Incident Report: Suspicious Login Activity and Confirmed Compromise

Date of Report: 20 May 2025
Reported by: [REDACTED]
Affected Domain: `[ORG_DOMAIN][.]com`

Scope and Role

A family member approached me after receiving multiple “successful login” notifications from their work email address over several months. Despite changing their password as a precaution, the notifications continued.

I conducted an independent investigation to identify potential causes and assess risk. This report documents my investigative process, analysis and recommendations, and serves to demonstrate my incident response skills and methodology.

Executive Summary

Between 13-15 May 2025, a series of successful logins occurred from geographically diverse locations. The credentials used appear to be associated with a compromised account tied to `[ORG_DOMAIN][.]com`. Further inspection revealed indications of direct website tampering. Patterns observed suggest potential reconnaissance and credential abuse via exposed administrative information in the website’s source code, and potential access through vulnerabilities within a WordPress plugin or theme. The evidence does not suggest a widespread breach, but further proactive steps are advised to mitigate future risk.

Timeline of Events

	Attempt 1	Attempt 2	Attempt 3
Timestamp	13 May 2025 – 18:36:54 UTC	13 May 2025 – 19:37:15 UTC	15 May 2025 – 10:36:12 UTC
IP	`82[.]XXX[.]XXX[.]83`	`109[.]XXX[.]XXX[.]135`	`82[.]XXX[.]XXX[.]0`
Location	Edinburgh, Scotland, UK	Eyemouth, Scotland, UK	Abererch, Wales, UK
Port Used	61188	46086	23259
ISP Metadata	`dab[.]02[.]net` (O2 mobile data)	`btcentralplus[.]com` (home broadband)	`dab[.]02[.]net` (O2 mobile data)

Indicators and Artifacts

Source Code Discovery:

- Username for a valid email address `[USERNAME][@][ORG_DOMAIN][.]com` appeared in website source code via:

`view-source:hxxps[://][ORG_DOMAIN][.]com/wp-json/oembed/1.0/embed?...`

Public Exposure:

- Email address could also be located via:
    - Google Search
    - Public employer's website (hxxps[://]www[.][REDACTED][.]org)

Suspicious Web Activity:

- Website cache timestamp aligns closely with the first suspicious login.
- robots[.]txt and sitemap XML are accessible and provide full indexing instructions.
- Out of three suspicious login attempts, two source IP addresses have recently been positively identified as a source of spam.
- Evidence has been found of several suspicious published pages alluding to phishing infrastructure.
- Multiple suspicious HTTP requests have been found, targeting the website from abusive IP addresses.
- Evidence of attempted downloads of confidential material has been found.
- Anomalous website referring URLs have been found.
- The [ORG_DOMAIN][.]com shared hosting IP address has previously been listed as a source of spam in 2024.

Analysis:

- There is no evidence that the current credentials were part of a known breach. This suggests either:

(1) Credential harvesting via exposed source code and automated scraping tools, or
(2) Targeted reconnaissance with specific interest in administrative accounts.

- The use of mobile ISPs may indicate attempts to mask origin or leverage dynamic IPs.

- The shared hosting IP address has been specifically targeted by malicious activities, and hasn't been protected against malicious traffic.

- WordPress is known to be a common target for attackers, and has a reputation for vulnerabilities if not properly maintained and protected.

- Without proper security defences and mitigations, ongoing usage of the website to host ephemeral phishing webpages is a significant risk.

Potential Objectives

- **Credential stuffing or Brute-force Attack:** Use of known password wordlists targeting religion-affiliated credentials.
- **Impersonation Risk:** Possibility of using spoofed email addresses for phishing or unauthorized access.
- **Network Pivoting:** Gaining access (eg. to [HOSTING_DOMAIN][.]co[.]uk) via less secure third-party systems to escalate privileges.

- **Hosting Phishing Webpages:** Ephemeral hosting of phishing pages to evade detection and hide infrastructure.

Recommendations:

1. **Notify Affected Parties:**
- Inform BT about potential misuse of IP `109[.]XXX[.]XXX[.]135`.
- Alert `[HOSTING_DOMAIN][.]co[.]uk` of suspicious login activity.

2. **Credential Hygiene:**
- Change all administrative email addresses and passwords on `[ORG_DOMAIN][.]com`.
- Enforce strong password policies and store credentials securely.

3. **Website Hardening:**
- Remove admin contact details from public-facing pages.
- Remove or restrict sitemap access via `robots.txt`.
- Replace author names with aliases.
- Ensure plugins are kept updated and mitigate common vulnerabilities.
- Sanitise and whitelist redirect targets.
- Utilise free security filters, like Cloudflare.

4. **Monitoring & Response:**
- Audit login activity across domains.
- Search for unauthorized credentials or accounts.
- Monitor for further suspicious access or page updates.
- Request `[HOSTING_DOMAIN][.]co[.]uk` support to reassign the IP address and help to mitigate further attacks.

Conclusion

The wide-spread pattern of access and potential sourcing of sensitive data from public code suggest a deliberate attempt to compromise or impersonate administrative functions of `[ORG_DOMAIN][.]com`.
At least one successful attack leading to a direct compromise has been confirmed.
The account should be considered exposed and treated accordingly. I recommend escalation.

Prepared by: Kit S.
Date: 13 June 2025

Incident Write-up: Suspicious Login Activity and Potential Compromise

Attempt 1

13 May 2025 – 18:36:54 UTC

From: **cPanel Login Notification** <cpanel@su[redacted]en.co.uk>
Date: Tue, 13 May 2025, 19:37
Subject: [su[redacted]en.co.uk] ⚠️ Login as ca[redacted]re@su[redacted]er.com from an Unknown Network IP Address 82.[redacted]83
To: <ca[redacted]re@su[redacted]er.com>, <cl[redacted]en@gmail.com>, <cl[redacted]en@outlook.com>

⚠️ Successful Login as "ca[redacted]re@su[redacted]er.com" from an Unknown Network

Domain:	su[redacted]er.com
Service:	dovecot
Local IP Address:	82.[redacted].7
Local Port:	995
Remote IP Address:	82[redacted]83
Remote Port:	61188
Authentication Database:	mail
Username:	ca[redacted]re@su[redacted]er.com
Known Network †:	No ⚠️

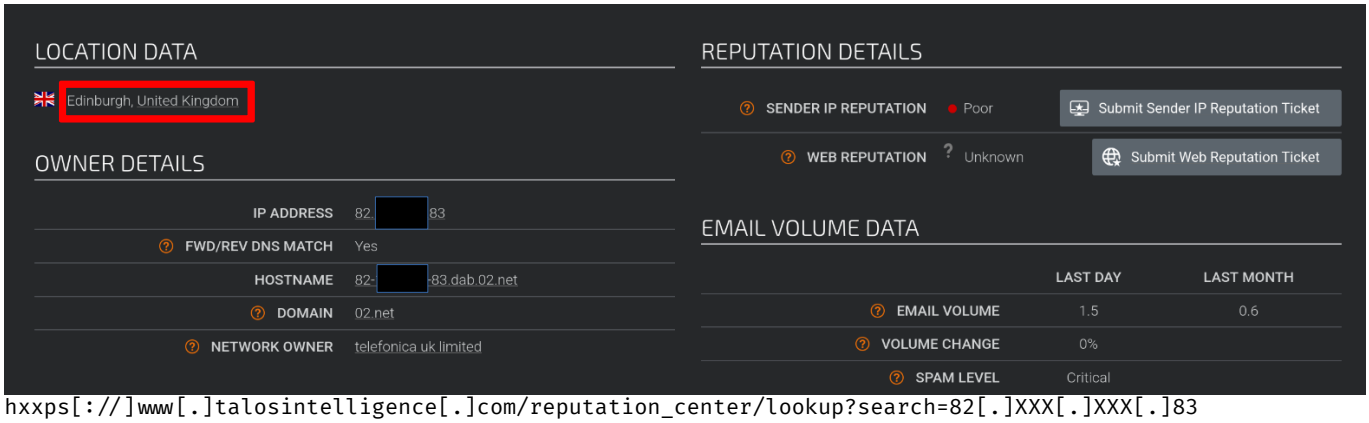
† A "Known Network" is an IP address range or netblock that contains an IP address from which a user successfully logged in previously.

This notice is the result of a request made by a computer with the IP address of "82[redacted]83" through the "dovecot" service on the server.

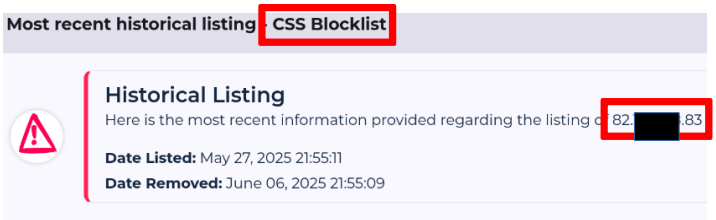
A reverse DNS lookup on the remote IP address returned the host name "82.[redacted]-8[redacted].dab.02.net"
The remote computer's location appears to be: United Kingdom (GB).
The remote computer's IP address is assigned to the provider "O2 Online (uk) O2 Online (UK)"
The system generated this notice on Tuesday, May 13, 2025 at 6:36:54 PM UTC.

You can disable the "cPHulkd Login Notifications" type of notification through the cPanel Webmail interface:
https://su[redacted]en.co.uk:2096/webmail/jupiter/contact/index.html

Do not reply to this automated message.



hxxps[://]www[.]talosintelligence[.]com/reputation_center/lookup?search=82[.]XXX[.]XXX[.]83



hxxps[://]check[.]spamhaus[.]org/

- Successful login from Edinburgh, Scotland, UK.
- `dab[.]02[.]net` is associated with O2's mobile data network.
- Has since been identified as a potential source of spam by Combined Spam Sources.

Attempt 2
13 May 2025 – 19:37:15 UTC

From: **cPanel Login Notification** <cpanel@su[redacted]en.co.uk>
Date: Tue, 13 May 2025, 20:37
Subject: [su[redacted]en.co.uk] ⚠ Login as ca[redacted]re@su[redacted]er.com from an Unknown Network IP Address 109.[redacted].135
To: <ca[redacted]re@su[redacted]er.com>, <cl[redacted]en@gmail.com>, <c[redacted]en@outlook.com>

⚠ Successful Login as "ca[redacted]re@su[redacted]er.com" from an Unknown Network

Domain:	su[redacted]er.com
Service:	dovecot
Local IP Address:	82.[redacted].7
Local Port:	993
Remote IP Address:	109[redacted].135
Remote Port:	46806
Authentication Database:	mail
Username:	ca[redacted]re@su[redacted]er.com
Known Network †:	No ⚠

† A "Known Network" is an IP address range or netblock that contains an IP address from which a user successfully logged in previously.

This notice is the result of a request made by a computer with the IP address of "109.[redacted]135" through the "dovecot" service on the server.

A reverse DNS lookup on the remote IP address returned the host name "host109-[redacted]-135.range109-15[redacted].btcentralplus.com".

The remote computer's location appears to be: United Kingdom (GB).

The remote computer's IP address is assigned to the provider: "IP Pools BT Public Internet Service"

The provider supplied the following remarks about the IP address allocation: "Please send abuse notification to abuse@bt.net"

The system generated this notice on Tuesday, May 13, 2025 a[redacted]7:37:15 PM UTC.

You can disable the "cPHulkd Login Notifications" type of notification through the cPanel Webmail interface:
https://su[redacted]er.myzen.co.uk:2096/webmail/jupiter/contact/index.html

Do not reply to this automated message.

LOCATION DATA

Eyemouth, United Kingdom

OWNER DETAILS

IP ADDRESS	109[redacted]135
FWD/REV DNS MATCH	Yes
HOSTNAME	-
DOMAIN	-
NETWORK OWNER	british telecommunications plc

REPUTATION DETAILS

SENDER IP REPUTATION	Poor	Submit Sender IP Reputation Ticket
WEB REPUTATION	Unknown	Submit Web Reputation Ticket

EMAIL VOLUME DATA

	LAST DAY	LAST MONTH
EMAIL VOLUME	0.0	0.0
VOLUME CHANGE	0%	
SPAM LEVEL	Critical	

`hxxps[://]www[.]talosintelligence[.]com/reputation_center/lookup?search=109[.]XXX[.]XXX[.]135`

- Successful login from Eyemouth, Scotland, UK
- `btcentralplus[.]com` primarily serves home broadband users.

Attempt 3
15 May 2025 – 10:36:12 UTC

From: **cPanel Login Notification** <cpanel@su[redacted]en.co.uk>
Date: Thu, 15 May 2025, 11:36
Subject: [su[redacted]en.co.uk] ⚠️ Login as ca[redacted]re@su[redacted]er.com from an Unknown Network IP Address 82.[redacted].0
To: <ca[redacted]re@su[redacted]er.com>, <cl[redacted]en@gmail.com>, <c[redacted]en@outlook.com>

⚠️ Successful Login as "ca[redacted]re@su[redacted]er.com" from an Unknown Network

Domain:	su[redacted]er.com
Service:	dovecot
Local IP Address:	82.[redacted].7
Local Port:	995
Remote IP Address:	82.[redacted].0
Remote Port:	23259
Authentication Database:	mail
Username:	ca[redacted]re@su[redacted]er.com
Known Network †:	No ⚠️

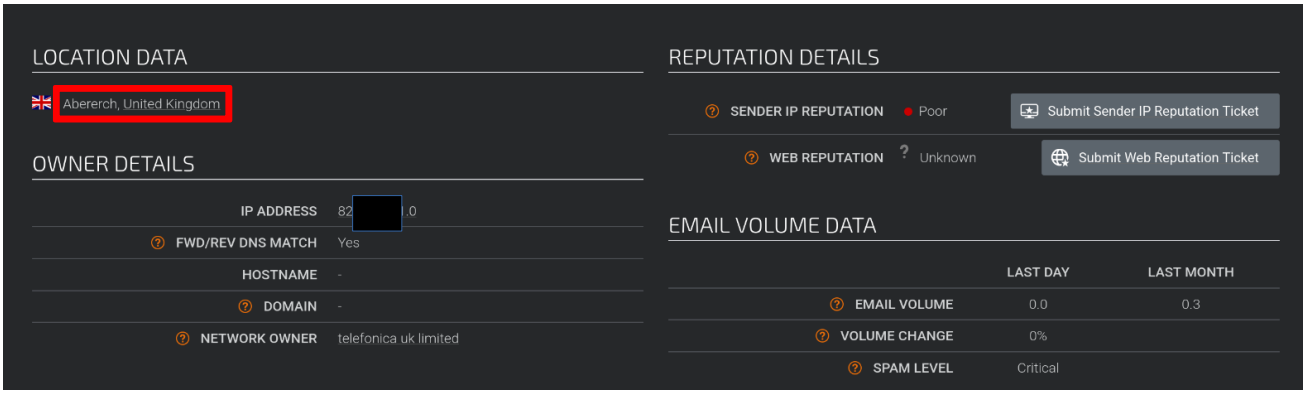
† A "Known Network" is an IP address range or netblock that contains an IP address from which a user successfully logged in previously.

This notice is the result of a request made by a computer with the IP address of "82.[redacted].0" through the "dovecot" service on the server.

A reverse DNS lookup on the remote IP address returned the host name "82-[redacted]dab.02.net"
The remote computer's location appears to be: United Kingdom (GB).
The remote computer's IP address is assigned to the provider: "02 Online (uk) O2 Online (UK)"
The system generated this notice on Thursday, May 15, 2025 at 10:36:12 AM UTC.

You can disable the "cPHulkd Login Notifications" type of notification through the cPanel Webmail interface:
https://su[redacted]er.myzen.co.uk:2096/webmail/jupiter/contact/index.html

Do not reply to this automated message.

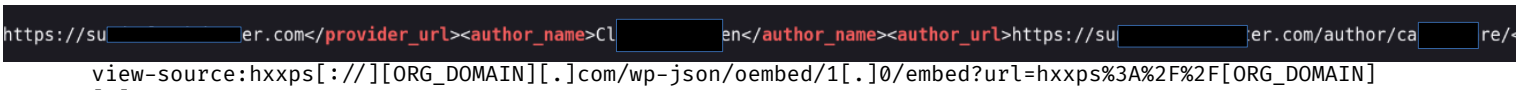


`hxxps[://]www[.]talosintelligence[.]com/reputation_center/lookup?search=82[.]XXX[.]XXX[.]0`

hxxps[://]check[.]spamhaus[.]org/

- Successful login from Abererch, Wales, UK.
- `dab[.]02[.]net` is associated with O2's mobile data network.
- Has since been identified as a potential source of spam by Combined Spam Sources.

