Incident Report: Suspicious Login Activity and Potential 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 using ports not officially assigned by the IANA. The credentials used appear to be associated with a compromised account tied to [ORG_DOMAIN].com. While there is no indication of direct website tampering, patterns observed suggest potential reconnaissance and credential abuse via exposed administrative information in the website’s source code. 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[.]132[.]xxx[.]xx	109[.]151[.]xxx[.]xxx	82[.]132[.]xxx[.]x
Location	Edinburgh, Scotland, UK	Eyemouth, Scotland, UK	Abererch, Wales, UK
Port Used	61188 (unusual, not IANA-assigned)	46086 (unusual, not IANA-assigned)	23259 (unusual not IANA-assigned)
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 [REDACTED]@[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 ([REDACTED])

Suspicious Web Activity:

- Website cache timestamp aligns closely with the first suspicious login.
- Sitemap update corresponds to a legitimate content change ("What's On" page).
- robots[.]txt and sitemap XML are accessible and provide full indexing instructions.

Analysis:

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

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

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

Potential Objectives

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

Recommendations:

1. **Notify Affected Parties:**
- Inform BT about potential misuse of IP 109[.]151[.]XXX[.]XXX.
- Alert myzen[.]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`:

```
User-agent: *
Disallow: /
```

- Replace author names with aliases.

4. **Monitoring & Response:**
- Audit login activity across domains.
- Search for unauthorized credentials or accounts.
- Monitor for further suspicious access or page updates.

