Anatomy of a Sophisticated Phishing Campaign:

The usps.otognluguws.top Case Study

Introduction:

In the ever-evolving landscape of cyber threats, a new sophisticated campaign has emerged, orchestrated through a malicious IP 43.252.172[.]35. This IP address has been implicated in an elaborate phishing scheme, targeting unsuspecting users with domain names crafted to mimic the United States Postal Service (USPS). This campaign, employing domain squatting tactics, leverages USPS's trust and widespread recognition to deceive individuals and potentially harvest sensitive personal information.

Content:

1. IP Profile and Status

A. IP Analytics

IP Address: 43.252.172[.]35

Creation Date: January 12, 2015

Update Date: March 05, 2017

Registrant: Dimension Network & Communication Limited

Country: Hong Kong

B. Open Ports and Services

Port 80: Running NGINX service (Open)

Port 443: Running NGINX service (Open)

Port 8888: Running NGINX service (Open)

C. Current Status

The IP is currently live and active.

2. Forward DNS Records

The IP is associated with numerous domains and subdomains that are variations on the legitimate USPS website. These are designed to deceive users into believing they are accessing official USPS services. The domains have a variety of subdomains, indicating a widespread squatting campaign.

A. Subdomains associated with the IP:

usps.wqbrjxizzhn.top
usps.ipkrhedanya.top
usps.fjmouodghvu.top
usps.hnwuxchpcvq.top
usps.rrdcdzdlbnz.top
usps.wyyyqoegsxh.top
usps.yriuezswutd.top
usps.otognluguws.top
usps.jpvqixkpmsu.top
usps.xoqkrnwwmib.top
usps.rcbzqwgvyzc.top
usps.aasypnhpnid.top
usps.dectckkfkrz.top
usps.sgddzhpotlv.top
usps.gpeytpzdswi.top

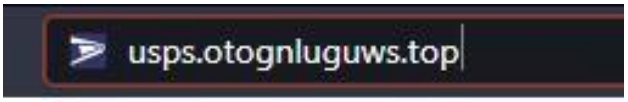
B. Domain life spam:

Domains	Created	Expires	Registrant Name	Status
usps.wqbrjxizzhn.top	2024-01-13	2025-01-13	Redacted	Active (nginx)
usps.ipkrhedanya.top	2024-01-13	2025-01-13	Redacted	Active (Redirect)
usps.fjmouodghvu.top	2024-01-13	2025-01-13	Redacted	Active (Redirect)
usps.hnwuxchpcvq.top	2024-01-13	2025-01-13	Redacted	Active (Redirect)
usps.rrdcdzdlbnz.top	2024-01-13	2025-01-13	Redacted	Active (Redirect)
usps.wyyyqoegsxh.top	2024-01-13	2025-01-13	Redacted	Active (Redirect)
usps.yriuezswutd.top	2024-01-13	2025-01-13	Redacted	Active (Redirect)
usps.otognluguws.top	2024-01-13	2025-01-13	Redacted	Active (Temporary)
usps.jpvqixkpmsu.top	2024-01-13	2025-01-13	Redacted	Active (Redirect)

usps.xoqkrnwwmib.top	2024-01-13	2025-01-13	Redacted	Active (Redirect)
usps.rcbzqwgvyzc.top	2024-01-13	2025-01-13	Redacted	Active (Redirect)
usps.aasypnhpnid.top	2024-01-13	2025-01-13	Redacted	Active (Redirect)
usps.dectckkfkrz.top	2024-01-13	2025-01-13	Redacted	Active (Redirect)
usps.sgddzhpotlv.top	2024-01-13	2025-01-13	Redacted	Active (Redirect)
usps.gpeytpzdswi.top	2024-01-13	2025-01-13	Redacted	Time out

Note:

During the investigation, the domain usps.otognluguws.top was active and had the UPS phishing website running; after a few hours, the website became redirected to UPS's original page, and the favicon was still there as a prove that the scam was on process.



usps.otognluguws.top

C. Distinguished Domains

usps.otognluguws.top: This domain appears to have higher activity with directories flagged as malicious.