Information found in source code of the website:



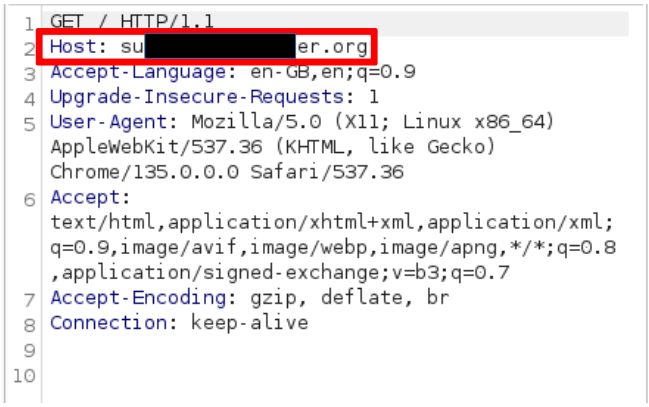
view-source:hxxps[://][ORG_DOMAIN][.]com/wp-json/oembed/1[.]0/embed?url=hxxps%3A%2F%2F[ORG_DOMAIN][.]com%2F&format=xml

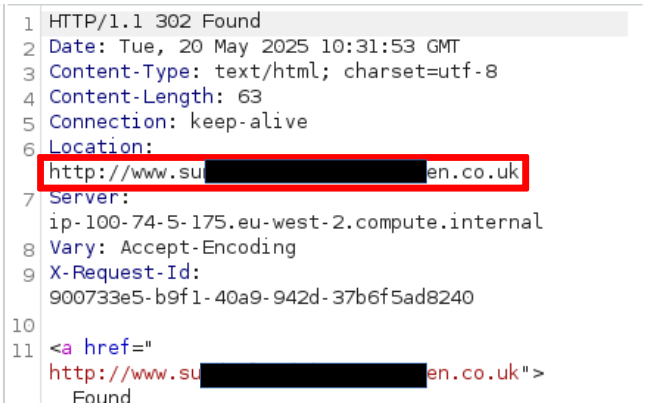
Information found on public-facing website pages:

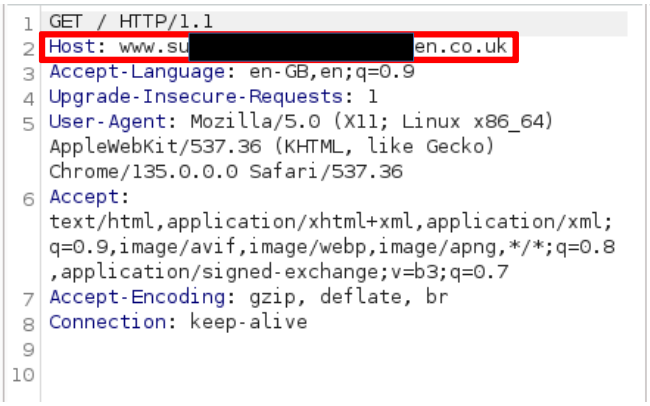
hxxps[://][ORG_DOMAIN][.]com/contact-us/#

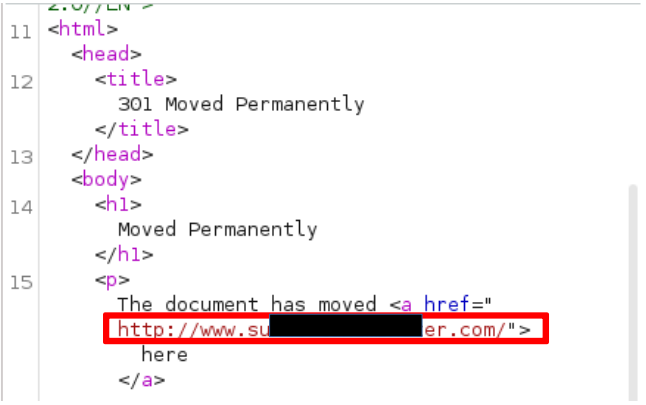
Information found using Burpsuite:

Attempting to view `[ORG_DOMAIN][.]org` leads to multiple redirects:



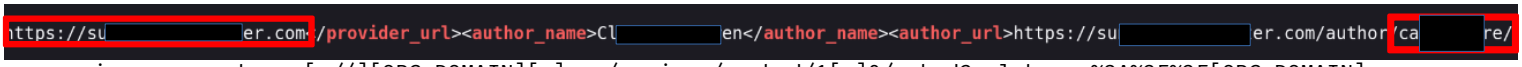




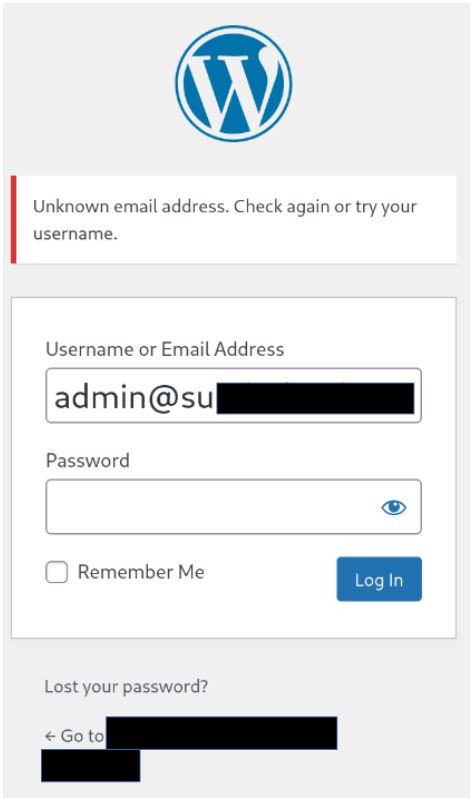


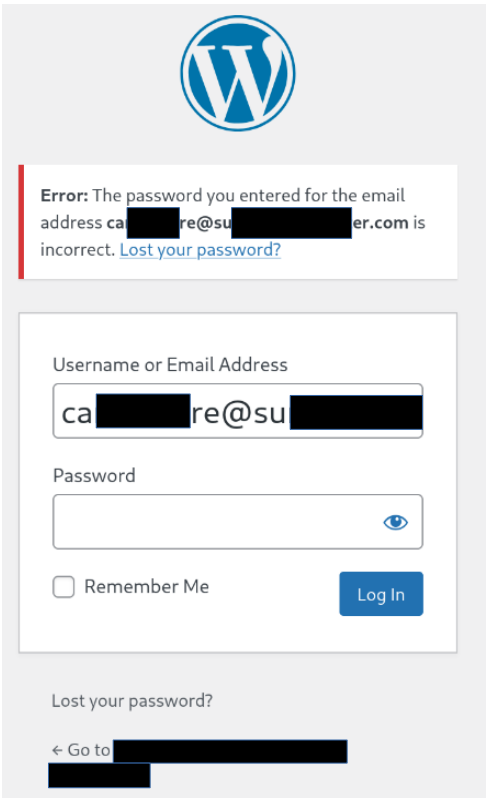
Proof of concept:

- Attempting to log in to `www[.][ORG_DOMAIN][.]com` with the admin credentials supplied shows the email address `admin[@][ORG_DOMAIN][.]org` or the variation – `admin[@][ORG_DOMAIN].com` – isn't valid, but our `[USERNAME]` can be combined with `[ORG_DOMAIN][.]com` and create a valid login address.



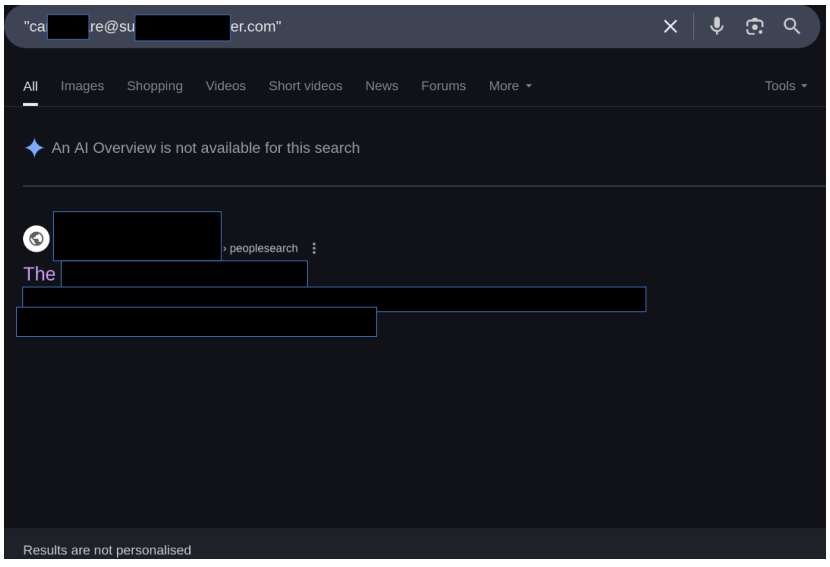
`view-source:hxxps[://][ORG_DOMAIN][.]com/wp-json/oembed/1[.]0/embed?url=hxxps%3A%2F%2F[ORG_DOMAIN][.]com%2F&format=xml`



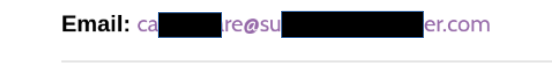


`hxxps[://][ORG_DOMAIN][.]com/wp-login[.]php`

- The only other way of finding this email address would be to use Google:



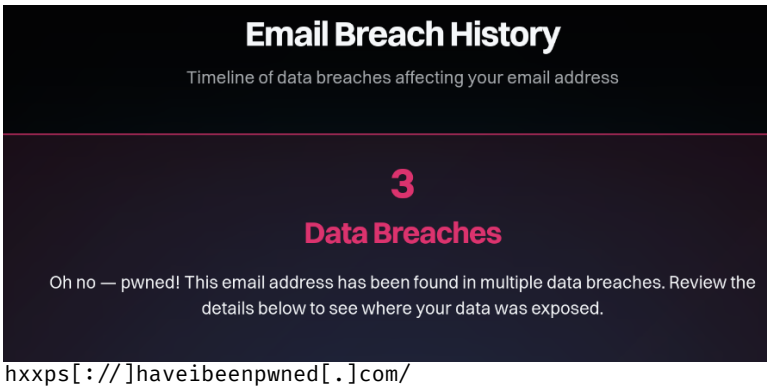
Or the [REDACTED] website:



`hxxps[://]www[.][REDACTED][.]org/peoplesearch/323732`

Both of these options seem targeted and personal, and there is no public evidence that this email address has been involved in a credential leak. This leads me to assume the information has been gained from the source code, rather than gained by a search specific to one person.

There is evidence to show that the old email address `admin[@][ORG_DOMAIN][.]org` has been breached three times – once in 2017, once in 2019, and once in 2021. This potentially provides a historical link.



`hxxps[://]haveibeenpwned[.]com/`

Web Crawlers:

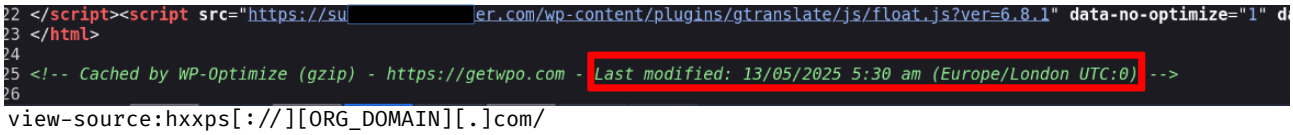
Some malicious bots will systematically browse and index the content of websites across the internet, scanning source codes and using the information from one website to log into another. They can then brute-force the password using wordlists (a collection of known passwords that have been previously leaked online).

Unfortunately, it isn't too difficult to brute-force a correct password (unless it's extremely complicated and/or not worth the time it would take to do so). There are also wordlists that target [REDACTED] specifically.

Without access to login logs, it's impossible to validate whether brute-force occurred – however, as the credentials have already been changed once before by the authorized user, it does seem likely.

Suspicious artifacts:

As part of this investigation, I am looking for suspicious artifacts that have been left by an attacker, to validate how much disruption has potentially been caused. This artifact could be coincidental and not an Indicator of Compromise (IOC) however, viewing the source code (viewed 20/05/2025) of the main web page shows it was last cached 13 hours before our first recorded email.



`view-source:hxxps[://][ORG_DOMAIN][.]com/`

This could be the result of a scheduled cache refresh, it could be the timestamp of the first visit to the website since the page's cache expired or had been cleared, or it could be that the web page content was modified legitimately – or illegitimately.

I don't have access to any earlier emails yet, although I'm aware they exist, and I also don't have any back-end access to any logs or login credentials, but I do have access to the website's sitemap XML.

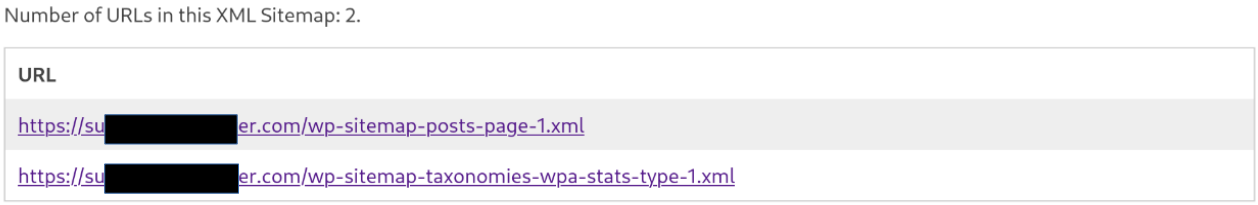
Explanation:

- Following the sitemap leads us to a completely innocuous update to the website's "What's On" page, updated at 6:30:26 am BST – ie. 5:30 am UTC. This matches the timestamp of the potential IOC, indicating a false positive.

(1)

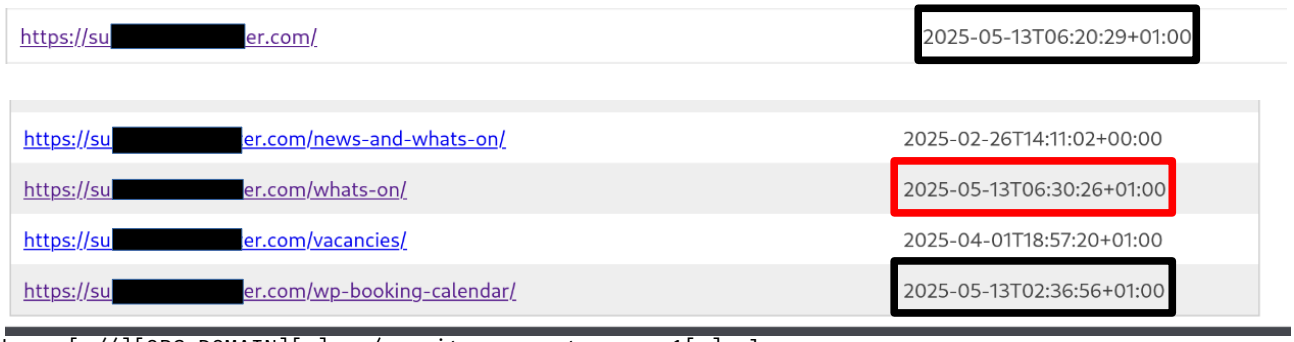
hxxps[://][ORG_DOMAIN][.]com/robots[.]txt

(2)



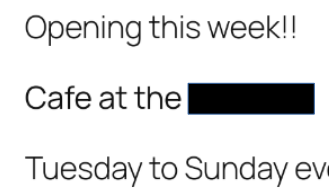
hxxps[://][ORG_DOMAIN][.]com/wp-sitemap[.]xml

(3)



hxxps[://][ORG_DOMAIN][.]com/wp-sitemap-posts-page-1[.]xml

(4)



hxxps[://][ORG_DOMAIN][.]com/whats-on/

WordPress Admin Site

On the 6th and 7th of June, I was given authorised access to the WordPress admin site. Here, I found evidence of ephemeral hosting via compromised infrastructure.

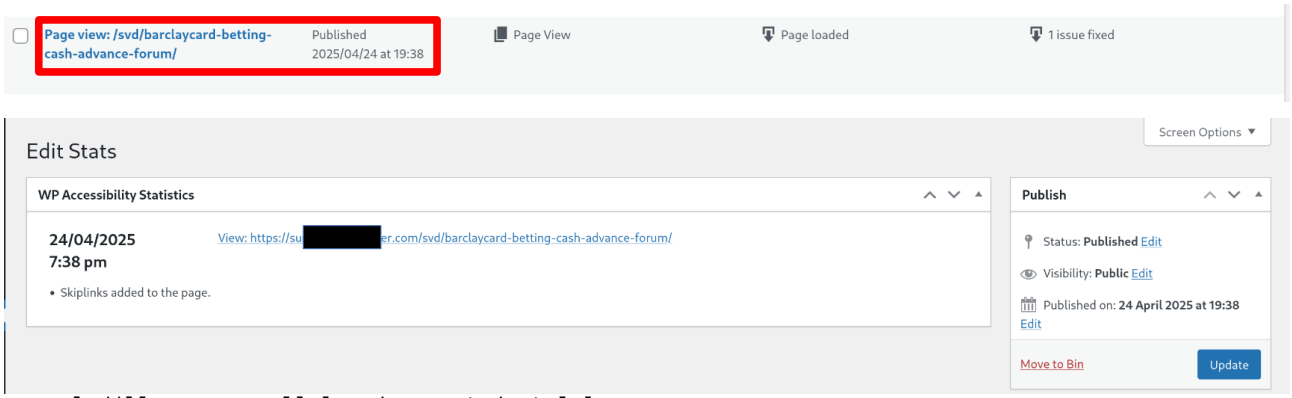
To gain some insight into any suspicious activity, I first looked at the “WP Accessibility Statistics” section of the website (`hxxps[://][ORG_DOMAIN][.]com/wp-admin/edit[.]php?post_type=wpa-stats`).

This is a WordPress plugin normally used to assess the overall accessibility of a WordPress site and guide efforts to make it more inclusive. This information is currently only collected when a user with administrative privileges browses the site, and statistics aren’t tied to specific users; they only collect the manipulations that “WP Accessibility” has performed on that page.

