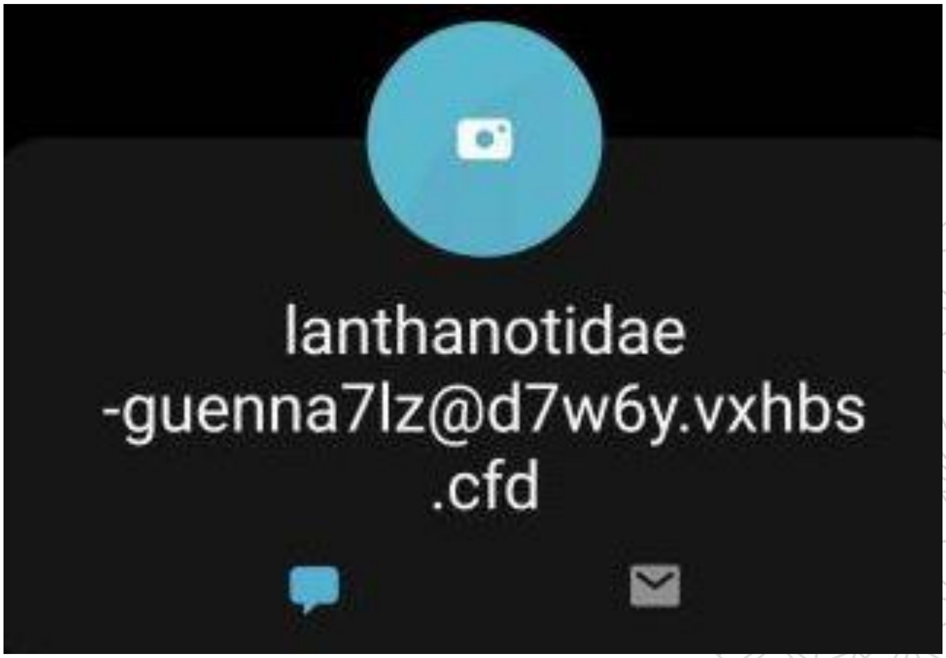
USPS Squatting Campaign

Domain: **vxhbs[.]cfd**

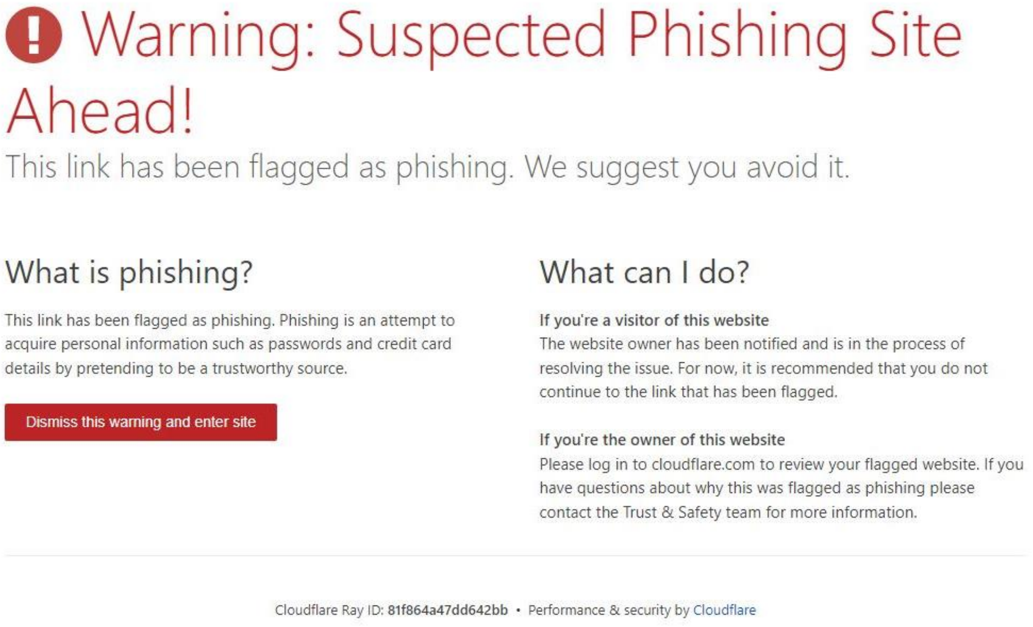
1. Email Sender Details:

- **Domain:** vxhbs[.]cfd
  - Flagged as a phishing website.
  - Displays a Cloudflare banner indicating it is a phishing website.



lanthanotidae
-guenna7lz@d7w6y.vxhbs
.cfd

- **IP Address:** 104.21.91.185 (Cloudflare Load Balancer).



