nov/2020:12:55:45 +0200] "GET /wp-content/plugins/coli
 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:12:55:45 +0200] "GET /wp-content/plugins/coli
ion/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Fi
10.10.100.10 - - [09/Nov/2020:12:55:45 +0200] "GET /wp-includes/css/dist/bl
 Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:12:55:45 +0200] "GET /wp-content/plugins/auth
:68.0) Gecko/20100101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:12:55:45 +0200] "GET /wp-includes/js/jquery/j
0101 Firefox/68.0"
10.10.100.10 - - [09/Nov/2020:12:55:45 +0200] "GET /wp-includes/js/jquery/j
cko/20100101 Firefox/68.0"
```

Figure 8- GET requests

Initial Reconnaissance

The attacker (10.10.100.10) makes multiple GET requests to various WordPress files and directories:

- /wp-includes/js/wp-emoji
- /wp-content/plugins/auth
- /wp-includes/js/jquery/
- /wp-includes/css/dist/
- /wp-content/plugins/coli

These requests indicate reconnaissance, possibly to detect vulnerabilities in plugins or themes.

Requests to Plugin and Upload Directories.

- Multiple requests to /wp-content/plugins/ suggests the attacker identified installed plugins.
- Requests to /wp-content/uploads/2020 indicate probing for file uploads, possibly checks for accessible malicious files or a misconfigured upload directory.

Attempt to Access Admin Panel

- The attacker attempts to access /intra/wp-admin/edit.php, which is an admin page.
- Then, they try to log in using /intra/wp-login.php?redi and multiple other requests related to authentication (wp-admin/css/login, wp-admin/js/password).

Exploitation Attempts

- Access to JavaScript files like /intra/wp-includes/js/zx and /intra/wp-admin/js/password indicate the attacker manipulated scripts related to authentication.
- The frequent access to wp-admin/css/ and wp-content/plugins/ suggests the attacker looked for security flaws in admin themes or outdated plugins.

Security Auditing Perspective

3 Identifying Major Security Threats

While going through the logs and analysing the system, a few things stood out to me as major security concerns:

- **Phishing & Social Engineering** – The whole thing started with a phishing email, and it's clear that if even one user fell for it, attackers could have gotten access to some serious data. This method is still very effective.
- **Default Credentials & Weak Authentication** –The WordPress admin username and password were just "admin: CyberSec4Europe". That's practically an open invitation for attackers. If those credentials aren't changed, anyone with basic knowledge can easily gain access and taken control.