Suspicious Published Pages:

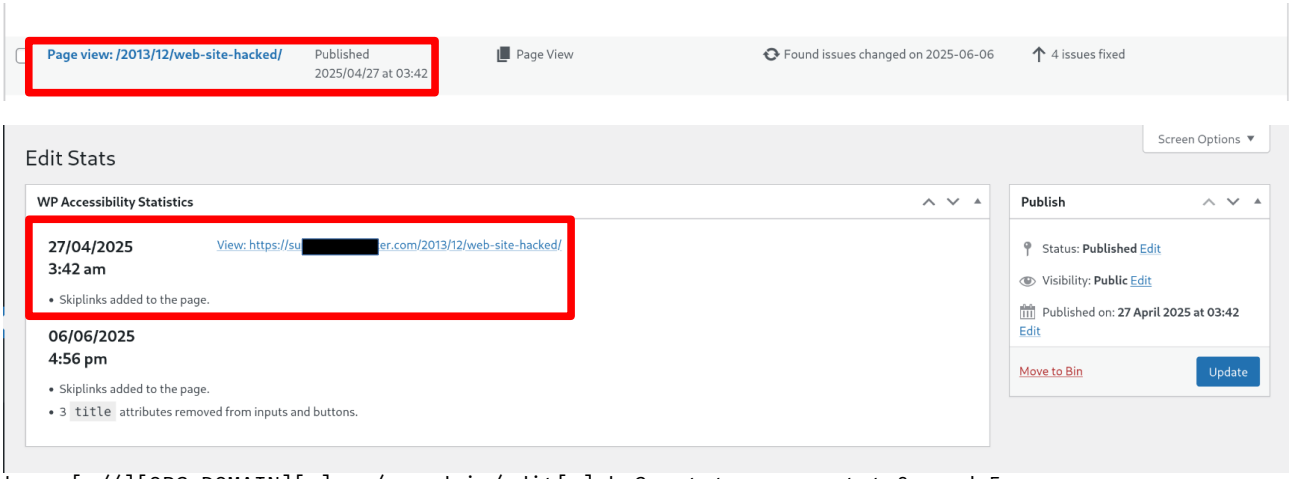
Viewing these statistics showed multiple suspicious, published pages that were either no longer available, or were publicly accessible – when they shouldn’t be.

(1)



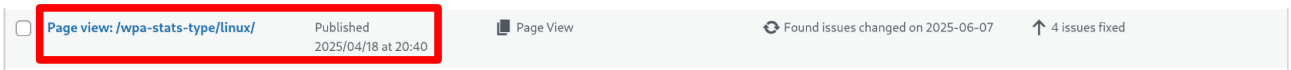
`hxxps[://][ORG_DOMAIN][.]com/wp-admin/edit[.]php?post_type=wpa-stats&paged=6`

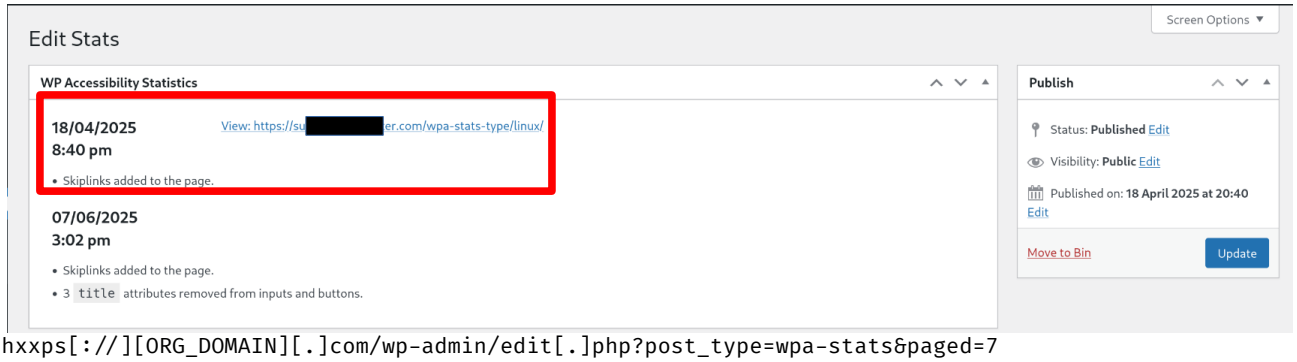
(2)



`hxxps[://][ORG_DOMAIN][.]com/wp-admin/edit[.]php?post_type=wpa-stats&paged=5`

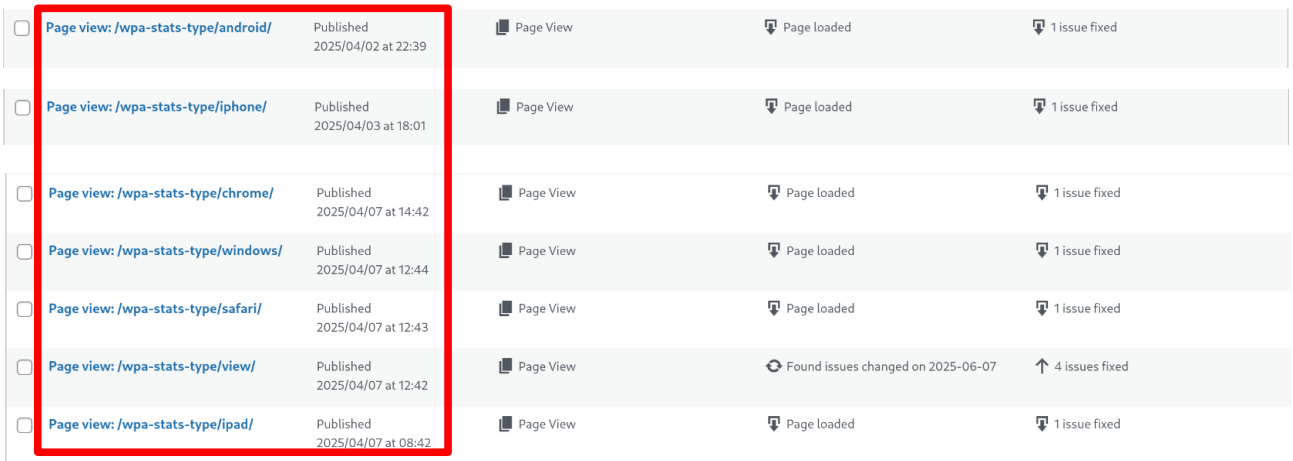
(3)





hxxps[://][ORG_DOMAIN][.]com/wp-admin/edit[.]php?post_type=wpa-stats&paged=7

(4)



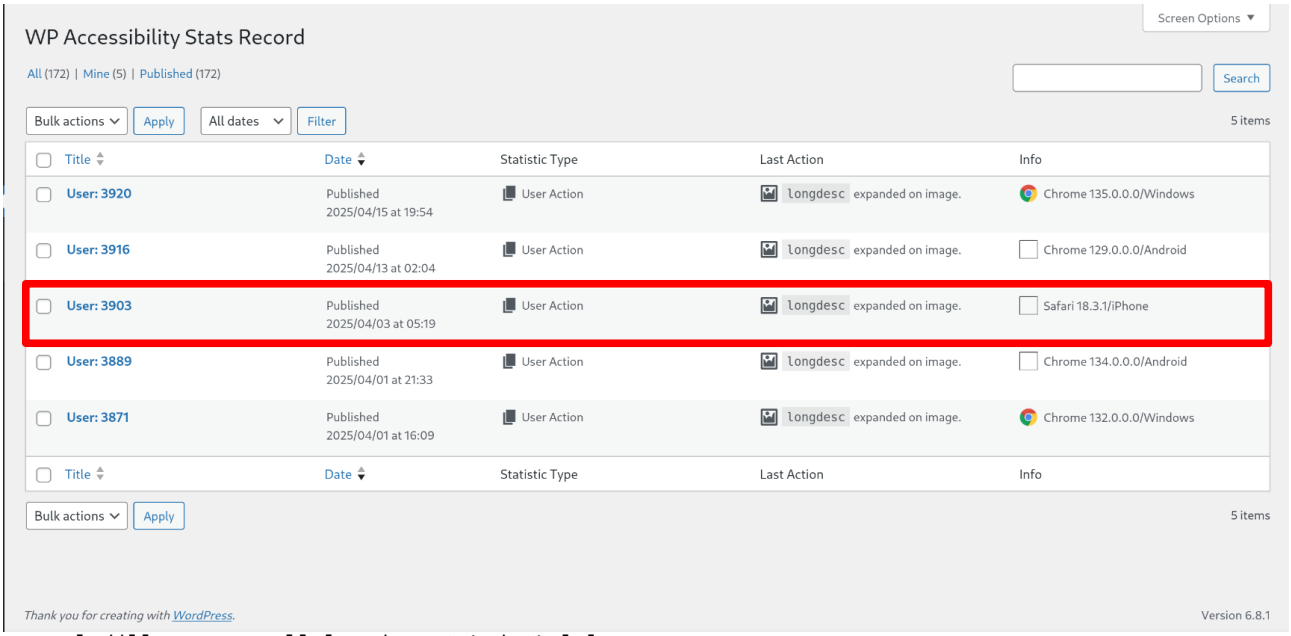
hxxps[://][ORG_DOMAIN][.]com/wp-admin/edit[.]php?post_type=wpa-stats&paged=8

Please note: The entries regarding the 6th and 7th June 2025 are my page views, before I logged out of the admin page. I have therefore highlighted the entries of concern.

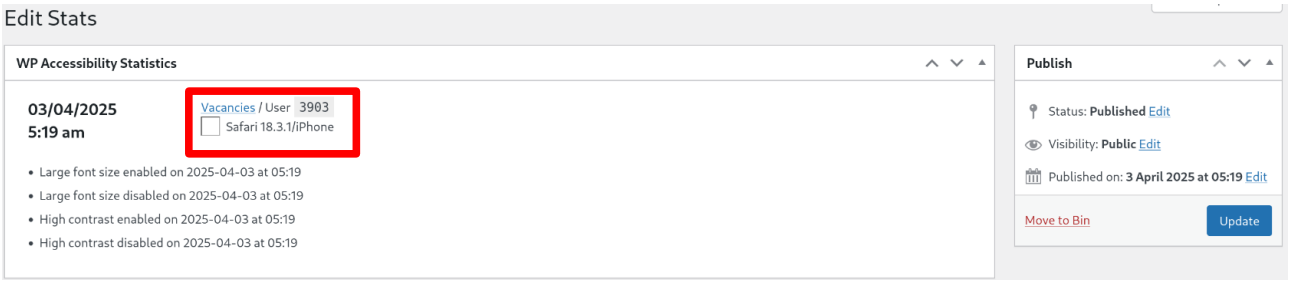
Suspicious User Activity:

I also found suspicious user activity where the users seem to have since been deleted. However, without matching logs or entries outside this plugin report, it may be a false positive or plugin misinterpretation – therefore a cross-check is needed.

I can confirm however, that there was no authorised user action concerning Safari on an iPhone in April 2025:

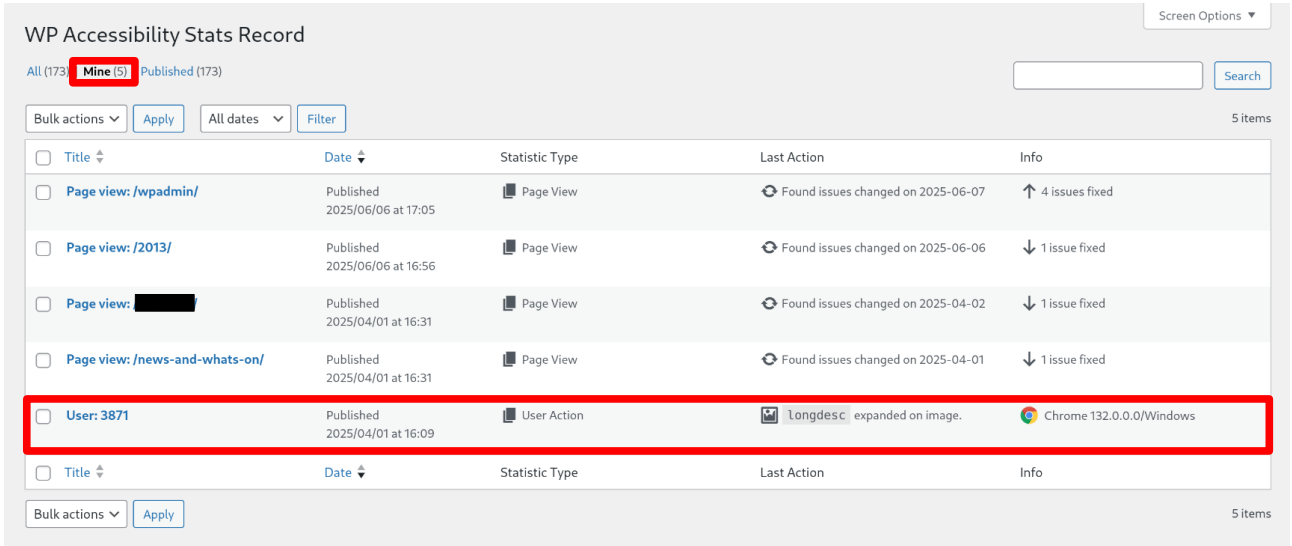


hxxps[://][ORG_DOMAIN][.]com/wp-admin/edit[.]php?post_type=wpa-stats&wpa-stats-type=event



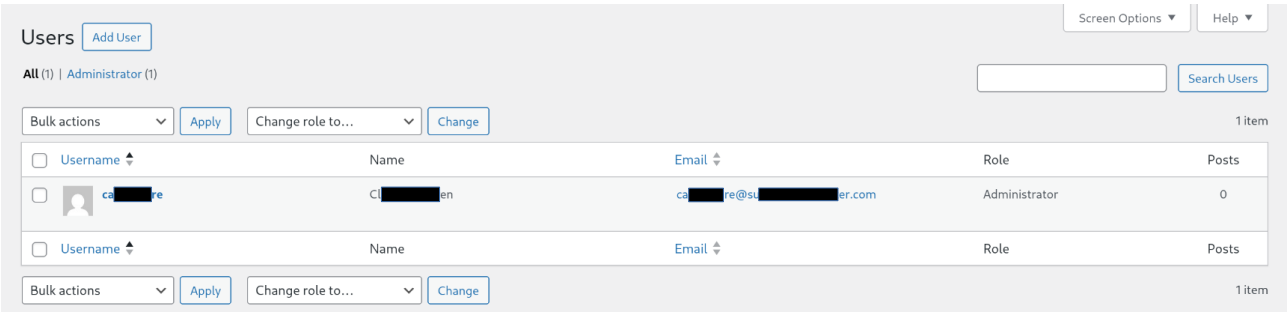
hxxps[://][ORG_DOMAIN][.]com/wp-admin/post[.]php?post=3903&action=edit

Furthermore, when viewing the “WP Accessibility Stats Record” filtered to only show “Mine”, the result suggests that the authorised admin account, `[USERNAME]`, should be `User:3871`, but not any of the other four user accounts shown previously. This potentially suggests that the attacker compromised the `[USERNAME]` admin account and then proceeded to create further user accounts in an attempt to avoid detection.



hxxps[://][ORG_DOMAIN][.]com/wp-admin/edit[.]php?post_type=wpa-stats&author=2

The current list of “Users” shows only one user – [USERNAME].



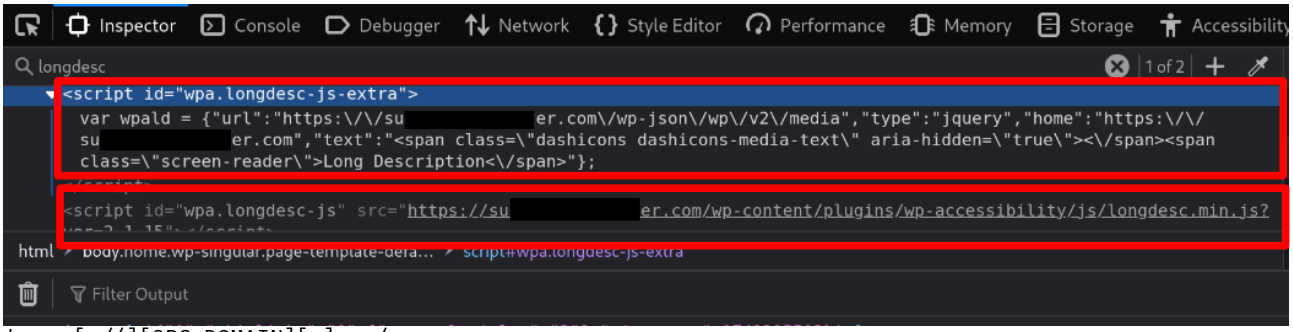
hxxps[://][ORG_DOMAIN][.]com/wp-admin/users[.]php

- It should be noted that [USERNAME] is classed as author=2 (see the previous post_type URL above) as the website was inherited from a former colleague who had been an administrator, and was therefore author=1.

Each “User Action” listed (hxxps[://][ORG_DOMAIN][.]com/wp-admin/edit[.]php?post_type=wpa-stats&wpa-stats-type=event), referred to “longdesc expanded on image.”

longdesc is a deprecated HTML attribute, used to allow authors to provide a URL to a detailed description of an image. It tends to be used for accessibility purposes eg. for screen readers etc. These could be genuine interactions, however, longdesc can also be used to obfuscate malicious links.