- usps.otognluguws.top /cc.php
- usps.otognluguws.top /wait2.php

3. Analysis of the IP

The IP **43.252.172[.]35** was caught hosting a malicious file:

- **Hash:** 251ecd1ac492fb7da375937888a5115e5271ed9f922ca5acdc28e012694507e9
- **Type:** "Unix.Trojan.Mirai-5607483-0" refers to a specific variant or signature of the Mirai Trojan, a type of malware that targets Unix systems. The breakdown of the components as following:
    - **Unix:** This indicates that the malware targets Unix-based systems. Unix-based systems include operating systems derived from the original Unix, with Linux being a well-known example.
    - **Trojan:** A Trojan is a type of malware that disguises itself as legitimate software. Unlike viruses, Trojans do not self-replicate. They are often used to create backdoors into systems or to deliver other types of malwares.
    - **Mirai:** Mirai is a well-known malware discovered around 2016. It primarily targets Internet of Things (IoT) devices like routers, cameras, and smart home devices. Mirai works by infecting these devices and turning them into a botnet, which can be used for various malicious activities, including large-scale Distributed Denial of Service (DDoS) attacks.
    - **5607483-0:** This is likely a specific signature ID used by a cybersecurity organization or antivirus program to identify this particular variant of the Mirai Trojan. Signature IDs allow security software to precisely identify and differentiate between various malware strains.

The Mirai malware gained notoriety for its role in some of the most significant and disruptive DDoS attacks. It's designed to scan the internet for IoT devices protected by factory default or hard-coded usernames and passwords, which users often do not change. Once it finds such a device, it infects and adds it to the botnet. The simplicity of the malware and the widespread vulnerability of IoT devices have made Mirai and its variants a significant threat in the cybersecurity landscape.

4. Analysis of the domain

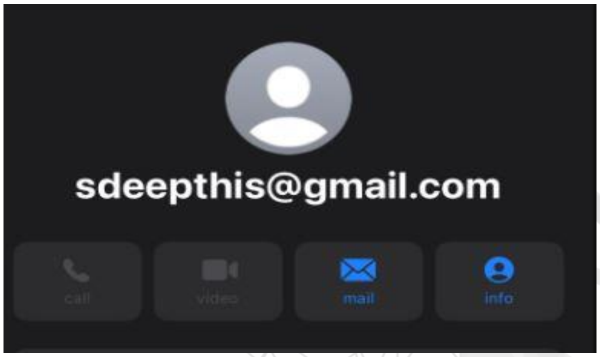
USPS.otognluguws.top was spotted in a smishing campaign from the sender email **sdeepthis@gmail.com** with the following message:

> "The USPS package has arrived at the warehouse and cannot be delivered due to incomplete address information. Please confirm your address in the link within 12 hours.
>
> http://usps.otognluguws.top
>
> (Please reply to Y, then exit the SMS, open the SMS activation link again, or copy the link to Safari browser and open it)
>
> The US Postal team wishes you a wonderful day."

The email address: **sdeepthis@gmail.com**

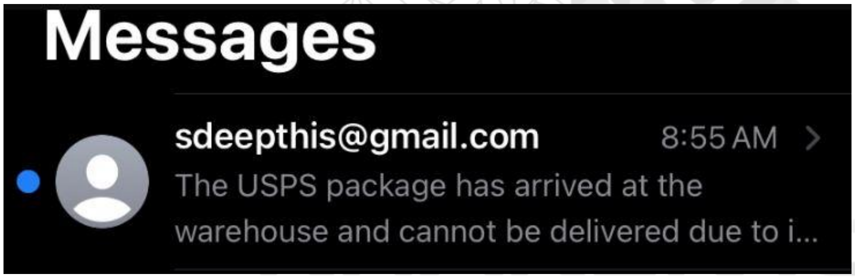
- first_seen: 05/05/2012
- last_seen: 01/25/2023

The email was spot on carrd.co. A free website use to create one-page websites, which indicate that the threat actors are actively using various tools to deliver their scam.



sdeepthis@gmail.com

Figure 1: The sender's information.