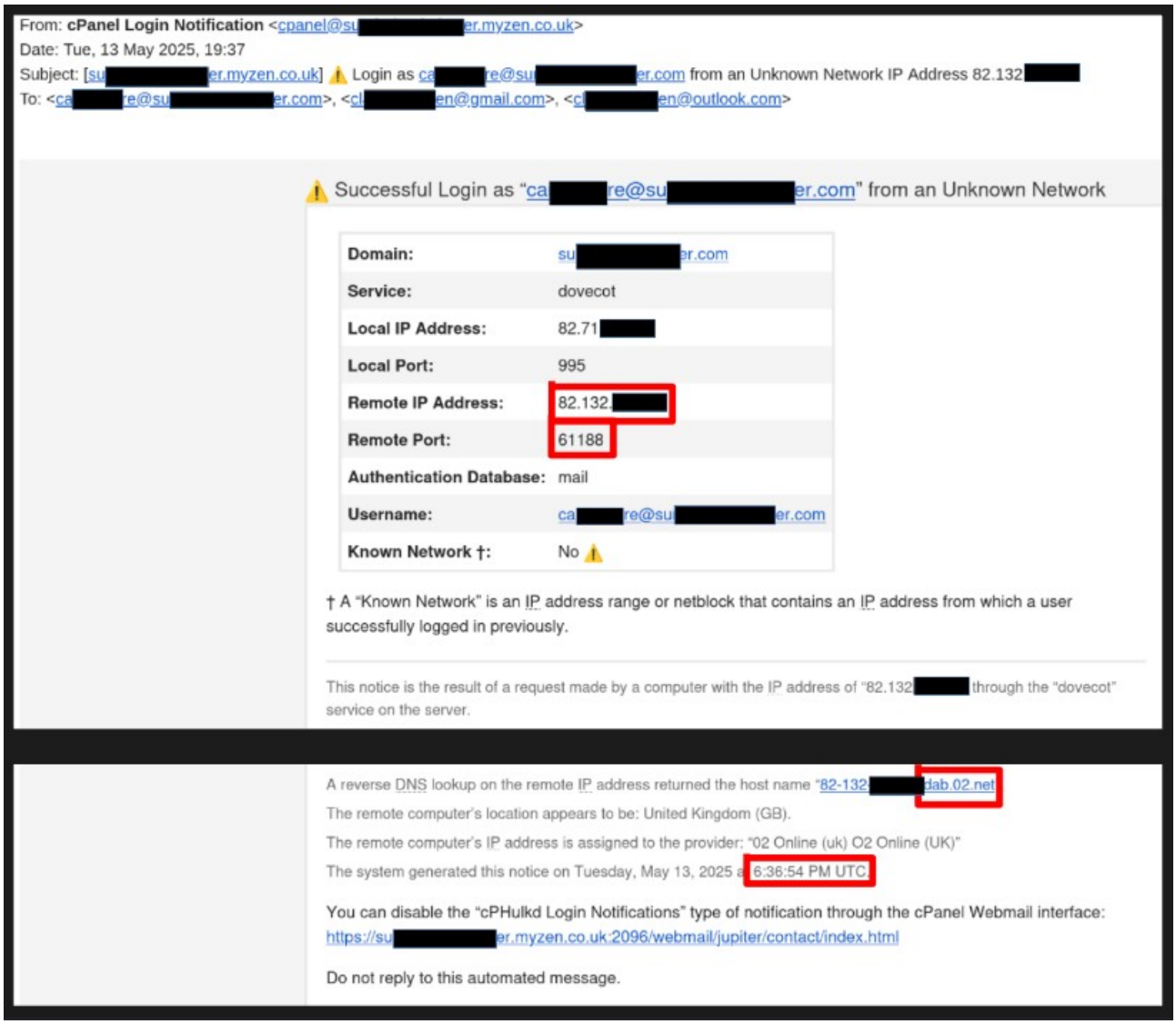
Conclusion

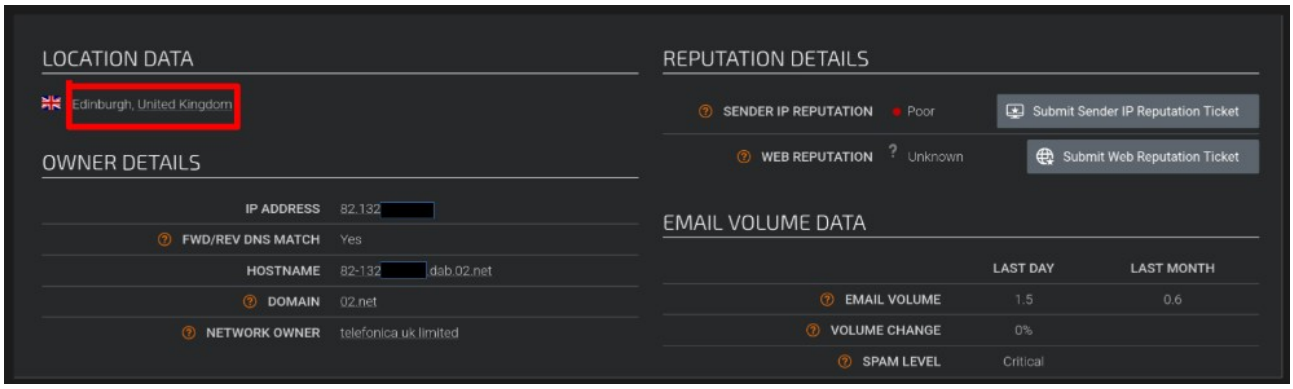
Although the attacker's goals remain unclear, the pattern of access, obscure ports, and sourcing of sensitive data from public code suggest a deliberate attempt to compromise or impersonate administrative functions of `[ORG_DOMAIN].com`. No direct compromise has been confirmed, but the account should be considered exposed and treated accordingly.