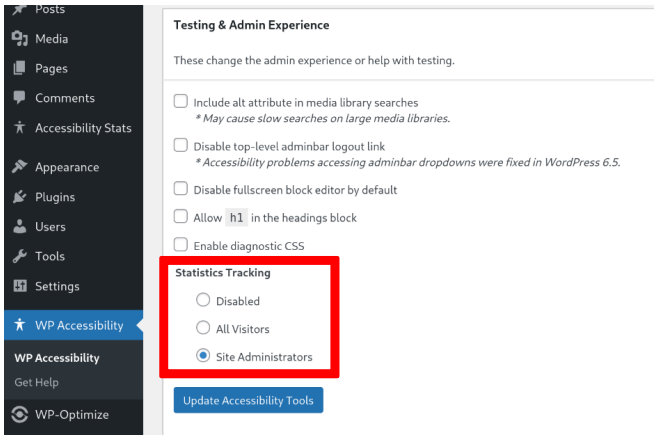
The longdesc attributes on the “Welcome” and “Vacancies” pages as they are now, appear to be usual.



hxxps[://][ORG_DOMAIN][.]com/

Unusual Devices:

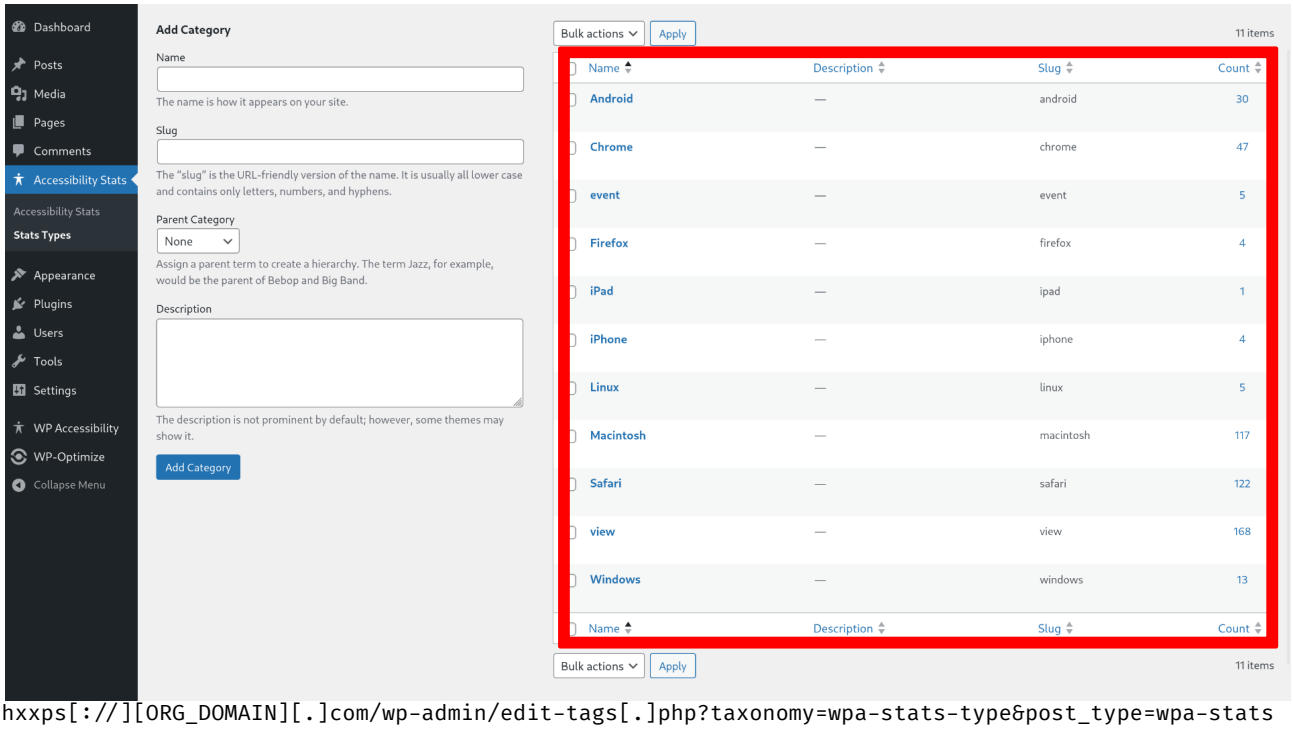
Reviewing the “Accessibility Stats” by type shows all categories but “iPad” have had multiple objects assigned to them, some significant (see “Macintosh” and “Safari”). Our “Accessibility Stats” only record the actions of an administrative user, and we have confirmed that there are no Apple products currently in use.



hxxps[://][ORG_DOMAIN][.]com/wp-admin/admin[.]php?page=wp-accessibility

This record suggests that the “WP Accessibility” plugin has recorded what OS/devices were used by site administrators.

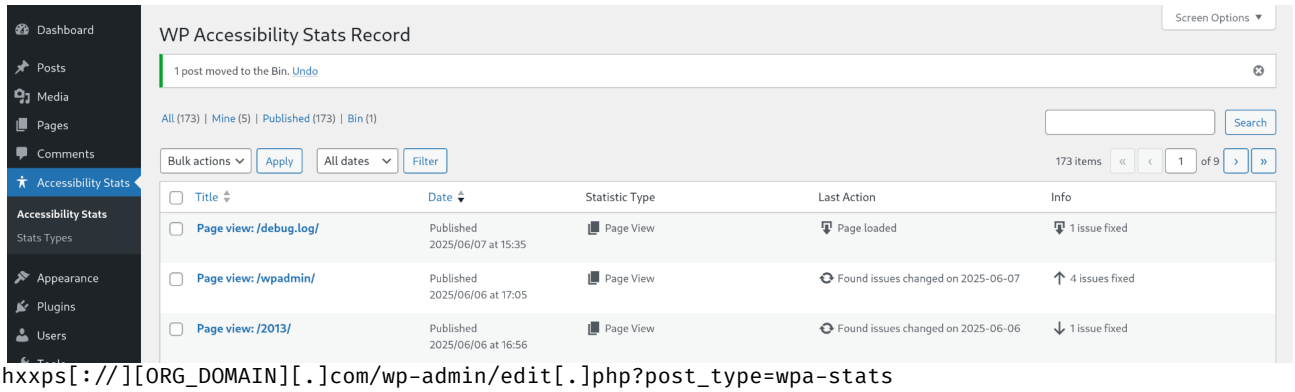
This is suspicious, as there is currently only one authorised administrator, and they don’t use Safari, Macintosh, Linux, iPhone, iPad or Firefox. One issue that should be considered however, is that there isn’t a time frame for this record. These results may be showing the full history of the website, including the activities of the previous administrator.



hxxps[://][ORG_DOMAIN][.]com/wp-admin/edit-tags[.]php?taxonomy=wpa-stats-type&post_type=wpa-stats

Deleting Evidence:

Lastly, I moved one of my “Page View” records to the “Bin” to observe what would be expected to happen, and a new filter was added called “Bin”. The next day, the “Bin” filter was no longer there, and there was no record of that “Page View”. This suggests that evidence could easily be deleted in an attempt to successfully evade detection, and that an attacker may have mistakenly left some artifacts behind.



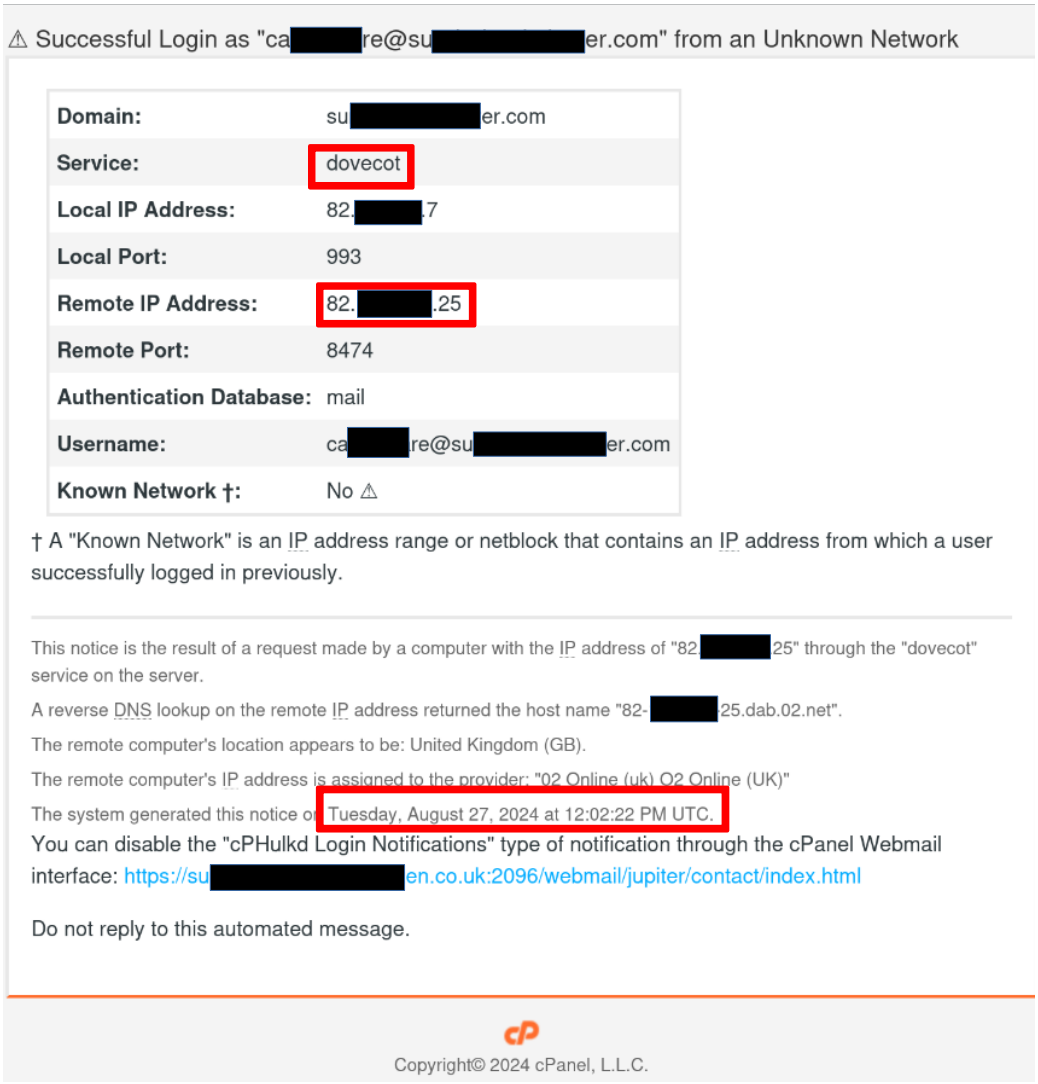
hxxps[://][ORG_DOMAIN][.]com/wp-admin/edit[.]php?post_type=wpa-stats

Observing these artifacts suggests that the website has been probed for vulnerabilities, subsequently breached and used to create short-lived, potentially malicious phishing pages. It also seems that attempts to clean up after use have been made.

cPanel WebMail Interface

On the 9th of June, I was granted access to the “cPanel WebMail” interface (`hxxps[://][ORG_DOMAIN][.]com:2096/cpsess2516470662/webmail/jupiter/index[.]html?mailclient=none`).

To begin, I start looking through the “WebMail” inbox for any suspicious emails, and I find that these suspicious emails, specifically for the user account `[USERNAME]`, have been recurring since August 2024.



The source IP address for this first email has also been identified as a potential source of spam by Combined Spam Sources.

`hxxps[://]check[.]spamhaus[.]org/`

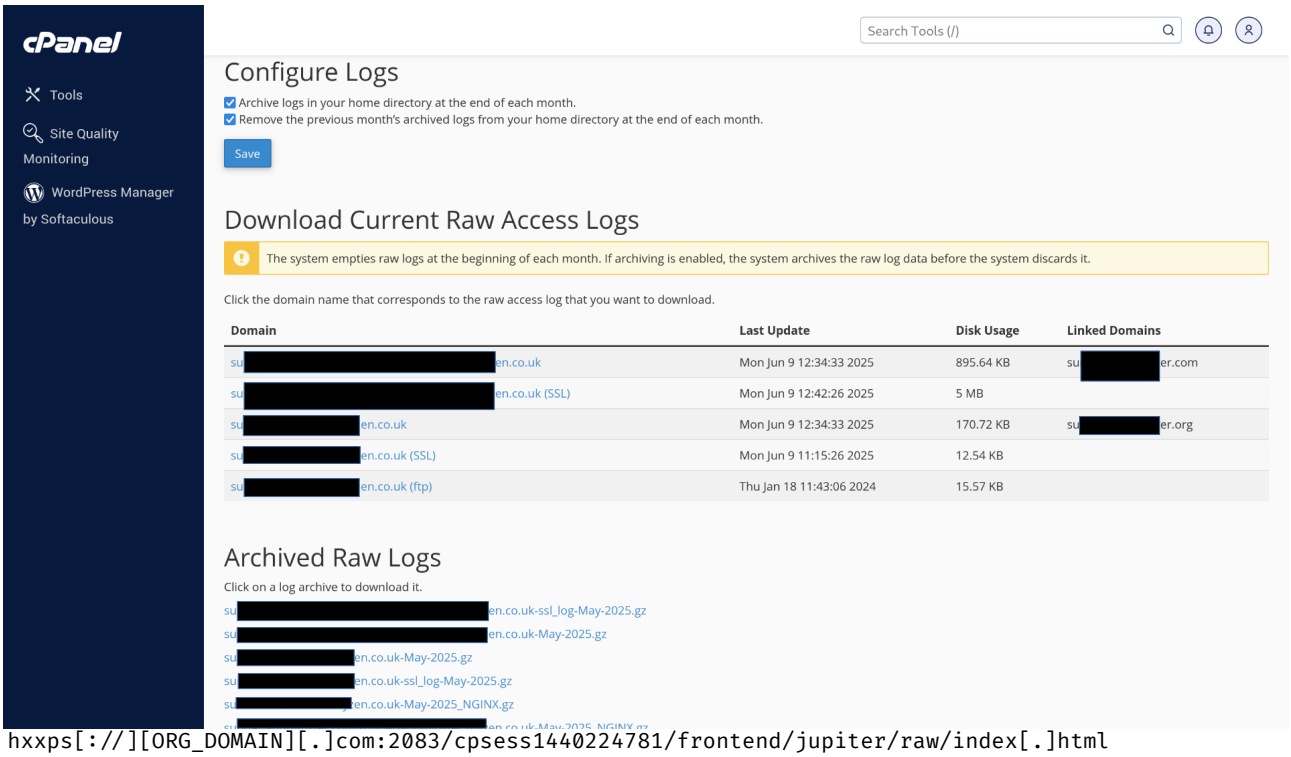
cPanel Control Panel

The credentials I was given to log into the “cPanel Control Panel” account weren’t allowing anyone access, but by looking through the email “Track Delivery”, I was able to obtain the username. I then submitted a password change request to the work email I had access to and was able to log in to the “cPanel Control Panel”.

I attempted to check for further evidence, correlate my findings and view the WordPress database and logs.

Raw Access Logs

I immediately went to access the Raw Access Logs.

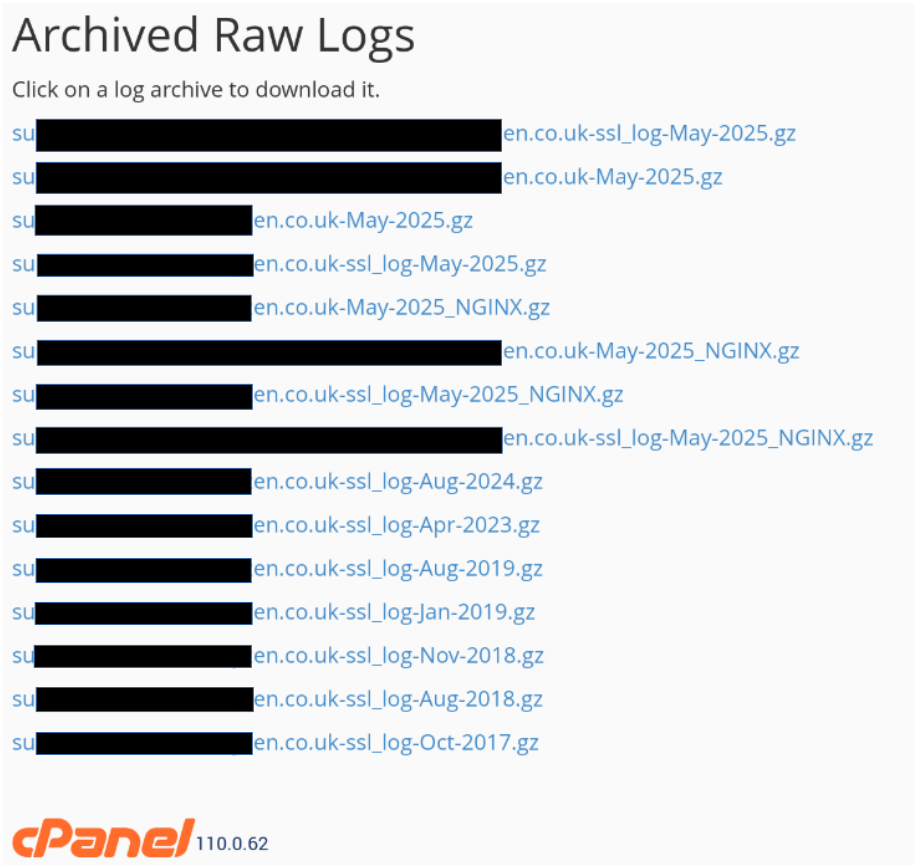


hxxps[://][ORG_DOMAIN][.]com:2083/cpsess1440224781/frontend/jupiter/raw/index[.]html

Unfortunately, the logs for April have been automatically removed. This means I can’t cross-check the logs for any of the suspicious user accounts, web page creations or suspicious activity in April 2025. I therefore can’t verify if there was any attempt to delete evidence or any log tampering.

I can’t view any suspicious behaviour attempted between the end of August 2024 and April 29th 2025.

Archived Raw Logs:



hxxps[://][ORG_DOMAIN][.]com:2083/cpsess1440224781/frontend/jupiter/raw/index[.]html

The archived logs for May 2025 run from 30/04/25 to 31/05/25.
I downloaded the raw logs from May 2025 and first looked for entries that lined up with our unauthorised login attempts.