Warning: Suspected Phishing Site Ahead!

This link has been flagged as phishing. We suggest you avoid it.

What is phishing?

This link has been flagged as phishing. Phishing is an attempt to acquire personal information such as passwords and credit card details by pretending to be a trustworthy source.

What can I do?

If you're a visitor of this website
The website owner has been notified and is in the process of resolving the issue. For now, it is recommended that you do not continue to the link that has been flagged.

If you're the owner of this website
Please log in to cloudflare.com to review your flagged website. If you have questions about why this was flagged as phishing please contact the Trust & Safety team for more information.

Cloudflare Ray ID: **81f864a47dd642bb** • Performance & security by Cloudflare

2. Phishing Message Content:

- **Sender Claim:** USPS package delivery notification.
- **Message:** A package needs to be updated with the correct delivery address to avoid being returned to the sender.
- **Action Requested:** Update the delivery address via the provided link.

The message was sent to a phone with the following message

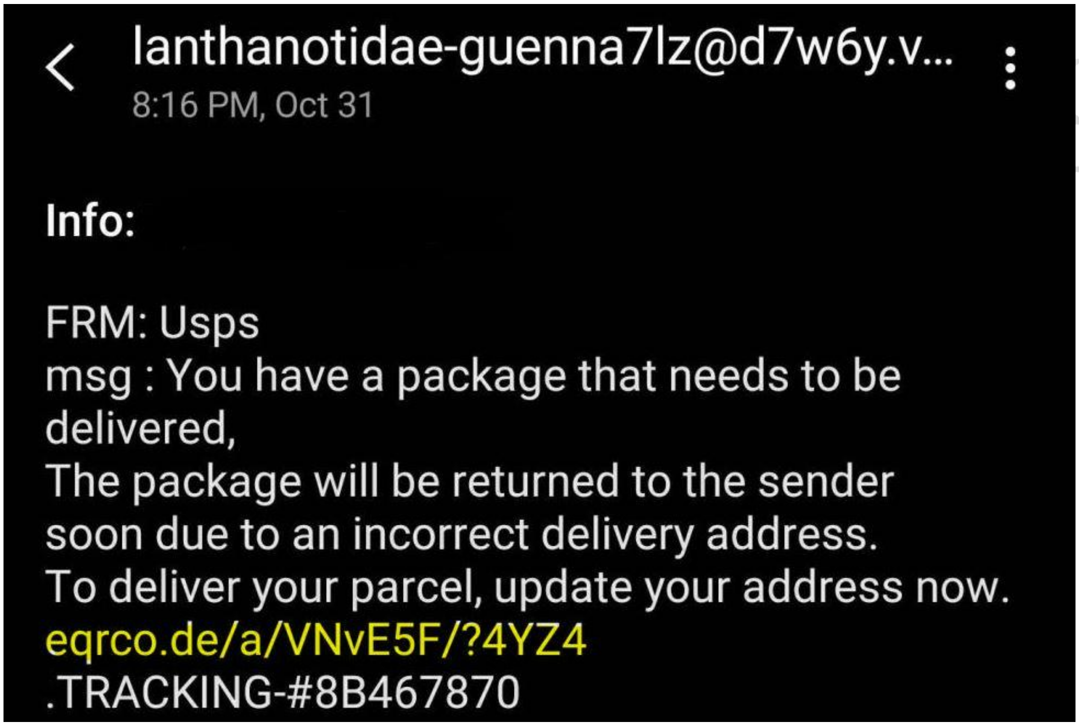
"<SMS -9353-9Y88L>

FROM Usps
Msg: You have a package that needs to be delivered, the package will be returned to the sender soon due to an incorrect delivery address.

To deliver your parcel, update your address now.