Prepared by: Kit S.
Date: 20 May 2025

Incident Write-up: Suspicious Login Activity and Potential Compromise

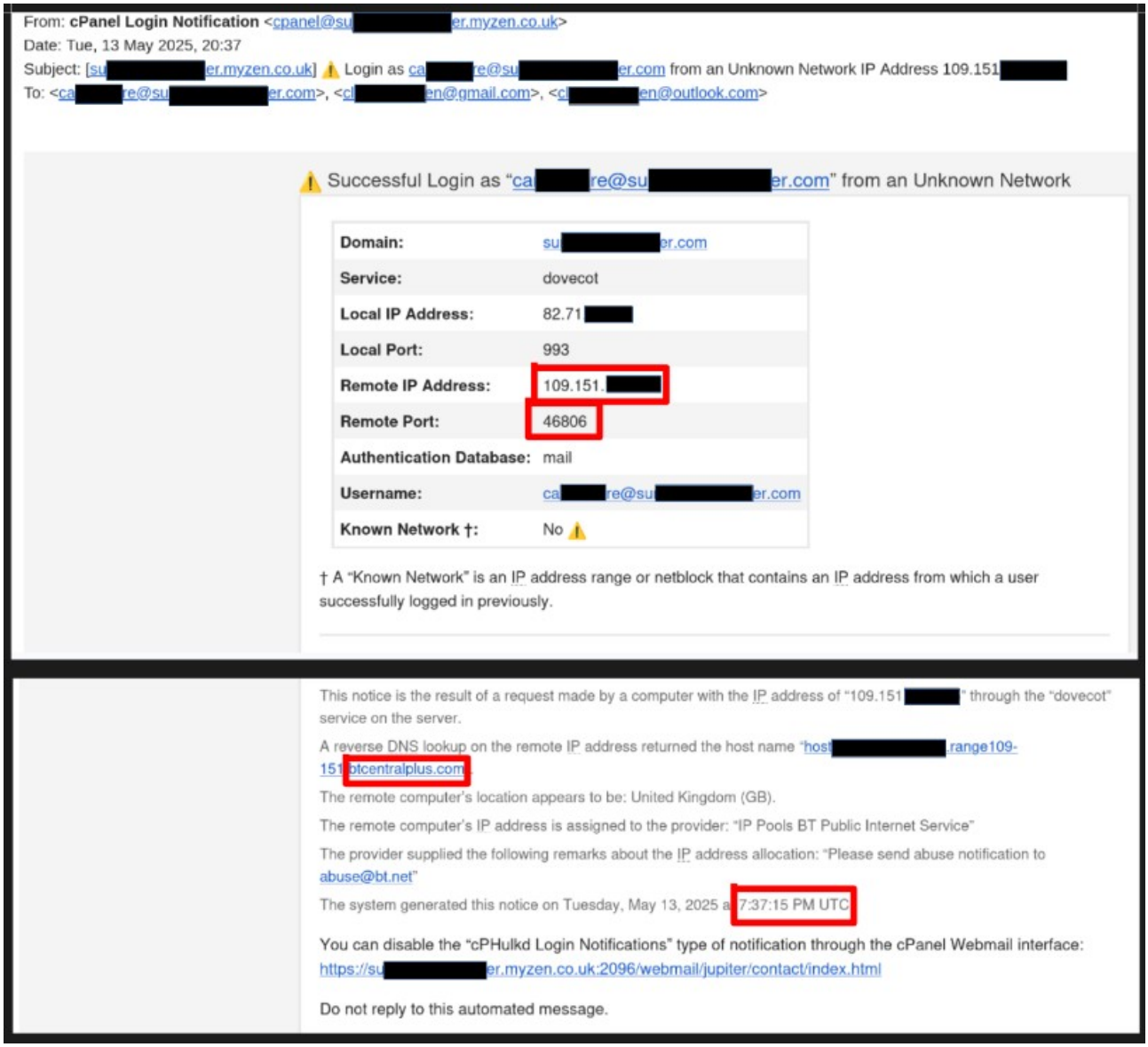
Attempt 1
13 May 2025 – 18:36:54 UTC





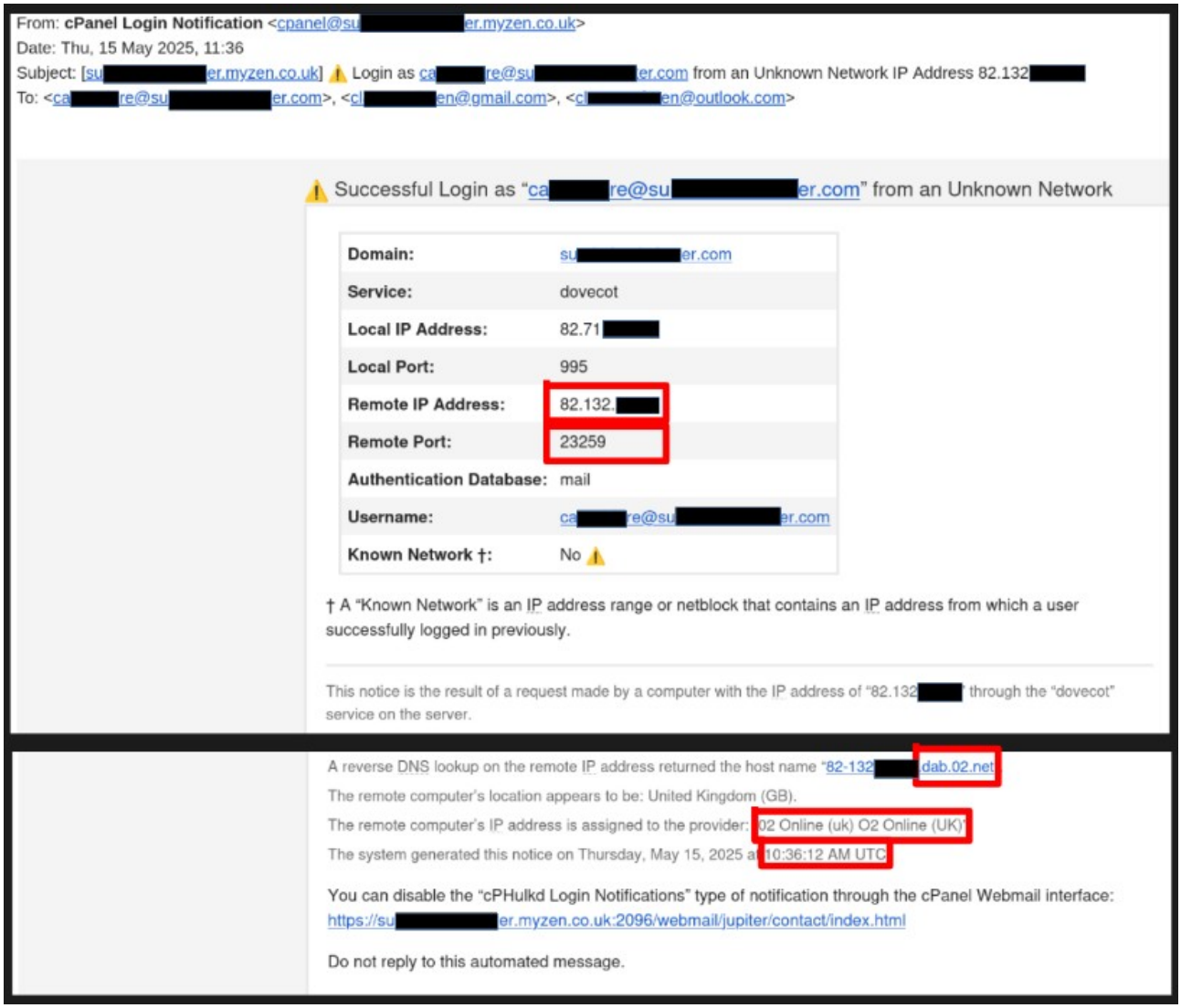
- Successful login from Edinburgh, Scotland, UK.
- Use of port 61188 is unusual, and not officially assigned by the IANA (Internet Assigned Numbers Authority).
- `dab[.]02[.]net` is associated with O2's mobile data network.