13th May 2025:

There were no log entries matching the exact minute of login attempts, but there were suspicious entries in close proximity:

(1) 13/May: Unsuccessful `GET` requests from `144[.]XXX[.]XXX[.]147` to access an Incutio XML-RPC Library, from user-agent `Mozlila/5.0`:

```
144.[redacted].147 - - [13/May/2025:18:31:13 +0000] "GET /wp-content/IXR/index.php HTTP/1.1" 301 - "-" "Mozlila/5.0 (Linux; Android 7.0; SM-G892A Bulid/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/60.0.3112.107 Moblie Safari/537.36"
144.[redacted].147 - - [13/May/2025:18:31:20 +0000] "GET /wp-content/IXR/ HTTP/1.1" 404 78930 "-" "Mozlila/5.0 (Linux; Android 7.0; SM-G892A Bulid/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/60.0.3112.107 Moblie Safari/537.36"
3.[redacted]128 - - [13/May/2025:19:05:16 +0000] "HEAD /wordpress HTTP/1.1" 404 - "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36"
```

[ORG_DOMAIN].com.[ORG_DOMAIN].[HOSTING_DOMAIN].co.uk-May-2025

(2) 13/May: Unsuccessful `GET` request from `144[.]XXX[.]XXX[.]10` to receive information about the WordPress plugins in use on the website, from user-agent `Mozlila/5.0`:

```
144.[redacted].10 - - [13/May/2025:19:45:37 +0000] "GET /wp-content/plugins/about.php HTTP/1.1" 404 78958 "-" "Mozlila/5.0 (Linux; Android 7.0; SM-G892A Bulid/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/60.0.3112.107 Moblie Safari/537.36"
```

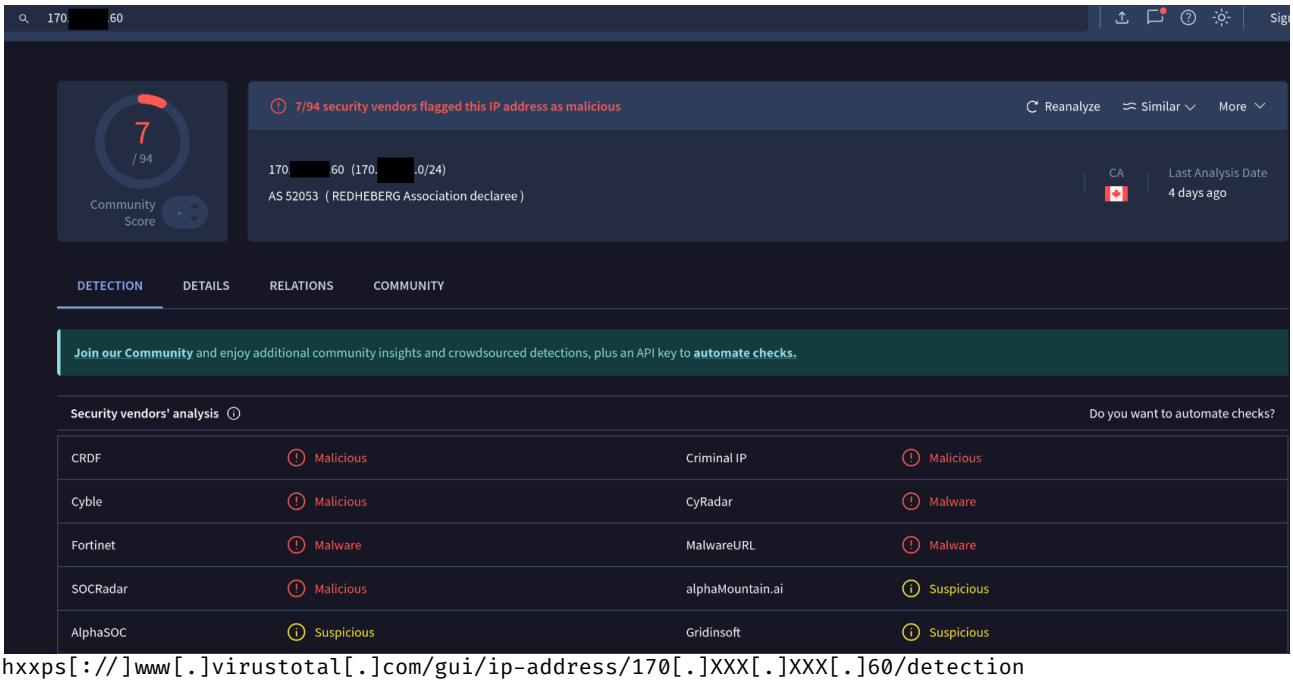
[ORG_DOMAIN].com.[ORG_DOMAIN].[HOSTING_DOMAIN].co.uk-May-2025

(3) 13/May: Unsuccessful `GET` request from `170[.]XXX[.]XXX[.]60` potentially scanning for misconfigured or exposed `autodiscover.xml` files:

```
170.[redacted].60 - - [13/May/2025:18:22:41 +0000] "GET /autodiscover/autodiscover.xml HTTP/1.1" 400 52 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 Chrome/121.0.0.0"
```

[ORG_DOMAIN].[HOSTING_DOMAIN].co.uk-ssl_log-May-2025

Out of the three IP addresses I identified as suspicious, the third was flagged by `virustotal[.]com` as malicious.



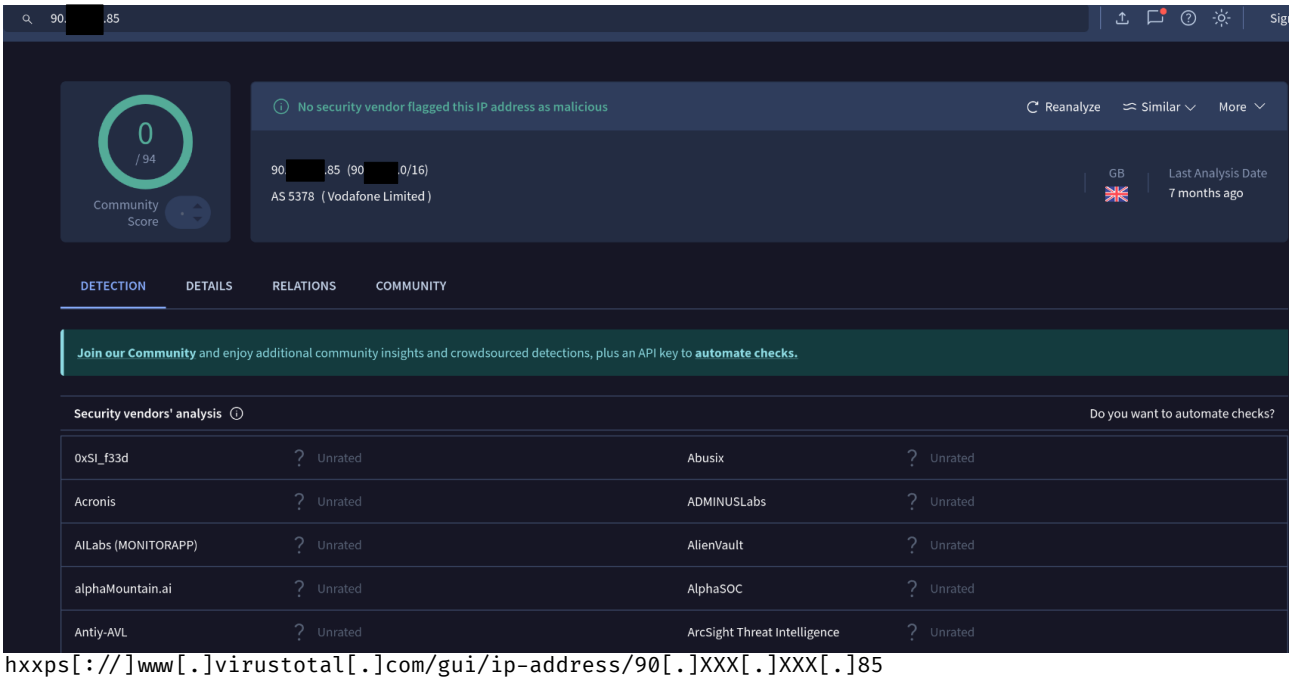
`hxxps[://]www[.]virustotal[.]com/gui/ip-address/170[.]XXX[.]XXX[.]60/detection`

Another log showed multiple successful `GET` requests from `90[.]XXX[.]XXX[.]85` in quick succession.

The requests seem to be targeting various plugins, referred from `hxxps[://][ORG_DOMAIN][.]com/whos-who/`.

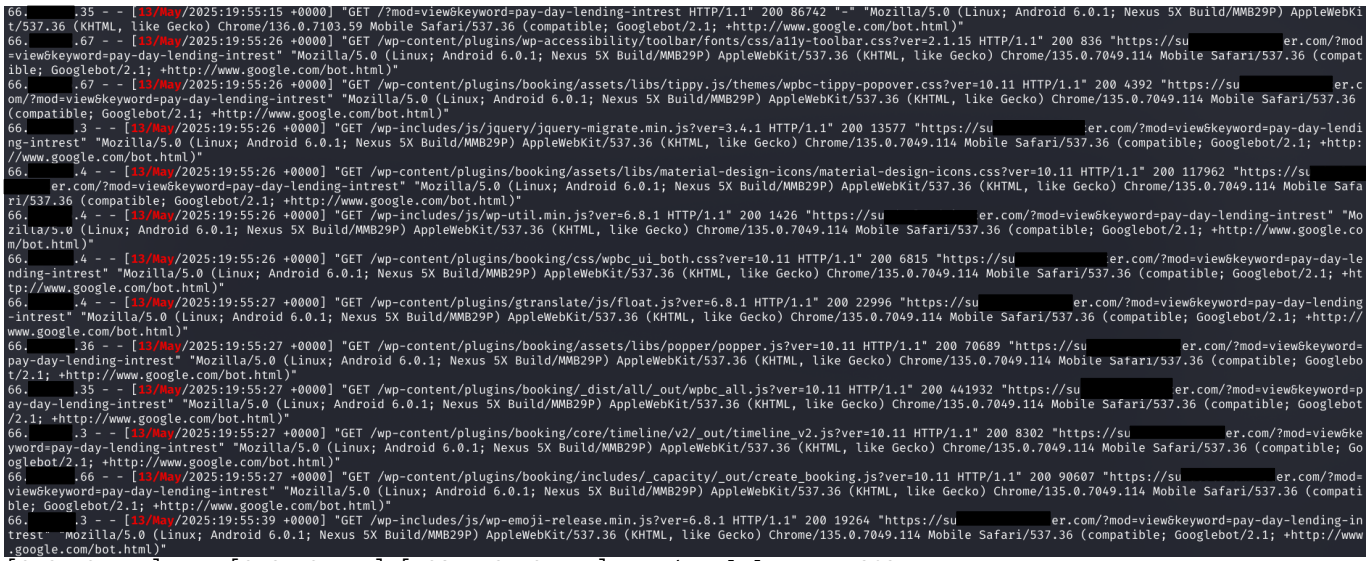
`virustotal[.]com` has no record of this IP address, however the last record of these attempts is a successful `POST` request of `/wp-admin/admin-ajax.php` at 19:35:29. This could potentially be evidence of searching for a vulnerability, as `/wp-admin/admin-ajax.php` has been exploited using SQL injections through vulnerable plugins before (see CVE-2014-8375).

`[ORG_DOMAIN].com.[ORG_DOMAIN].[HOSTING_DOMAIN].co.uk-ssl_log-May-2025`



hxxps[://]www[.]virustotal[.]com/gui/ip-address/90[.]XXX[.]XXX[.]85

The next entry is at 19:55:15 by an official “Googlebot”. This is a successful `GET` request for `/?mod=view&keyword=pay-day-lending-intrest`. The following entries use this URL as the referrer:



[ORG_DOMAIN].com.[ORG_DOMAIN].[HOSTING_DOMAIN].co.uk-ssl_log-May-2025

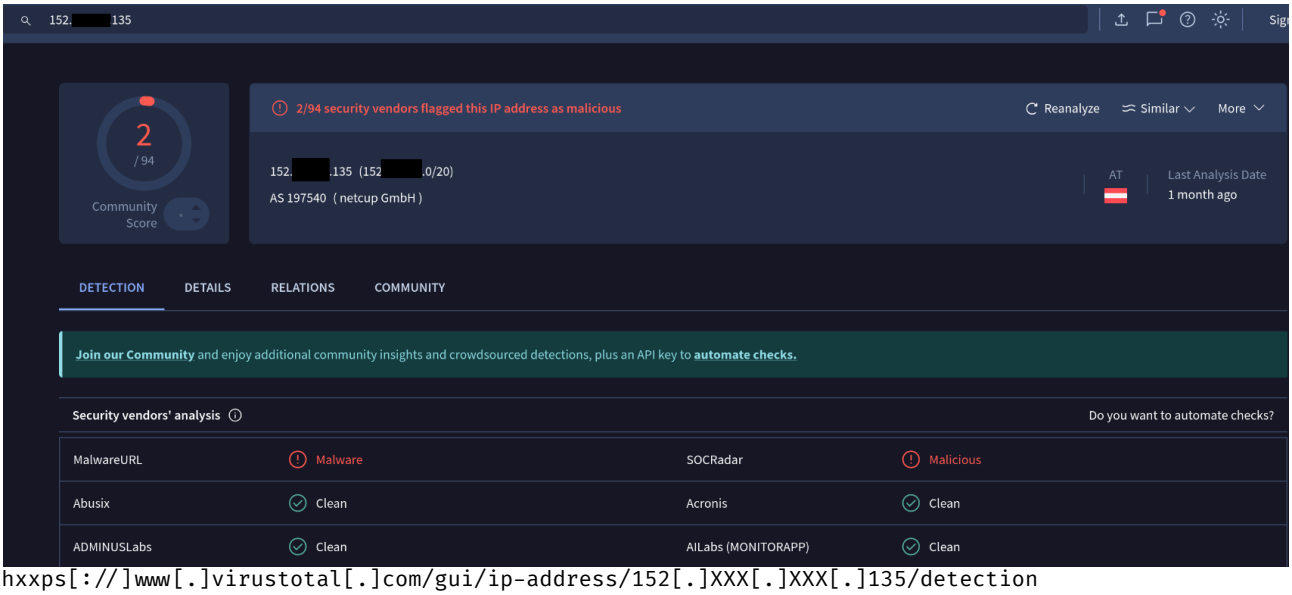
This is suspicious, as this suggests “Googlebot” is using an internal or external link to this URL.

15th May 2025:

(1) 15/May: Unsuccessful `GET` requests for `image001.jpg` from `152[.]XXX[.]XXX[.]135` at 10:36:47.

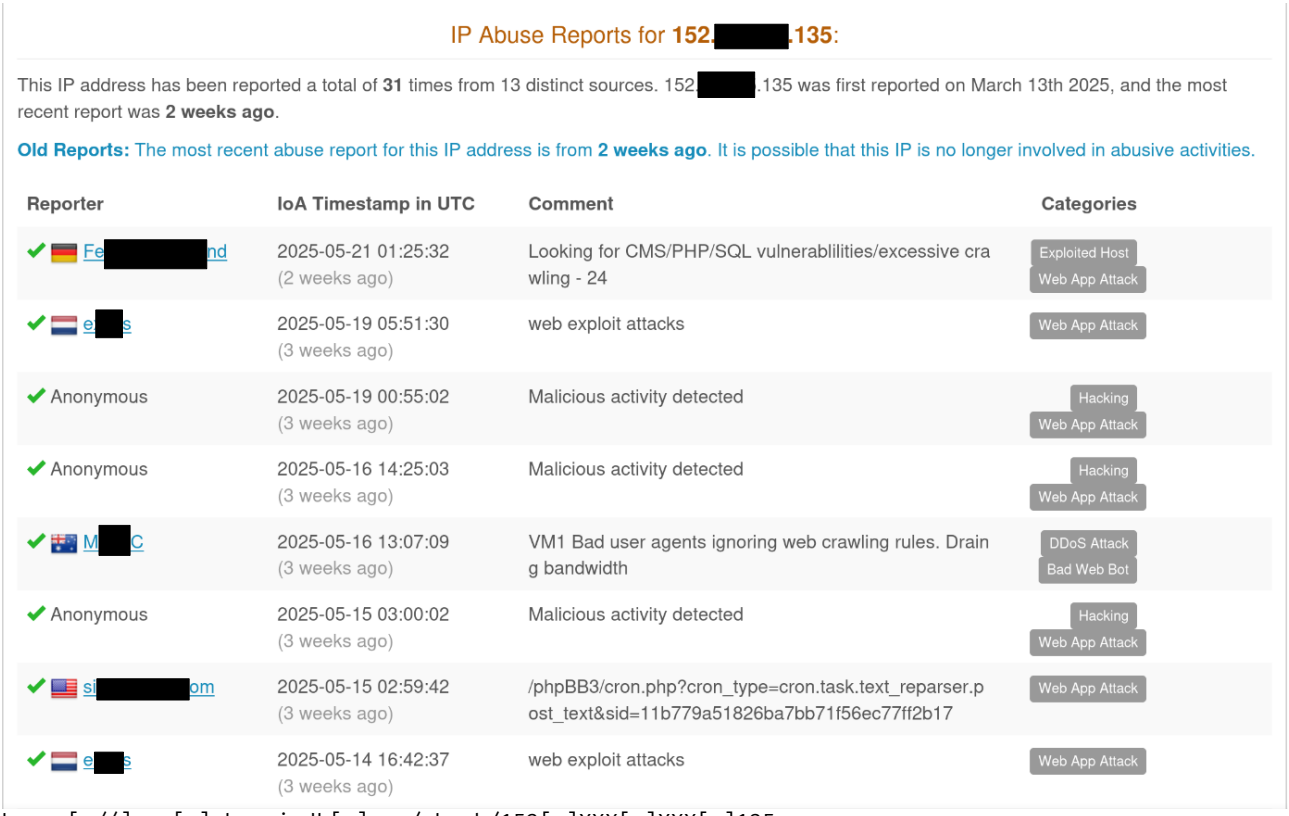
[ORG_DOMAIN].com.[ORG_DOMAIN].[HOSTING_DOMAIN].co.uk-May-2025

This IP address is listed as malicious by `virustotal[.]com`, however with only 1-2 detections it could be misidentified.



hxxps[://]www[.]virustotal[.]com/gui/ip-address/152[.]XXX[.]XXX[.]135/detection

Looking on abuseipdb[.]com however, shows that this IP is indeed abusive, and has been previously reported for malicious activity.



IP Abuse Reports for 152.[redacted].135:

This IP address has been reported a total of **31** times from 13 distinct sources. 152.[redacted].135 was first reported on March 13th 2025, and the most recent report was **2 weeks ago**.