Eqrco[.]de/a/VNvE5F/?4YZ4

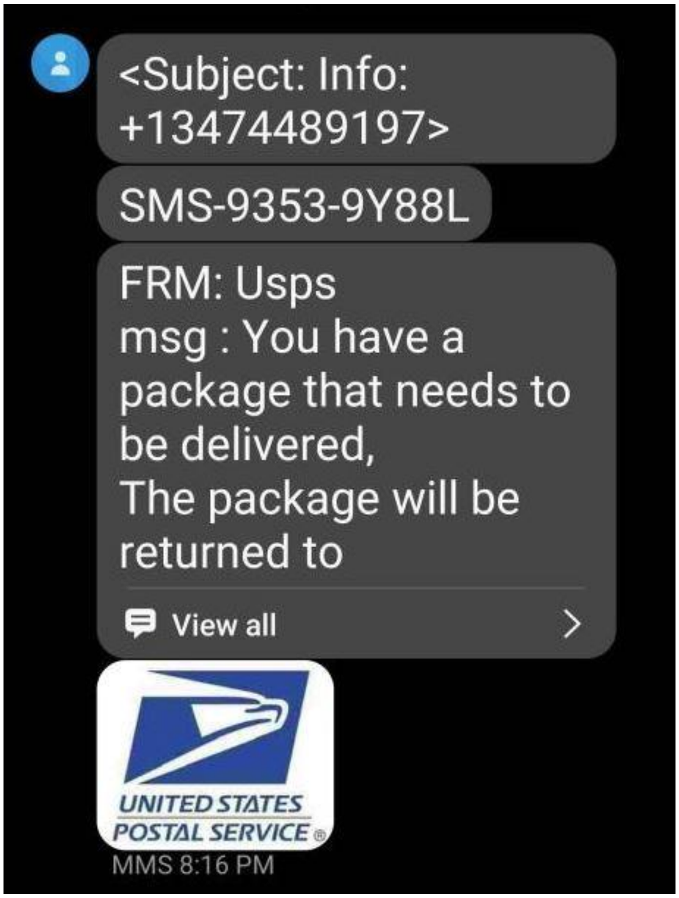
.TRACKING-#8B467870"



lanthanotidae-guenna7lz@d7w6y.v...
8:16 PM, Oct 31

Info:

FRM: Usps
msg : You have a package that needs to be delivered,
The package will be returned to the sender soon due to an incorrect delivery address.
To deliver your parcel, update your address now.
eqrco.de/a/VNvE5F/?4YZ4
.TRACKING-#8B467870



<Subject: Info:
+13474489197>

SMS-9353-9Y88L

FRM: Usps
msg : You have a
package that needs to
be delivered,
The package will be
returned to

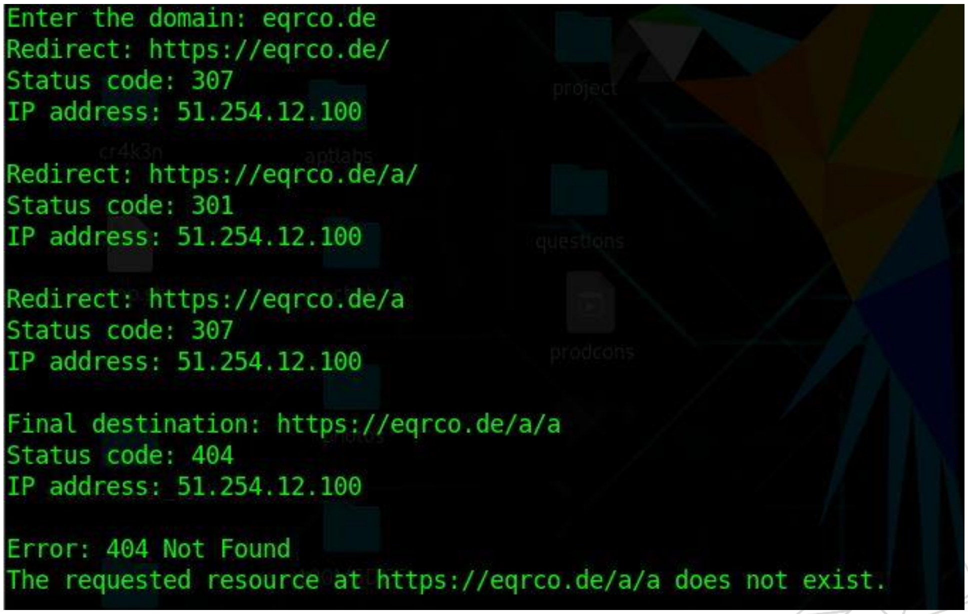
MMS 8:16 PM

3. Forensic Linguistic Analysis:

- The use of the word "parcel" suggests that the author may not be from the United States but rather from a region where British English is prevalent, such as Europe, Asia, or the Middle East.