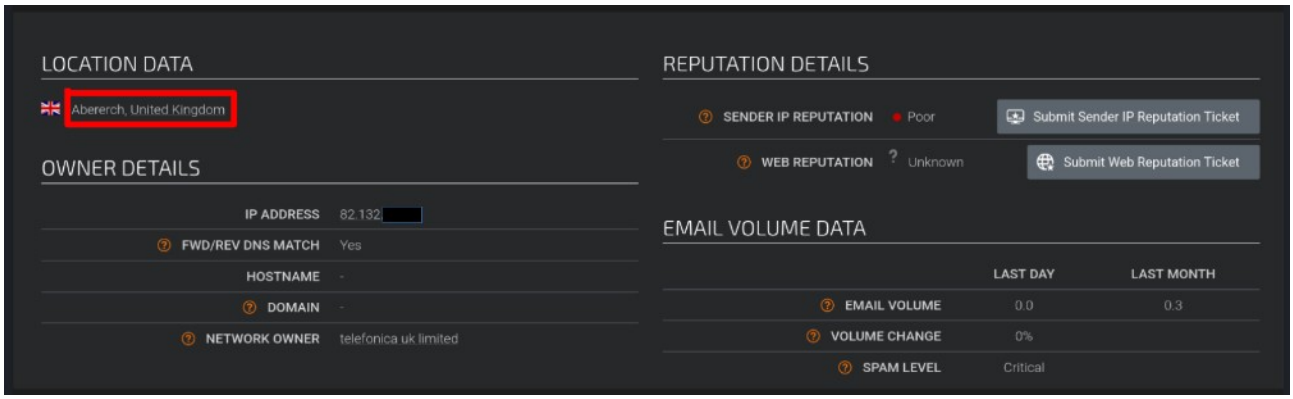
Attempt 2
13 May 2025 – 19:37:15 UTC



- Successful login from Eyemouth, Scotland, UK.
- Use of port 46086 is also unusual, and not officially assigned by the IANA (Internet Assigned Numbers Authority).
- `btcentralplus[.]com` primarily serves home broadband users.

Attempt 3
15 May 2025 – 10:36:12 UTC





- Successful login from Abererch, Wales, UK.
- Use of port 23259 is, again, unusual, and not officially assigned by the IANA (Internet Assigned Numbers Authority).
- `dab[.]02[.]net` is associated with O2's mobile data network.

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:

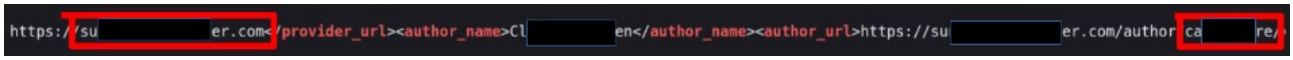
hxxps[://][ORG_DOMAIN][.]com/contact-us/#

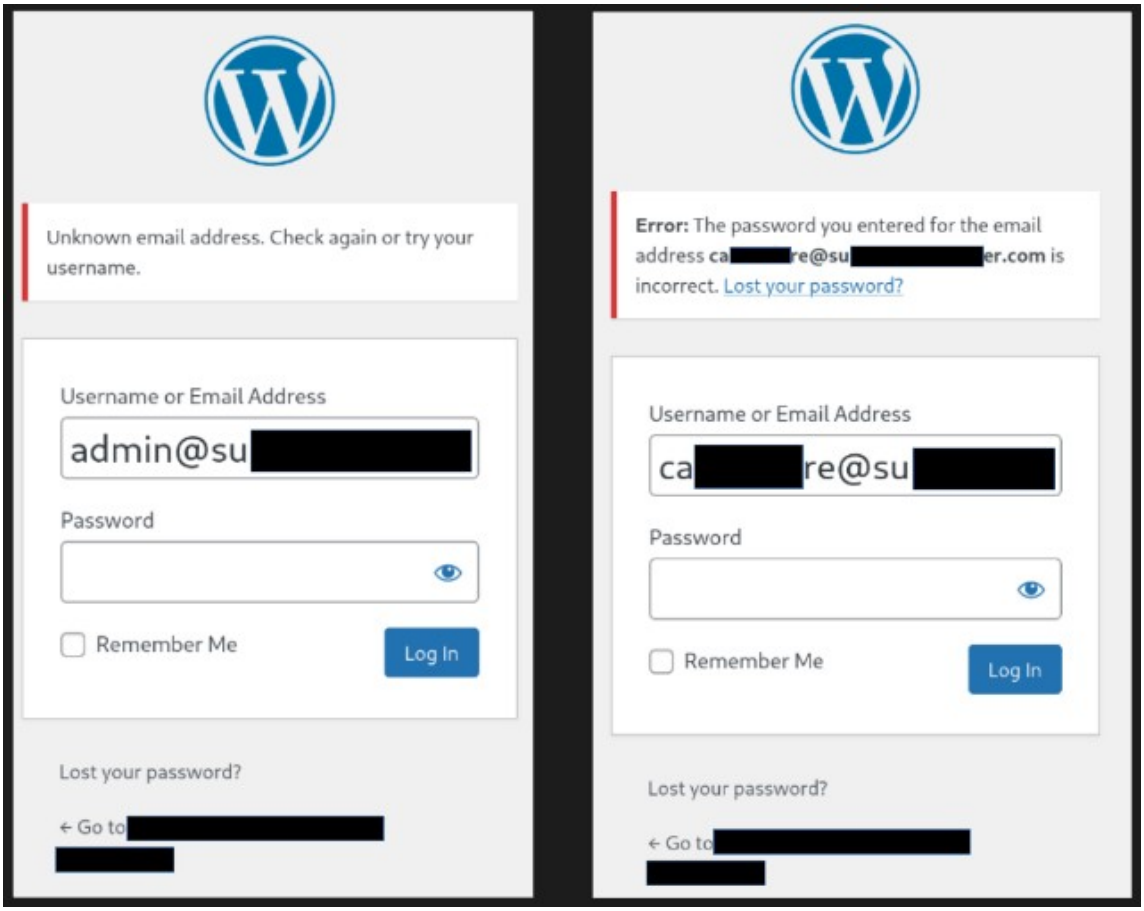
Information found using Burpsuite:

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

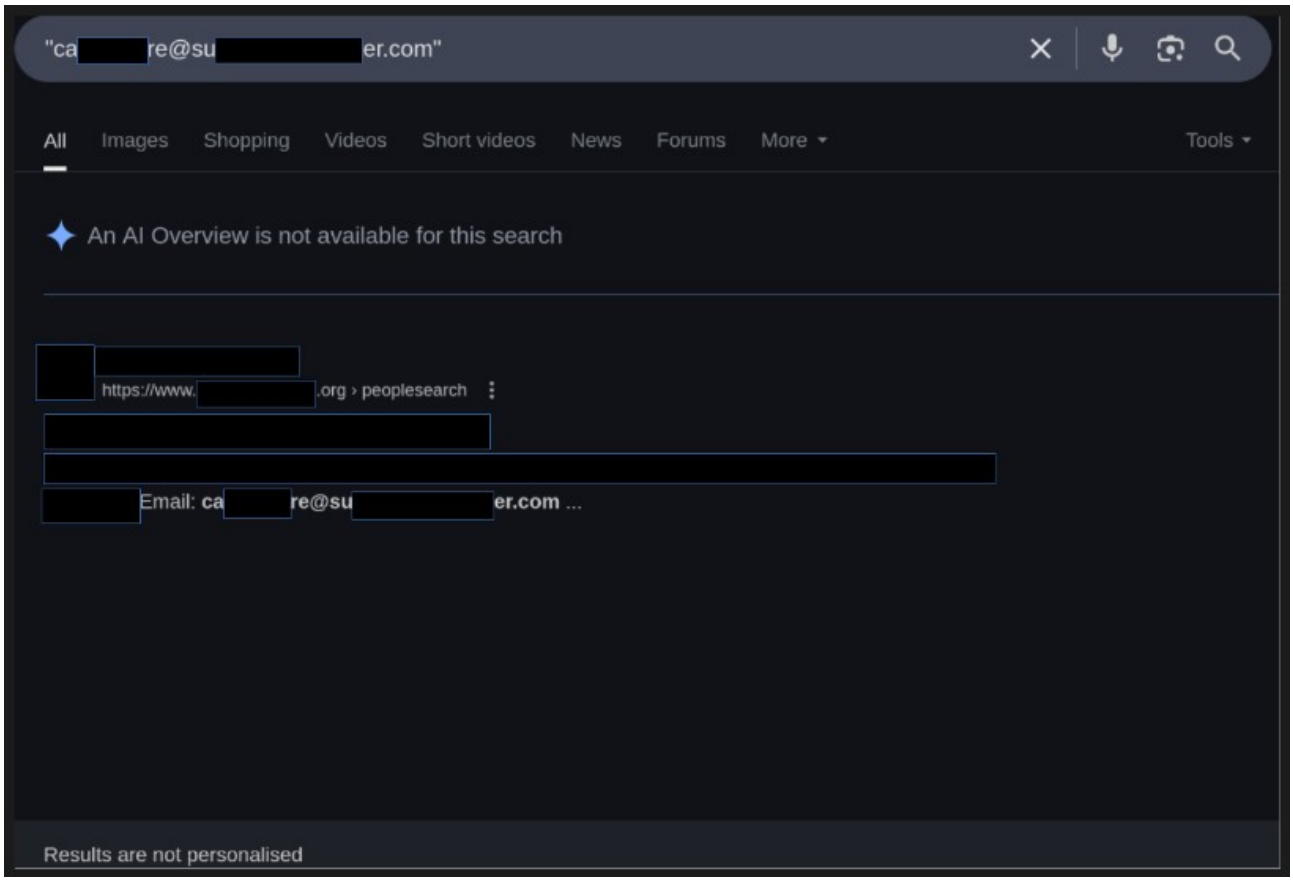
Proof of concept:

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





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



Or the employer's [REDACTED] website:

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

Both of these options seem targeted and personal, and there is no public evidence that the 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.

Web Crawlers:

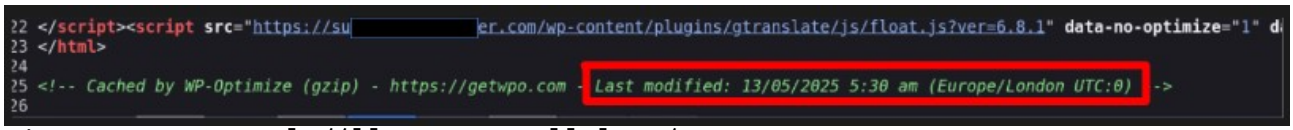
Some malicious bots will systematically browse and index the content of websites across the internet, scanning source codes and using the information from one website to log into another. They can then brute-force the password using wordlists (a collection of known passwords that have been previously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

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

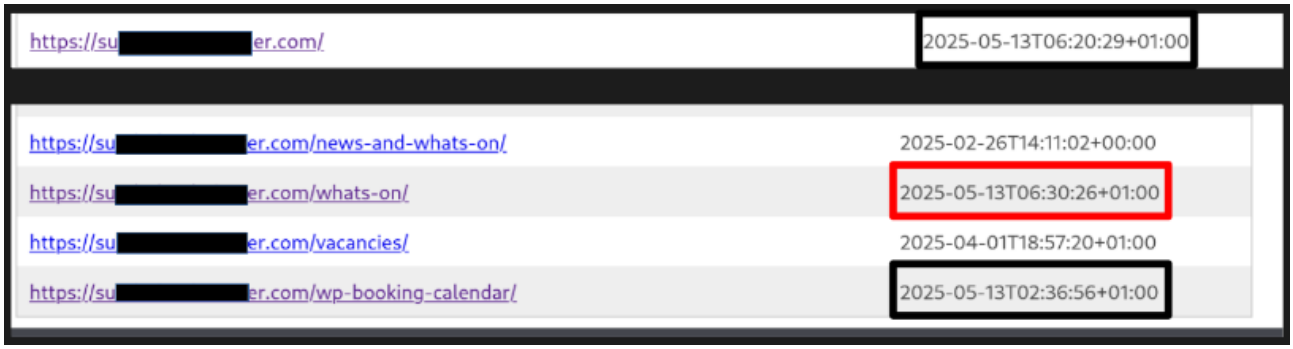
Explanation:

- Following the sitemap leads to a completely innocuous update to the website's "What's On" page, updated at 6:30:26 am GMT – 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/

Conclusion:

- My initial thought is that the goal may be an attempt to compromise myzen[.]co[.]uk using third-party, less secure credentials to gain initial access. Once they have access to a server, a talented hacker can move through the network and do what they want to/with it.

- Another possibility is that someone could be trying to impersonate an official [ORG_DOMAIN][.]com email address for nefarious reasons, or access data using authorised credentials.

- 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, but there is nothing to suggest that anything on the website has been directly affected, or that the account credentials have been leaked.

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[.]151[.]XXX[.]XXX**)** and detail of how their network has been abused on this occasion (see: Attempt 2 – 13 May 2025 – 19:37:15 UTC).

(2) Inform myzen of suspicious activity on your [ORG_DOMAIN][.]com user account – dnsmaster[@]zen[.]co[.]uk**.**

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

(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][.]myzen[.]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 all crawlers from accessing your entire website:

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

```
User-agent: *
Disallow: /
```

Prepared by: Kit S.
Date: 20 May 2025