Old Reports: The most recent abuse report for this IP address is from **2 weeks ago**. It is possible that this IP is no longer involved in abusive activities.

Reporter	IoA Timestamp in UTC	Comment	Categories
Fe[redacted]nd	2025-05-21 01:25:32 (2 weeks ago)	Looking for CMS/PHP/SQL vulnerablilities/excessive crawling - 24	Exploited Host, Web App Attack
e[redacted]s	2025-05-19 05:51:30 (3 weeks ago)	web exploit attacks	Web App Attack
Anonymous	2025-05-19 00:55:02 (3 weeks ago)	Malicious activity detected	Hacking, Web App Attack
Anonymous	2025-05-16 14:25:03 (3 weeks ago)	Malicious activity detected	Hacking, Web App Attack
M[redacted]C	2025-05-16 13:07:09 (3 weeks ago)	VM1 Bad user agents ignoring web crawling rules. Draing bandwidth	DDoS Attack, Bad Web Bot
Anonymous	2025-05-15 03:00:02 (3 weeks ago)	Malicious activity detected	Hacking, Web App Attack
si[redacted]om	2025-05-15 02:59:42 (3 weeks ago)	/phpBB3/cron.php?cron_type=cron.task.text_reparser.post_text&sid=11b779a51826ba7bb71f56ec77ff2b17	Web App Attack
e[redacted]s	2025-05-14 16:42:37 (3 weeks ago)	web exploit attacks	Web App Attack

hxxps[://]www[.]abuseipdb[.]com/check/152[.]XXX[.]XXX[.]135

Suspicious Activity Throughout May 2025:

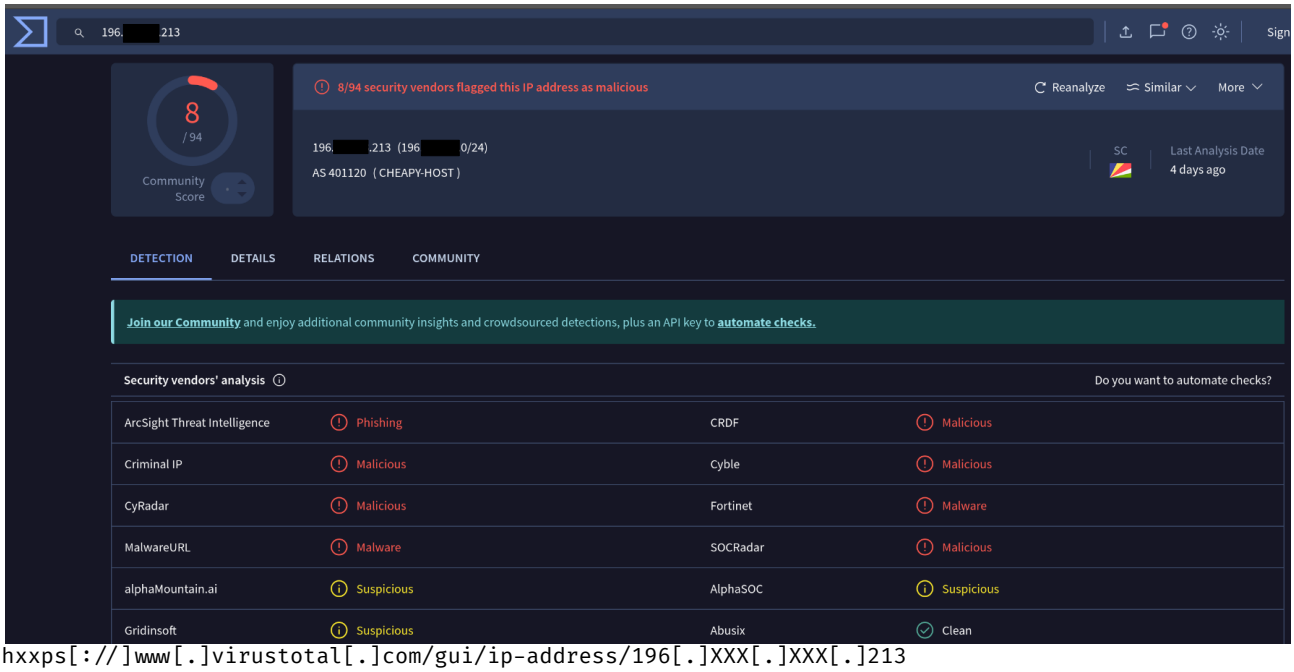
Next, I look to see if there's any suspicious activity in the hours preceding the login attempts. I quickly find some more references to the user-agent mozlila.

```
196.[redacted].213 - - [13/May/2025:01:10:10 +0000] "POST /ALFA_DATA/alfacgiapi/perl.alfa HTTP/1.1" 200 10953 "www.google.com" "Mozlila/5.0 (Linux; Android 7.0; SM-G892A Bulid/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/60.0.3112.107 Moblie Safari/537.36"
196.[redacted].213 - - [13/May/2025:01:10:10 +0000] "POST /alfacgiapi/perl.alfa HTTP/1.1" 200 10941 "www.google.com" "Mozlila/5.0 (Linux; Android 7.0; SM-G892A Bulid/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/60.0.3112.107 Moblie Safari/537.36"
```

[ORG_DOMAIN].com.[ORG_DOMAIN].[HOSTING_DOMAIN].co.uk-May-2025

These successful `POST` results are particularly concerning as they seem to refer to a perl script, hosted on a German web hosting provider, [REDACTED]. It is potentially referring to a CGI script handler provided by their shared hosting environment.

`virustotal[.]com` identifies the source IP as malicious.



hxxps[://]www[.]virustotal[.]com/gui/ip-address/196[.]XXX[.]XXX[.]213

Looking further through the logs, it is clear that this website is a target for opportunistic attacks, botnets and brute-force login attempts:

```
51.[redacted].247 - - [13/May/2025:01:54:15 +0000] "GET /wp-admin/admin-ajax.php?action=duplicator_download&file=../wp-config.php HTTP/1.1" 404 78947 "-" "python-requests/2.22.0"
```
[ORG_DOMAIN].com.[ORG_DOMAIN].[HOSTING_DOMAIN].co.uk-May-2025

```
205.[redacted].3 - - [17/May/2025:23:30:06 +0000] "GET /z0f76a1d14fd21a8fb5fd0d03e0fdc3d3cedae52f?wsidchk=10077808&pdata=http%253A%252F%252Fmail.su[redacted]en.co.uk%252F&id=7fa3b767
c460b54a2be4d49030b349c7&ts=1747524605 HTTP/1.1" 302 226 "http://mail.su[redacted]en.co.uk/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chr
ome/117.0.5938.132 Safari/537.36"
```
[ORG_DOMAIN].[HOSTING_DOMAIN].co.uk-May-2025

```
158.[redacted].79 - - [13/May/2025:19:47:14 +0000] "GET /wp-content/plugins/cve-2024-46188/views/viewsecurity.php HTTP/1.1" 404 79016 "-" "Linux Mozilla"
152.[redacted].211 - - [13/May/2025:21:54:24 +0000] "GET /wp-content/uploads/2013/04/[redacted]-150x150.png HTTP/1.1" 404 79004 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537
.36 (KHTML, like Gecko) Chrome/100.0.4503.685 Safari/537.36"
74.[redacted].69 - - [13/May/2025:22:48:12 +0000] "HEAD /Archive.zip HTTP/1.1" 404 - "-" "-"
137.[redacted].200 - - [13/May/2025:22:48:13 +0000] "HEAD /backup.zip HTTP/1.1" 404 - "-" "-"
```
[ORG_DOMAIN].com.[ORG_DOMAIN].[HOSTING_DOMAIN].co.uk-May-2025

```
103.[redacted].66 - - [30/May/2025:10:12:15 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0"
103.[redacted].45 - - [30/May/2025:05:59:11 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0"
124.[redacted].148 - - [31/May/2025:01:24:54 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0"
129.[redacted].91 - - [30/May/2025:20:26:57 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:80.0) Gecko/20100101 Firefox/80.0"
134.[redacted].153 - - [30/May/2025:02:23:13 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:45.0) Gecko/20100101 Firefox/45.0"
13.5[redacted].79 - - [28/May/2025:06:40:21 +0000] "POST /wp-login.php HTTP/1.1" 302 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0"
138.[redacted]0 - - [30/May/2025:12:48:02 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:53.0) Gecko/20100101 Firefox/53.0"
139.[redacted].71 - - [27/May/2025:20:54:03 +0000] "POST /wp-login.php HTTP/1.1" 302 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0"
139.[redacted].19 - - [29/May/2025:18:39:00 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:51.0) Gecko/20100101 Firefox/51.0"
141.[redacted].85 - - [27/May/2025:15:08:54 +0000] "POST /wp-login.php HTTP/1.1" 302 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:54.0) Gecko/20100101 Firefox/54.0"
142.[redacted].108 - - [28/May/2025:11:24:10 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0"
142.[redacted].108 - - [31/May/2025:08:27:43 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0"
142.[redacted].194 - - [30/May/2025:00:52:01 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:52.0) Gecko/20100101 Firefox/52.0"
142.[redacted].194 - - [30/May/2025:04:13:17 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:54.0) Gecko/20100101 Firefox/54.0"
143.[redacted].102 - - [28/May/2025:22:22:47 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0"
143.[redacted].102 - - [30/May/2025:14:26:46 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/93.0"
143.[redacted].102 - - [30/May/2025:22:50:48 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:40.0) Gecko/20100101 Firefox/40.0"
143.[redacted].39 - - [28/May/2025:12:22:31 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0"
146.[redacted].61 - - [28/May/2025:18:54:37 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:64.0) Gecko/20100101 Firefox/64.0"
157.[redacted].5 - - [30/May/2025:19:40:12 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0"
158.[redacted].34 - - [28/May/2025:21:00:15 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:57.0) Gecko/20100101 Firefox/57.0"
159.[redacted].190 - - [29/May/2025:09:10:14 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0"
159.[redacted].103 - - [28/May/2025:13:21:29 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:45.0) Gecko/20100101 Firefox/45.0"
159.[redacted].12 - - [28/May/2025:08:28:21 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko/20100101 Firefox/66.0"
159.[redacted].37 - - [30/May/2025:03:18:23 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:53.0) Gecko/20100101 Firefox/53.0"
161.[redacted].41 - - [29/May/2025:05:33:08 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:70.0) Gecko/20100101 Firefox/70.0"
161.[redacted].7 - - [28/May/2025:00:50:01 +0000] "POST /wp-login.php HTTP/1.1" 302 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:47.0) Gecko/20100101 Firefox/47.0"
164.[redacted].250 - - [28/May/2025:02:48:33 +0000] "POST /wp-login.php HTTP/1.1" 302 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0"
164.[redacted].250 - - [28/May/2025:10:25:16 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:63.0) Gecko/20100101 Firefox/63.0"
164.[redacted].122 - - [27/May/2025:18:55:43 +0000] "POST /wp-login.php HTTP/1.1" 302 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:49.0) Gecko/20100101 Firefox/49.0"
165.[redacted].49 - - [28/May/2025:21:25:49 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0"
167.[redacted].27 - - [29/May/2025:00:56:43 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0"
170.[redacted].210 - - [27/May/2025:16:08:57 +0000] "POST /wp-login.php HTTP/1.1" 302 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:73.0) Gecko/20100101 Firefox/73.0"
170.[redacted].210 - - [30/May/2025:09:20:17 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:50.0) Gecko/20100101 Firefox/50.0"
172.[redacted].147 - - [30/May/2025:17:55:21 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:84.0) Gecko/20100101 Firefox/84.0"
178.[redacted].66 - - [28/May/2025:05:42:54 +0000] "POST /wp-login.php HTTP/1.1" 302 0 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:88.0) Gecko/20100101 Firefox/88.0"
178.[redacted].66 - - [31/May/2025:03:13:03 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:43.0) Gecko/20100101 Firefox/43.0"
178.[redacted].48 - - [31/May/2025:04:51:14 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0"
184.[redacted].130 - - [29/May/2025:10:30:02 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0"
184.[redacted].130 - - [30/May/2025:16:12:22 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:67.0) Gecko/20100101 Firefox/67.0"
185.[redacted].59 - - [29/May/2025:03:40:14 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:66.0) Gecko/20100101 Firefox/66.0"
185.[redacted].59 - - [29/May/2025:20:16:49 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:78.0) Gecko/20100101 Firefox/78.0"
190.[redacted].218 - - [29/May/2025:06:46:51 +0000] "POST /wp-login.php HTTP/1.1" 415 9192 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:62.0) Gecko/20100101 Firefox/62.0"
```
[ORG_DOMAIN].com.[ORG_DOMAIN].[HOSTING_DOMAIN].co.uk-May-2025_NGINX

```
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 415 2751 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 508 288 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 508 288 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 508 288 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 508 288 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 508 288 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 508 288 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 508 288 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 508 288 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 508 288 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 415 2751 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 415 2751 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 415 2751 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 415 2751 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 415 2751 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 415 2751 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 415 2751 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 415 2751 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 415 2751 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 415 2751 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 415 2751 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 415 2751 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 415 2751 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 415 2751 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 415 2751 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 415 2751 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 415 2751 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 415 2751 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 415 2751 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:29 +  00] "POST /wp-login.php HTTP/1.1" 415 2751 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:30 +  00] "POST /wp-login.php HTTP/1.1" 415 2751 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:30 +  00] "POST /wp-login.php HTTP/1.1" 415 2751 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:30 +  00] "POST /wp-login.php HTTP/1.1" 508 288 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:30 +  00] "POST /wp-login.php HTTP/1.1" 508 288 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:30 +  00] "POST /wp-login.php HTTP/1.1" 508 288 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:30 +  00] "POST /wp-login.php HTTP/1.1" 508 288 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:30 +  00] "POST /wp-login.php HTTP/1.1" 508 288 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:30 +  00] "POST /wp-login.php HTTP/1.1" 508 288 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:30 +  00] "POST /wp-login.php HTTP/1.1" 508 288 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:30 +  00] "POST /wp-login.php HTTP/1.1" 508 288 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:30 +  00] "POST /wp-login.php HTTP/1.1" 415 2751 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:30 +  00] "POST /wp-login.php HTTP/1.1" 415 2751 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
22.[redacted].25 - - [21/May/2025:23:51:30 +  00] "POST /wp-login.php HTTP/1.1" 415 2751 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
00] "POST /wp-login.php HTTP/1.1" 415 2751 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:135.0) Gecko/20100101 Firefox/135.0"
```

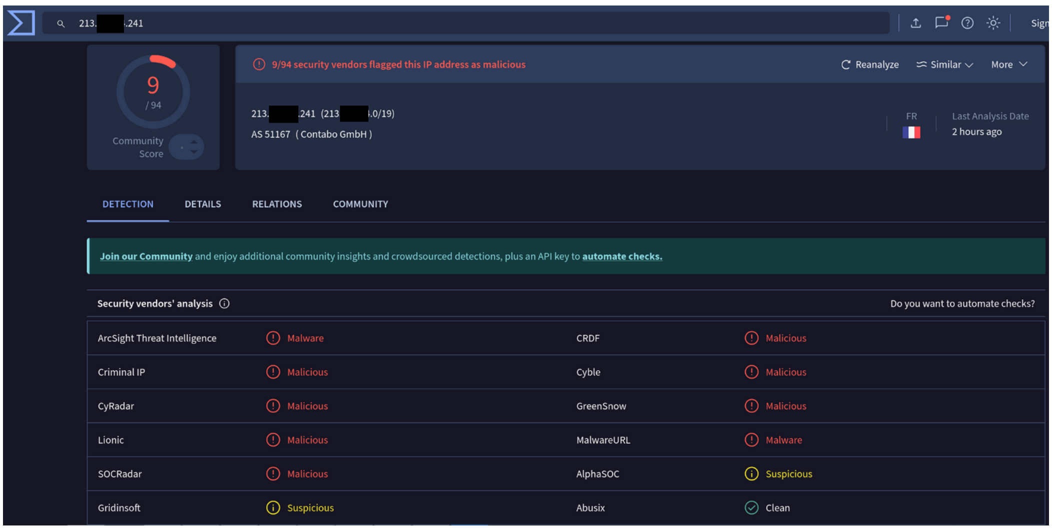
[ORG_DOMAIN].com.[ORG_DOMAIN].[HOSTING_DOMAIN].co.uk-May-2025

The site has also been attacked with attempts to download any vulnerable compressed data archives:

```
213.[redacted].241 - - [13/May/2025:16:58:12 +0000] "GET /temp.zip HTTP/1.1" 200 10941 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"
213.[redacted].241 - - [13/May/2025:16:58:12 +0000] "GET /dump.zip HTTP/1.1" 200 10941 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"
213.[redacted].241 - - [13/May/2025:16:58:12 +0000] "GET /api.zip HTTP/1.1" 200 10940 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"
213.[redacted].241 - - [13/May/2025:16:58:12 +0000] "GET /htdocs.zip HTTP/1.1" 200 10943 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"
213.[redacted].241 - - [13/May/2025:16:58:12 +0000] "GET /app.zip HTTP/1.1" 200 10940 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"
213.[redacted].241 - - [13/May/2025:16:58:12 +0000] "GET /db.zip HTTP/1.1" 200 10939 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"
213.[redacted].241 - - [13/May/2025:16:58:12 +0000] "GET /backup_1.zip HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"
213.[redacted].241 - - [13/May/2025:16:58:12 +0000] "GET /bak.zip HTTP/1.1" 200 10940 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"
213.[redacted].241 - - [13/May/2025:16:58:12 +0000] "GET /www.zip HTTP/1.1" 200 10940 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"
213.[redacted].241 - - [13/May/2025:16:58:12 +0000] "GET /webapps.zip HTTP/1.1" 200 10944 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"
213.[redacted].241 - - [13/May/2025:16:58:12 +0000] "GET /backup_2.zip HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"
213.[redacted].241 - - [13/May/2025:16:58:12 +0000] "GET /dbadmin.zip HTTP/1.1" 200 10944 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"
213.[redacted].241 - - [13/May/2025:16:58:12 +0000] "GET /uploads.zip HTTP/1.1" 200 10944 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"
213.[redacted].241 - - [13/May/2025:16:58:12 +0000] "GET /backup_3.zip HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"
213.[redacted].241 - - [13/May/2025:16:58:12 +0000] "GET /admin.zip HTTP/1.1" 200 10942 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"
213.[redacted].241 - - [13/May/2025:16:58:12 +0000] "GET /old.zip HTTP/1.1" 200 10940 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"
213.[redacted].241 - - [13/May/2025:16:58:12 +0000] "GET /ftp.zip HTTP/1.1" 200 10940 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"
213.[redacted].241 - - [13/May/2025:16:58:12 +0000] "GET /dbase.zip HTTP/1.1" 200 10942 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"
213.[redacted].241 - - [13/May/2025:16:58:12 +0000] "GET /Release.zip HTTP/1.1" 200 10944 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"
213.[redacted].241 - - [13/May/2025:16:58:12 +0000] "GET /web.zip HTTP/1.1" 200 10940 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"
213.[redacted].241 - - [13/May/2025:16:58:12 +0000] "GET /test.zip HTTP/1.1" 200 10941 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"
213.[redacted].241 - - [13/May/2025:16:58:12 +0000] "GET /database.zip HTTP/1.1" 200 10945 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"
```

[ORG_DOMAIN].[HOSTING_DOMAIN].co.uk-May-2025

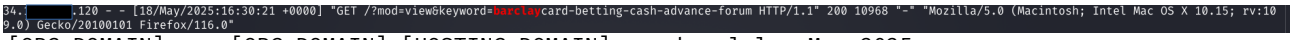
This source IP (`213[.]XXX[.]XXX[.]241`) has been identified as malicious by `virustotal[.]com`.