- **Vulnerable WordPress Plugins** – The logs showed multiple requests targeting plugins (/wp-content/plugins/auth and /wp-content/plugins/coli). That's a sign of someone checking for outdated or exploitable plugins.
- **Potential SQL Injection Risks** – If WordPress is not properly secured, SQL injection could be a serious issue. This could let an attacker mess with the database, dump credentials, or even execute commands on the server.

3.1 Critical Vulnerabilities Found (CPE Analysis)

Using CPE analysis, the following vulnerabilities were identified:

- **WordPress**: Outdated WordPress installations was targeted by attacker through plugin vulnerabilities and XML-RPC exploits.
- **SQL**: SQL injection remains a major concern, especially if database queries aren't properly sanitized or if WordPress site had a vulnerable input field that didn't sanitize inputs properly.

4 Visual Representation

4.1 Attack Flow and Investigation Diagram

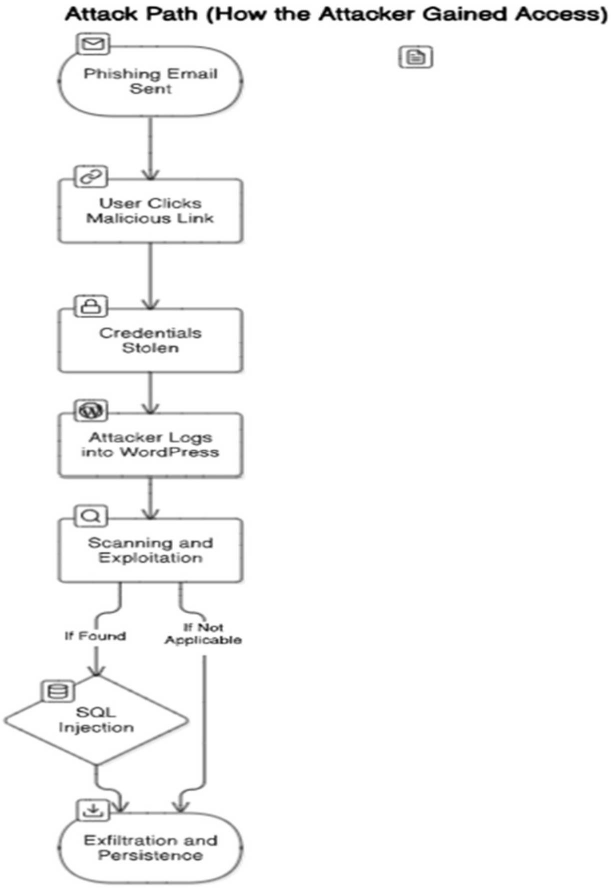

Attack Path (How the Attacker Gained Access)
Phishing Email Sent
User Clicks Malicious Link
Credentials Stolen
Attacker Logs into WordPress
Scanning and Exploitation
If Found
If Not Applicable
SQL Injection
Exfiltration and Persistence

Figure 9- Attack Path

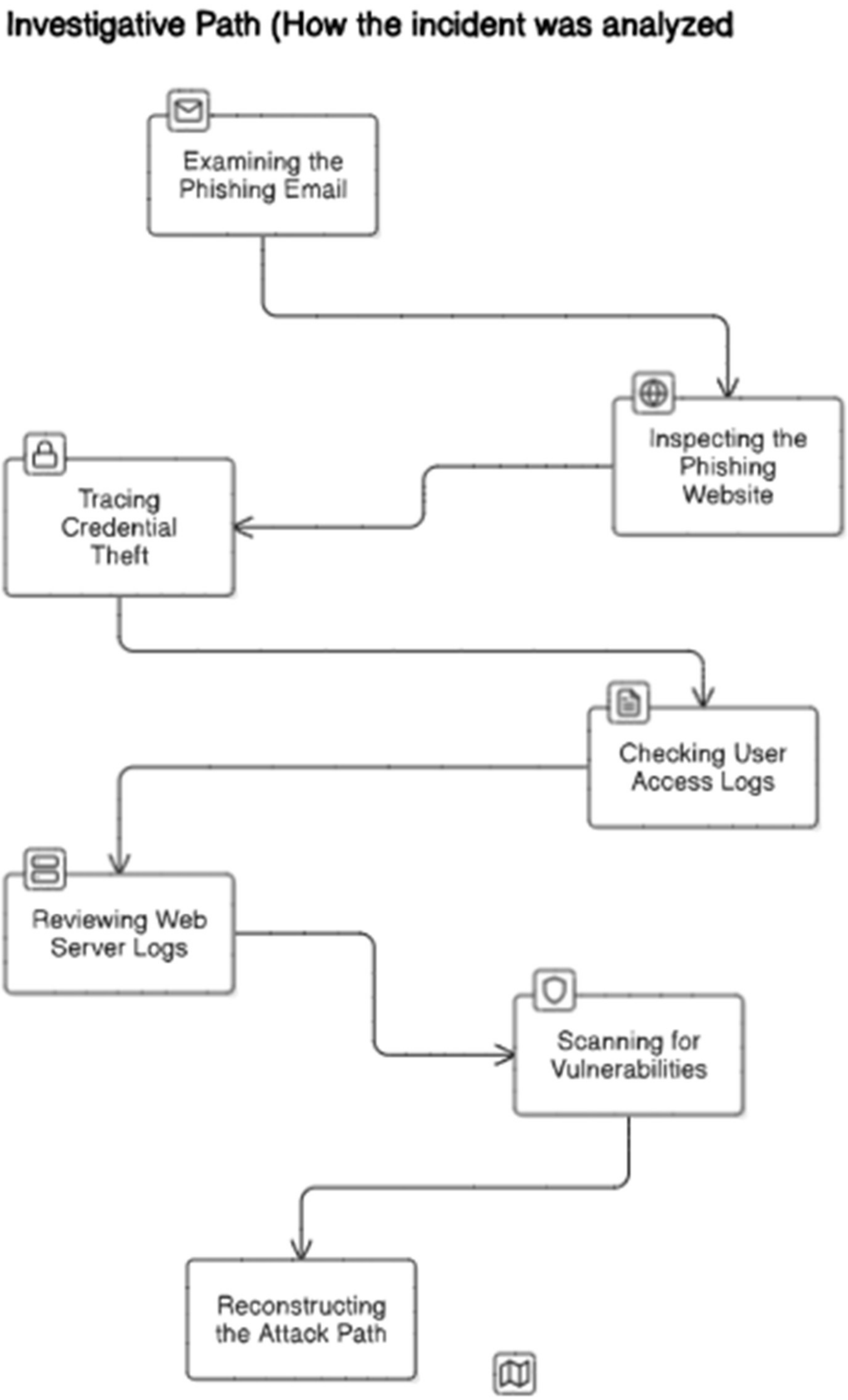

Investigative Path (How the incident was analyzed
Examining the Phishing Email
Inspecting the Phishing Website
Tracing Credential Theft
Checking User Access Logs
Reviewing Web Server Logs
Scanning for Vulnerabilities
Reconstructing the Attack Path

Figure 10- Investigative Path

5 Reflection

This whole investigation is a great reminder of how easy it is for attackers to take advantage of weak spots in a system. Starting from a simple phishing email, it was possible to trace the attack path, see how credentials were stolen, and figure out what the attacker did once inside. It is interesting how something as simple as a fake login page can lead to a much bigger security breach.

One big note is how important user awareness is. If employees aren't trained to recognize phishing emails, even the best security systems won't stop an attack like this. On top of that, we saw how vulnerabilities in WordPress and outdated plugins can open the door for attackers.

From a forensic standpoint, this exercise really showed the value of logs and structured investigation. Being able to piece together an attack from server requests, login attempts, and network activity is important for understanding what happened and preventing it from happening again.

REFERENCES

FIGURE 1- EMAIL SCREENSHOT.

https://cs4e.pages.labranet.jamk.fi/ooc/40-Digital_Forensics/image/Phishingmail.PNG