4. Payload and Host Information:

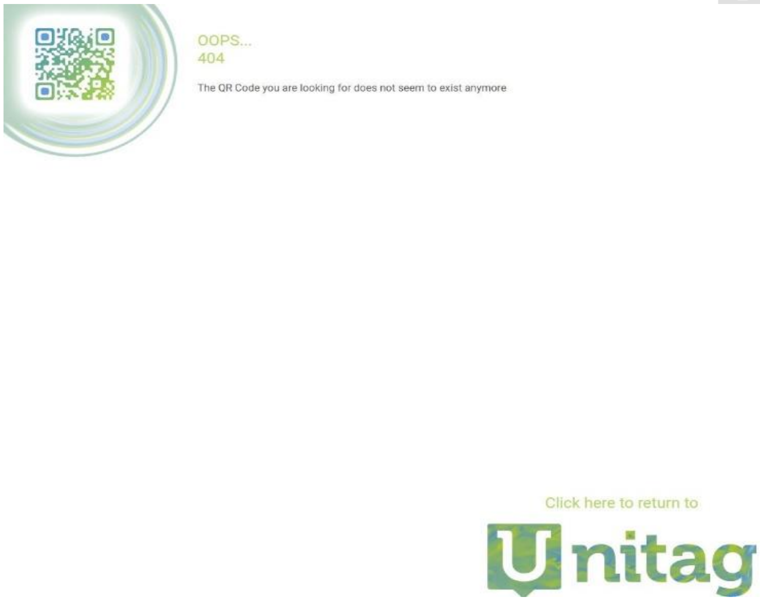
- **Payload Link:** `eqrco[.]de/a/VNvE5F/?4YZ4`
  - Shortened URL with a status code of `301 Permanent Redirect`.
- **Redirect Behavior:**
  - Several redirects with a status code of `301 Permanent Redirect` or `307 Temporary Redirect`.
  - Final destination URL: `https://eqrco[.]de/a/a` with a status code of `404 Not Found`.



```
Enter the domain: eqrco.de
Redirect: https://eqrco.de/
Status code: 307
IP address: 51.254.12.100

Redirect: https://eqrco.de/a/
Status code: 301
IP address: 51.254.12.100

Redirect: https://eqrco.de/a
Status code: 307
IP address: 51.254.12.100

Final destination: https://eqrco.de/a/a
Status code: 404
IP address: 51.254.12.100

Error: 404 Not Found
The requested resource at https://eqrco.de/a/a does not exist.
```

5. Host and Redirect Link Details:

- **Host IP:** `51.254.12[.]100`
  - Flagged as a phishing domain.
  - Associated with multiple redirect statuses, including `301`, `307`, and a final `404 Not Found`.
- **Final Landing Page Message:** "OOP.. 404 the QR Code you are looking for does not seem to exist anymore."



OOPS...
404

The QR Code you are looking for does not seem to exist anymore

Click here to return to

6. Additional Host Information:

- The IP `34.133.40[.]248` is flagged as malicious and for phishing activities.
    - **Host Provider:** Google
    - **Status Code:** `404 Not Found`

7. Reference Topic:

- Smishing (SMS phishing) related to package tracking text scams.

Additional Notes:

- **Wayback Machine Evidence:** The automatic download of an empty file from `vxhbs.cfd` suggests a technique commonly used by malicious actors to either implant malware or to test the deployment capabilities of their infrastructure for future attacks.

Resources:

Redirect script (the inspector)

https://github.com/TheKrakenIO/The_Inspector

Smishing: Package Tracking Text Scams

https://www.uspis.gov/news/scam-article/smishing-package-tracking-text-scams#:~:text=Have%20you%20received%20unsolicited%20mobile%20text%20messages%20indicating%20that%20a,is%20a%20scam%20called%20smishing.

Parcel word definition

https://www.wordreference.com/englishusage/parcel#:~:text=The%20two%20words%20have%20almost,used%20rather%20than%20'parcel'.