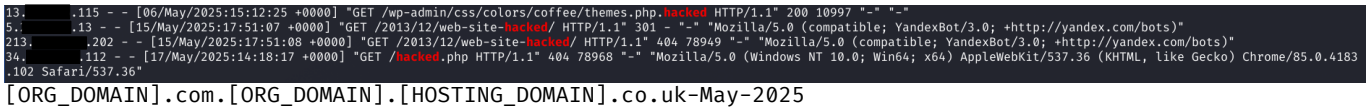
hxxps[://]www[.]virustotal[.]com/gui/ip-address/213[.]XXX[.]XXX[.]241

I also find references to our “barclaycard” page and our “hacked” page:

[ORG_DOMAIN].com.[ORG_DOMAIN].[HOSTING_DOMAIN].co.uk-May-2025_NGINX



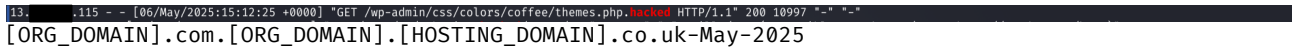
[ORG_DOMAIN].com.[ORG_DOMAIN].[HOSTING_DOMAIN].co.uk-ssl_log-May-2025



[ORG_DOMAIN].com.[ORG_DOMAIN].[HOSTING_DOMAIN].co.uk-May-2025

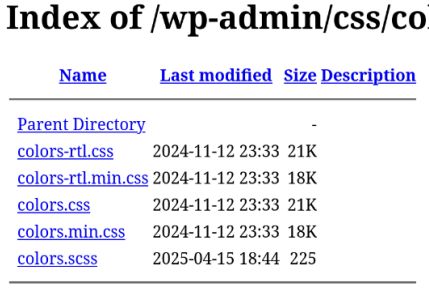
These results, especially from `Barkrowler` and `YandexBot` (web crawlers) strongly suggest that these posts existed at one point on `[ORG_DOMAIN][.]com`, as bots don’t generally brute-force or generate URLs without some basis (like links or past data).

The log entry below looks especially suspicious as there is no user-agent listed, which in the context of the web request suggests malicious or stealthy access.



[ORG_DOMAIN].com.[ORG_DOMAIN].[HOSTING_DOMAIN].co.uk-May-2025

This URL (`/wp-admin/css/colors/coffee/themes.php.hacked`) doesn’t exist now, but following the URL string leads us to a Parent Directory that may have potentially held `themes.php.hacked`.



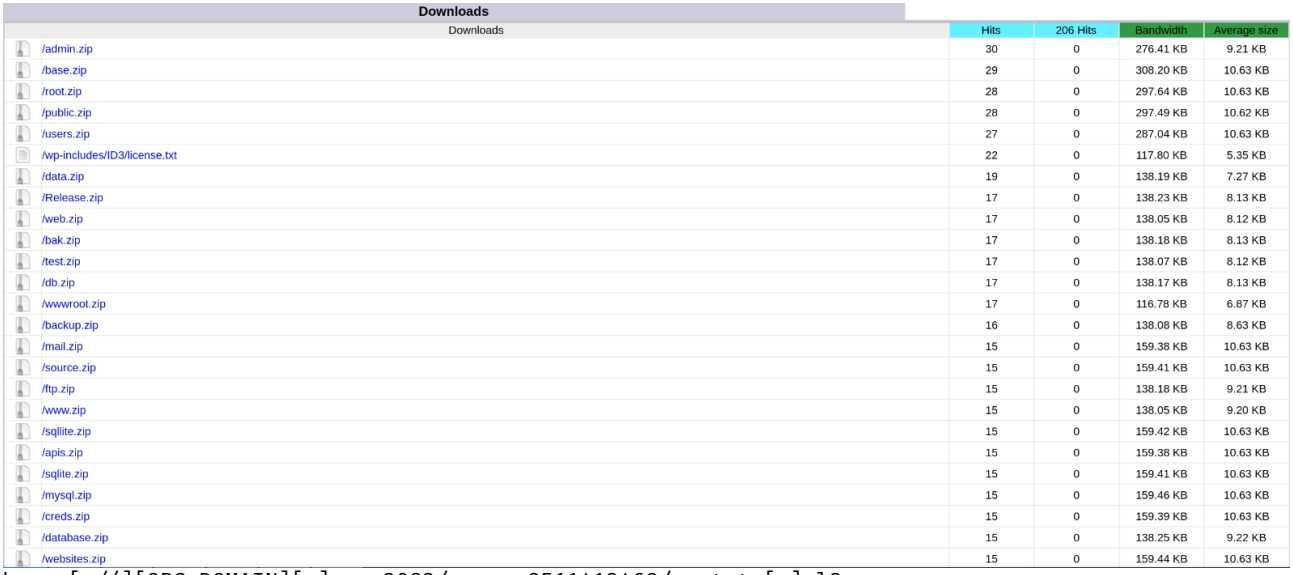
Index of /wp-admin/css/colors/coffee

Name	Last modified	Size	Description
Parent Directory		-	
colors-rtl.css	2024-11-12 23:33	21K	
colors-rtl.min.css	2024-11-12 23:33	18K	
colors.css	2024-11-12 23:33	21K	
colors.min.css	2024-11-12 23:33	18K	
colors.scss	2025-04-15 18:44	225	

hxxps[://][ORG_DOMAIN][.]com/wp-admin/css/colors/coffee/

Statistics

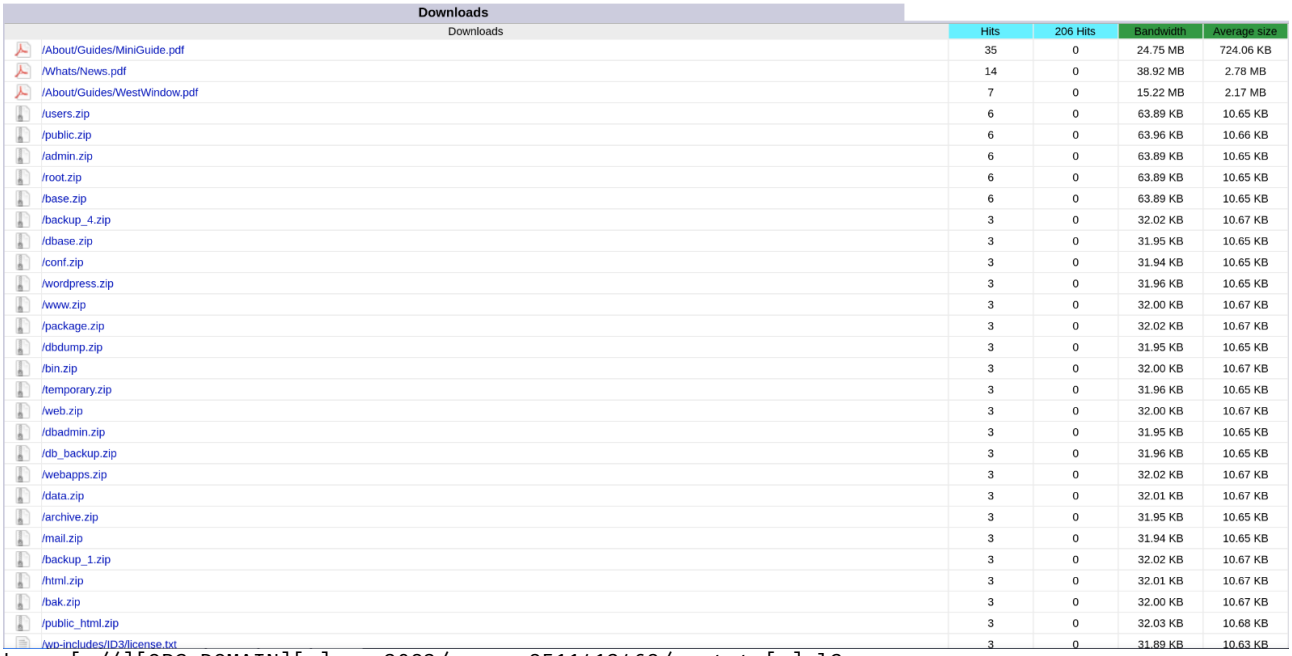
I access the “cPanel Statistics” section of the “cPanel Control Panel” to see what, if anything, has been successfully downloaded. There are multiple successful downloads averaging `~10.6 KB`.



Downloads

Downloads	Hits	206 Hits	Bandwidth	Average size
/admin.zip	30	0	276.41 KB	9.21 KB
/base.zip	29	0	308.20 KB	10.63 KB
/root.zip	28	0	297.64 KB	10.63 KB
/public.zip	28	0	297.49 KB	10.62 KB
/users.zip	27	0	287.04 KB	10.63 KB
/wp-includes/ID3/license.txt	22	0	117.80 KB	5.35 KB
/data.zip	19	0	138.19 KB	7.27 KB
/Release.zip	17	0	138.23 KB	8.13 KB
/web.zip	17	0	138.05 KB	8.12 KB
/bak.zip	17	0	138.18 KB	8.13 KB
/test.zip	17	0	138.07 KB	8.12 KB
/db.zip	17	0	138.17 KB	8.13 KB
/wwwroot.zip	17	0	116.78 KB	6.87 KB
/backup.zip	16	0	138.08 KB	8.63 KB
/mail.zip	15	0	159.38 KB	10.63 KB
/source.zip	15	0	159.41 KB	10.63 KB
/ftp.zip	15	0	138.18 KB	9.21 KB
/www.zip	15	0	138.05 KB	9.20 KB
/sqllite.zip	15	0	159.42 KB	10.63 KB
/apis.zip	15	0	159.38 KB	10.63 KB
/sqlite.zip	15	0	159.41 KB	10.63 KB
/mysql.zip	15	0	159.46 KB	10.63 KB
/creds.zip	15	0	159.39 KB	10.63 KB
/database.zip	15	0	138.25 KB	9.22 KB
/websites.zip	15	0	159.44 KB	10.63 KB

`hxxps[://][ORG_DOMAIN][.]com:2083/cpsess8511412468/awstats[.]pl?databasebreak=month&month=all&year=2025&output=main&config=[ORG_DOMAIN][.]com[.][ORG_DOMAIN][.][HOSTING_DOMAIN][.]co[.]uk&lang=en&ssl=&framename=index`



Downloads

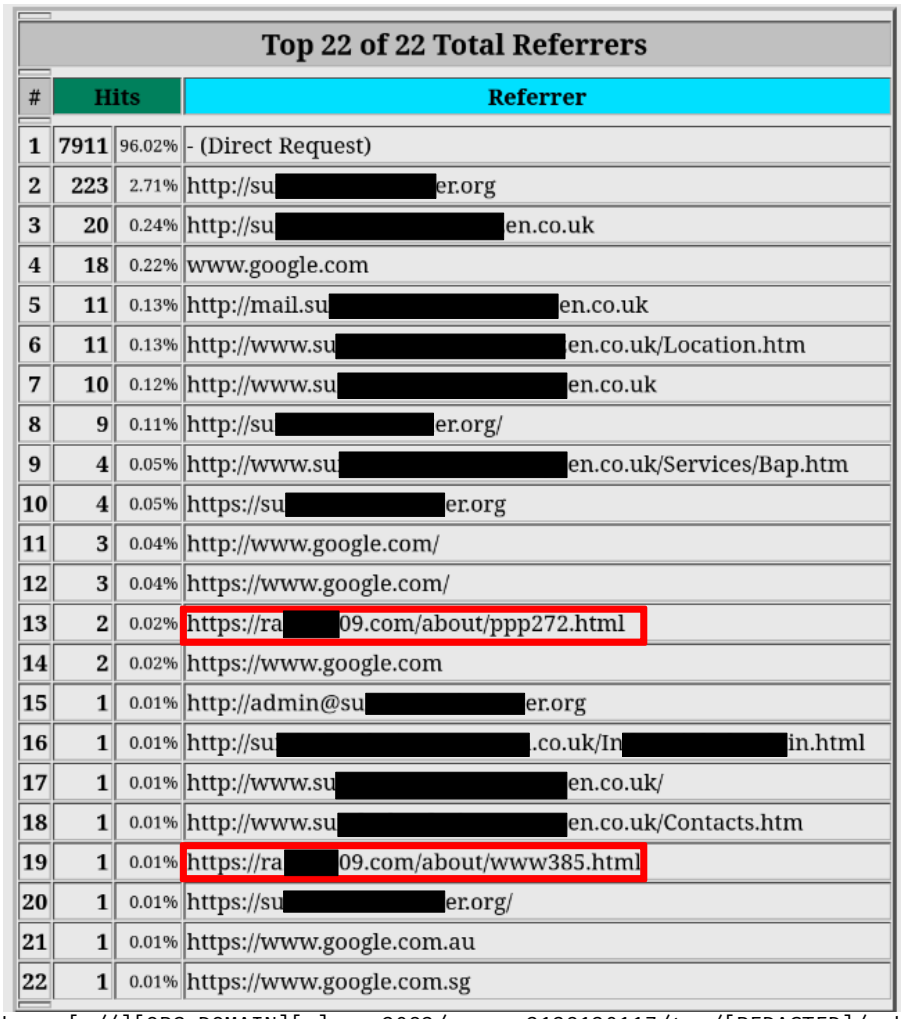
Downloads	Hits	206 Hits	Bandwidth	Average size
/About/Guides/MiniGuide.pdf	35	0	24.75 MB	724.06 KB
/Whats/News.pdf	14	0	38.92 MB	2.78 MB
/About/Guides/WestWindow.pdf	7	0	15.22 MB	2.17 MB
/users.zip	6	0	63.89 KB	10.65 KB
/public.zip	6	0	63.96 KB	10.66 KB
/admin.zip	6	0	63.89 KB	10.65 KB
/root.zip	6	0	63.89 KB	10.65 KB
/base.zip	6	0	63.89 KB	10.65 KB
/backup_4.zip	3	0	32.02 KB	10.67 KB
/dbase.zip	3	0	31.95 KB	10.65 KB
/conf.zip	3	0	31.94 KB	10.65 KB
/wordpress.zip	3	0	31.96 KB	10.65 KB
/www.zip	3	0	32.00 KB	10.67 KB
/package.zip	3	0	32.02 KB	10.67 KB
/dbdump.zip	3	0	31.95 KB	10.65 KB
/bin.zip	3	0	32.00 KB	10.67 KB
/temporary.zip	3	0	31.96 KB	10.65 KB
/web.zip	3	0	32.00 KB	10.67 KB
/dbadmin.zip	3	0	31.95 KB	10.65 KB
/db_backup.zip	3	0	31.96 KB	10.65 KB
/webapps.zip	3	0	32.02 KB	10.67 KB
/data.zip	3	0	32.01 KB	10.67 KB
/archive.zip	3	0	31.95 KB	10.65 KB
/mail.zip	3	0	31.94 KB	10.65 KB
/backup_1.zip	3	0	32.02 KB	10.67 KB
/html.zip	3	0	32.01 KB	10.67 KB
/bak.zip	3	0	32.00 KB	10.67 KB
/public_html.zip	3	0	32.03 KB	10.68 KB
/wp-includes/ID3/license.txt	3	0	31.89 KB	10.63 KB

`hxxps[://][ORG_DOMAIN][.]com:2083/cpsess8511412468/awstats[.]pl?databasebreak=month&month=all&year=2025&output=downloads&config=[ORG_DOMAIN][.][HOSTING_DOMAIN][.]co[.]uk&lang=en&ssl=&framename=index`

I download `admin.zip` as a test, and the result is `~71 KB`. All the downloaded `.zip` files are averaging `~10.6 KB` which strongly suggests either a partial download, or the download of an error message. This looks like a false positive.

Usage Statistics

Next, I want to see if there are any referrals from suspicious websites or locations. I use “Webalizer”, a web log analysis tool that gives a historical overview of website traffic. Here, I find two suspicious domains.

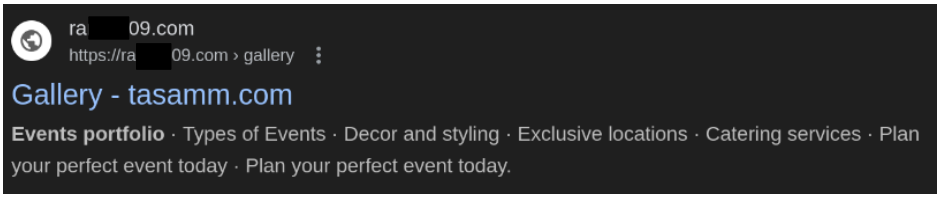


Top 22 of 22 Total Referrers

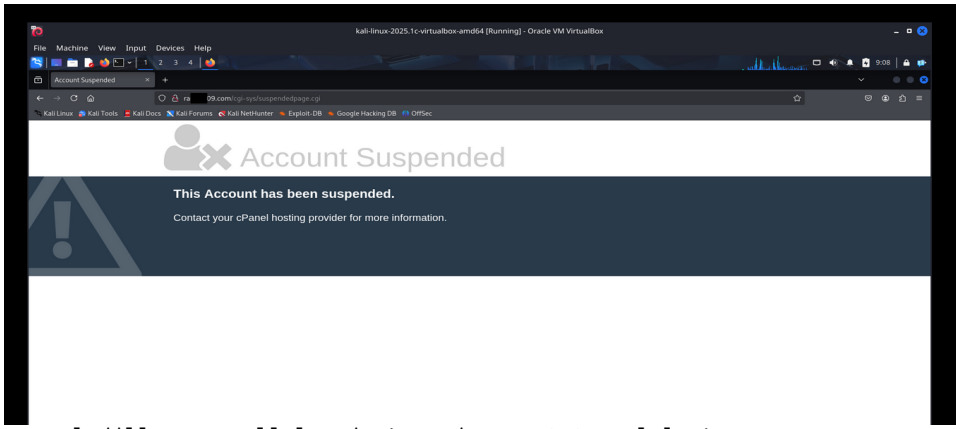
#	Hits		Referrer
1	7911	96.02%	- (Direct Request)
2	223	2.71%	http://su[redacted]er.org
3	20	0.24%	http://su[redacted]en.co.uk
4	18	0.22%	www.google.com
5	11	0.13%	http://mail.su[redacted]en.co.uk
6	11	0.13%	http://www.su[redacted]en.co.uk/Location.htm
7	10	0.12%	http://www.su[redacted]en.co.uk
8	9	0.11%	http://su[redacted]er.org/
9	4	0.05%	http://www.su[redacted]en.co.uk/Services/Bap.htm
10	4	0.05%	https://su[redacted]er.org
11	3	0.04%	http://www.google.com/
12	3	0.04%	https://www.google.com/
13	2	0.02%	https://ra[redacted]09.com/about/ppp272.html
14	2	0.02%	https://www.google.com
15	1	0.01%	http://admin@su[redacted]er.org
16	1	0.01%	http://su[redacted].co.uk/In[redacted]in.html
17	1	0.01%	http://www.su[redacted]en.co.uk/
18	1	0.01%	http://www.su[redacted]en.co.uk/Contacts.htm
19	1	0.01%	https://ra[redacted]09.com/about/www385.html
20	1	0.01%	https://su[redacted]er.org/
21	1	0.01%	https://www.google.com.au
22	1	0.01%	https://www.google.com.sg

`hxxps[://][ORG_DOMAIN][.]com:2083/cpsess2128120117/tmp/[REDACTED]/webalizer/usage_202503[.]html`

I try to find some information about the first domain – `hxxps[://][REDACTED][.]com`. Preliminary research shows the domain to have been registered in March 2025 in the US, and it appears to be an events website:



I use a virtual machine to visit the website, and find it has been suspended.



`hxxps[://][REDACTED][.]com/cgi-sys/suspendedpage[.]cgi`

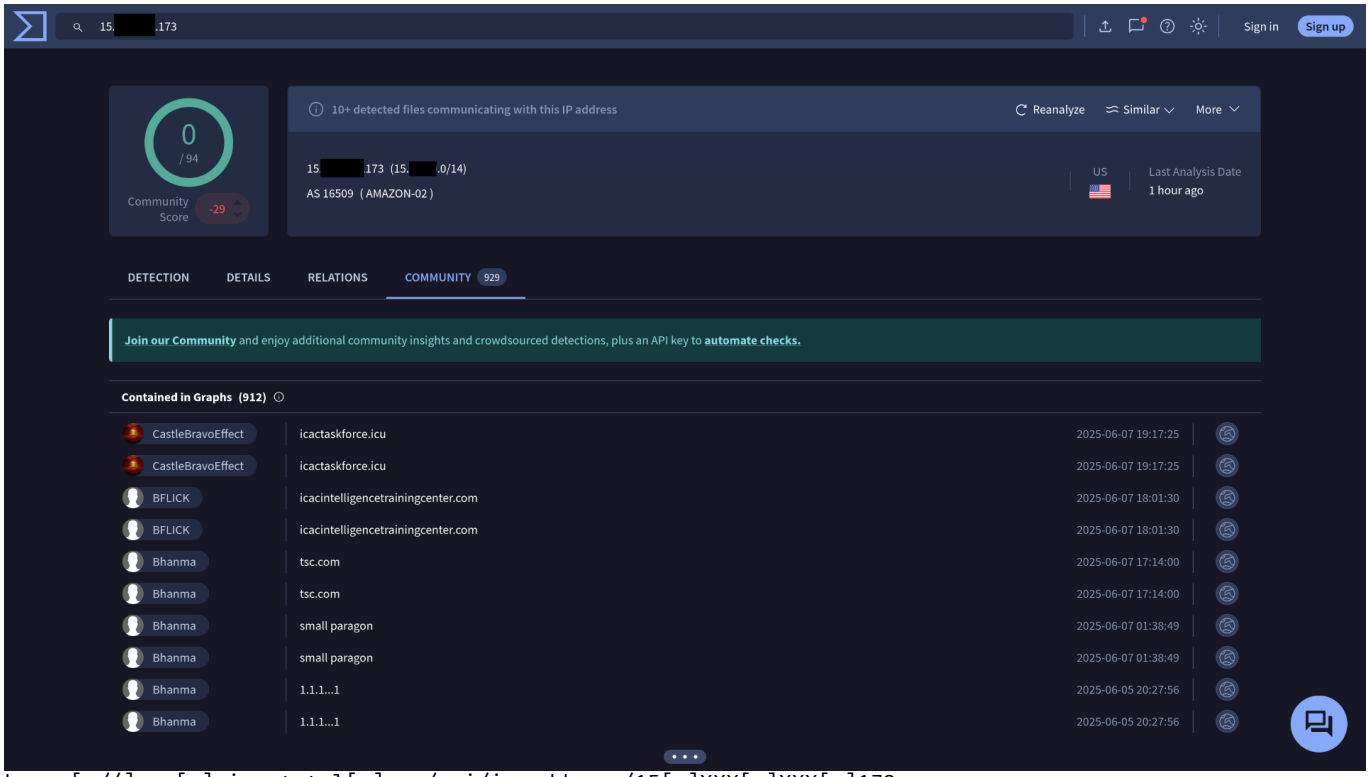
Top 18 of 18 Total Referrers

#	Hits		Referrer
1	8354	98.93%	- (Direct Request)
2	41	0.49%	http://su[redacted]er.org
3	16	0.19%	http://www.su[redacted]en.co.uk/
4	11	0.13%	http://su[redacted]er.org/
5	4	0.05%	http://www.su[redacted]en.co.uk/Se[redacted]es/We[redacted]gs.htm
6	3	0.04%	http://pa[redacted]st.blogspot.com/
7	3	0.04%	http://www.or[redacted]ls.com/1/past1101.php
8	2	0.02%	http://www.google.com/
9	1	0.01%	http://15.[redacted].173:80
10	1	0.01%	http://su[redacted]ce.blogspot.com/
11	1	0.01%	http://www.su[redacted]en.co.uk/[redacted].html
12	1	0.01%	https://duckduckgo.com/
13	1	0.01%	https://search.yahoo.com/
14	1	0.01%	https://www.google.co.uk/
15	1	0.01%	https://www.google.com
16	1	0.01%	https://www.google.com.au
17	1	0.01%	https://www.google.com/url
18	1	0.01%	su[redacted]er.org

hxxps[://][ORG_DOMAIN][.]com:2083/cpsess2128120117/tmp/[REDACTED]/webalizer/usage_202408[.]html

I check the next suspicious domain – hxxp[.]15[.]XXX[.]XXX[.]173

virustotal[.]com doesn't identify this IP address as malicious, but the "community" section of virustotal[.]com does. There are 176.4k files communicating with this address, and multiple community records of malicious behaviour. The IP is based in Seattle, US and it was registered in 2011.



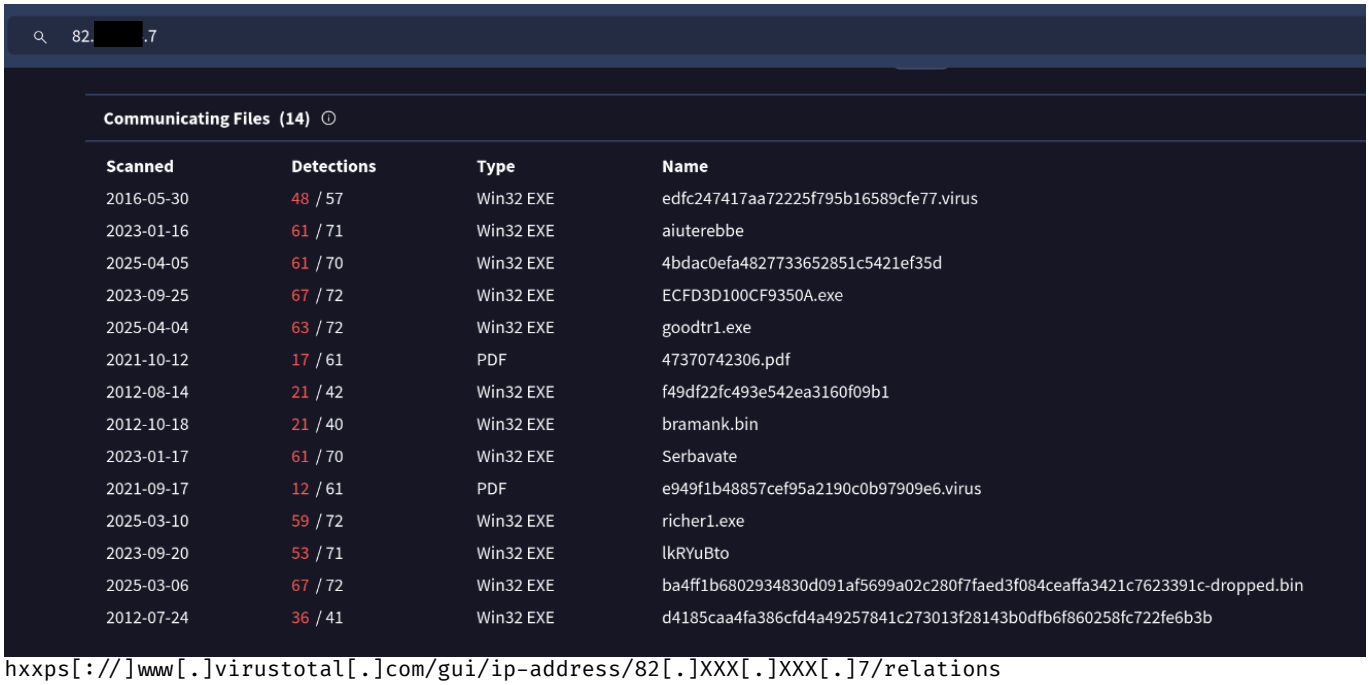
hxxps[://]www[.]virustotal[.]com/gui/ip-address/15[.]XXX[.]XXX[.]173

I decide to check various sources for our hosting IP address, to evaluate any potential external damage:

hxxps[://]www[.]abuseipdb[.]com/check/82[.]XXX[.]XXX[.]7

abuseipdb[.]com shows our shared IP address has been previously reported for spam in January 2024.

Additionally, virustotal[.]com shows that there are 14 malicious files identified as communicating with our host IP address – some scanned as recently as April 2025.
This is concerning behaviour, and potentially suggests the website's IP address is part of malware infrastructure – either the website, IP address or the server is being used as part of a wider attack.



Scanned	Detections	Type	Name
2016-05-30	48 / 57	Win32 EXE	edfc247417aa72225f795b16589cfe77.virus
2023-01-16	61 / 71	Win32 EXE	aiuterebbe
2025-04-05	61 / 70	Win32 EXE	4bdac0efa4827733652851c5421ef35d
2023-09-25	67 / 72	Win32 EXE	ECFD3D100CF9350A.exe
2025-04-04	63 / 72	Win32 EXE	goodtr1.exe
2021-10-12	17 / 61	PDF	47370742306.pdf
2012-08-14	21 / 42	Win32 EXE	f49df22fc493e542ea3160f09b1
2012-10-18	21 / 40	Win32 EXE	bramank.bin
2023-01-17	61 / 70	Win32 EXE	Serbavate
2021-09-17	12 / 61	PDF	e949f1b48857cef95a2190c0b97909e6.virus
2025-03-10	59 / 72	Win32 EXE	richer1.exe
2023-09-20	53 / 71	Win32 EXE	lkRYuBto
2025-03-06	67 / 72	Win32 EXE	ba4ff1b6802934830d091af5699a02c280f7faed3f084ceaffa3421c7623391c-dropped.bin
2012-07-24	36 / 41	Win32 EXE	d4185caa4fa386cfd4a49257841c273013f28143b0dfb6f860258fc722fe6b3b

hxxps[://]www[.]virustotal[.]com/gui/ip-address/82[.]XXX[.]XXX[.]7/relations

Each listed file has contacted our shared IP address when sandboxed and studied by virustotal[.]com.

Miscellaneous:

- The WordPress databases for [ORG_DOMAIN][.]com are empty.
- There is no evidence to suggest that any emails have been sent or accessed by an attacker.

Conclusion:

- My initial analysis is that [ORG_DOMAIN][.]com is being used as a hosting platform for malicious, criminal activities.

- There is no protection being used to defend [ORG_DOMAIN][.]com against attacks, either free or paid for.

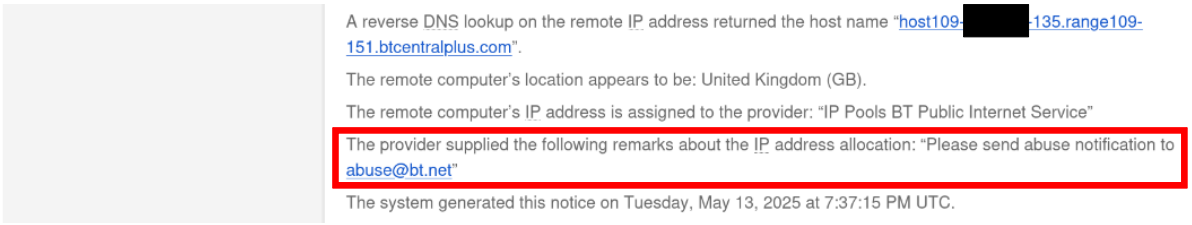
- Without mitigation, these attacks may persist indefinitely, leading to both legal and ethical implications.

- The extent of damage is unknown, but the possibilities for abuse are numerous – and the important thing is to notify the complete chain of those affected. The account has definitely been compromised.

Suggestions (in no particular order):

- The next steps are a suggested courtesy, and also provide practical steps to avoid a similar scenario happening in the future.

(1) Comply with BT's request – send an email to let them know the IP address (109[.]XXX[.]XXX[.]135**)** and detail of how their network has been abused on this occasion (see: Attempt 2 – 13 May 2025 – 19:37:15 UTC).


A reverse DNS lookup on the remote IP address returned the host name "host109-[redacted]-135.range109-151.btcentralplus.com".

The remote computer's location appears to be: United Kingdom (GB).

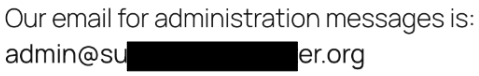
The remote computer's IP address is assigned to the provider: "IP Pools BT Public Internet Service"

The provider supplied the following remarks about the IP address allocation: "Please send abuse notification to abuse@bt.net"

The system generated this notice on Tuesday, May 13, 2025 at 7:37:15 PM UTC.

(2) Inform [HOSTING_DOMAIN][.]co[.]uk of suspicious activity on your [ORG_DOMAIN][.]com user account.

(3) Remove administration email address information from the [ORG_DOMAIN][.]com "**Contact us**" page:


Our email for administration messages is:
admin@su[redacted]er.org

(4) Ensure all [ORG_DOMAIN][.]com user account passwords are changed, with appropriate length and complexity, and stored securely.

(5) Ensure all [ORG_DOMAIN][.]com user account email addresses are changed and stored securely.

(6) Remove full [ORG_DOMAIN][.]com author details – use an alias or derivatives of your actual name and credentials.

(7) Search for and remove any unknown credentials on [ORG_DOMAIN][.]com and [ORG_DOMAIN][.][HOSTING_DOMAIN][.]co[.]uk

(8) Keep an eye on account login activity, and stay proactive in protecting data and credentials to the best of your ability.

(9) Remove the sitemap from your `robots.txt`, and consider blocking some crawlers from accessing your website to reduce bandwidth usage.

(10) As part of due diligence and data protection responsibilities, consider requesting clarification about the server environment hosting `[ORG_DOMAIN][.]com` to confirm that the operating system and hosting software are regularly patched against known vulnerabilities.

(11) Consider requesting a different IP address if possible – if not, consider migrating `[ORG_DOMAIN][.]com` to a more reliable, secure hosting provider.

Prepared by: Kit S.
Date: 13 June 2025