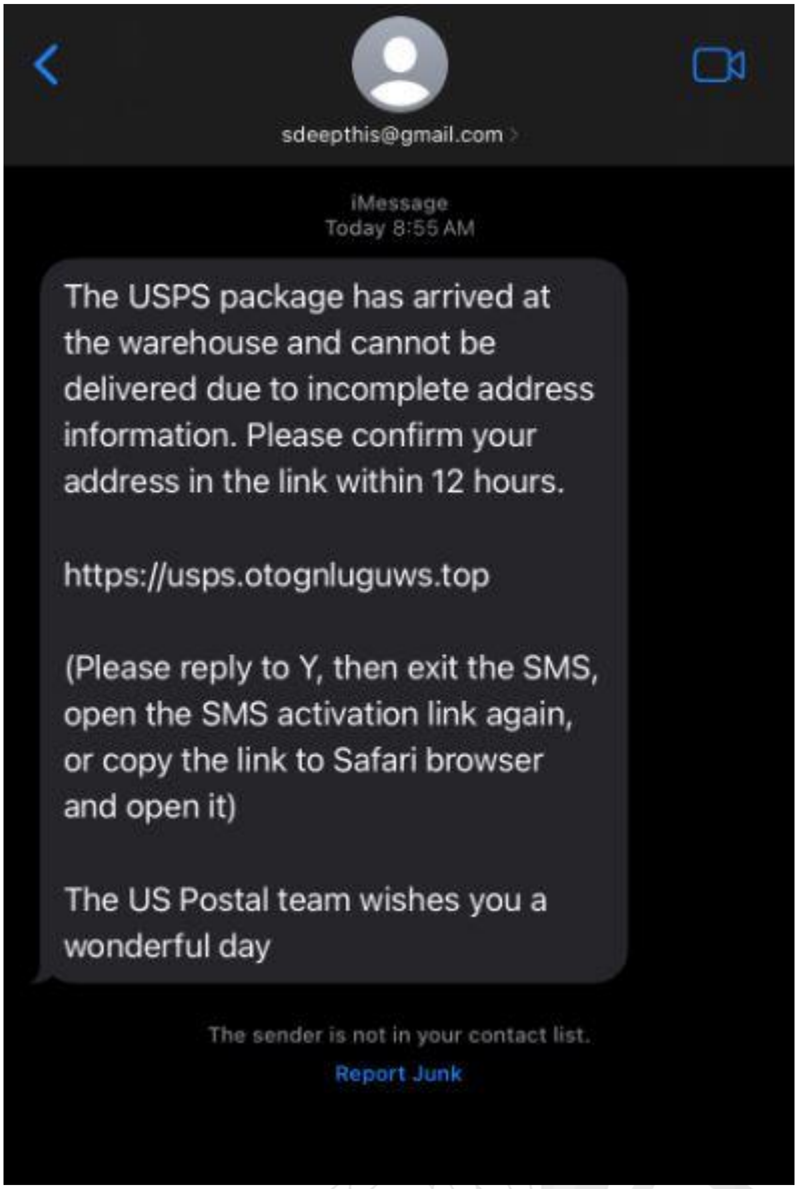


Messages

sdeepthis@gmail.com 8:55 AM

The USPS package has arrived at the warehouse and cannot be delivered due to i...

Figure 2: The smishing text message



The USPS package has arrived at the warehouse and cannot be delivered due to incomplete address information. Please confirm your address in the link within 12 hours.

https://usps.otognluguws.top

(Please reply to Y, then exit the SMS, open the SMS activation link again, or copy the link to Safari browser and open it)

The US Postal team wishes you a wonderful day

Figure 3: The smishing message content

5. Conclusion

The usps.otognluguws.top attack epitomizes a sophisticated, multi-layered cyber threat, seamlessly blending the deceptive allure of phishing with the intricate dangers of malware distribution. This attack is a standalone event, and a stark reminder of the evolving cyber threats organizations and individuals face today. It underscores the need for a vigilant, informed, and adaptive approach to cybersecurity.

In responding to such threats, the emphasis must be on a holistic strategy that combines robust technical defenses with proactive user education. The technical measures should include advanced email filtering, regular updates to security protocols, and rigorous network monitoring to detect and neutralize threats early. However, technical solutions alone are not sufficient. There must be a concerted effort to enhance user awareness, as human error often remains the weakest link in cybersecurity.

Furthermore, this case highlights the essential role of international cooperation in combating cyber threats. Cybercriminals exploit the internet's borderless nature, necessitating a response transcending national boundaries. This requires collaboration among law enforcement agencies, private sector entities, and cybersecurity communities worldwide.

Lastly, the usps.otognluguws.top attack serves as a call to action for continuous improvement and adaptation in cybersecurity practices. As attackers evolve their tactics, so too must our defenses. This includes staying abreast of the latest cyber threat intelligence, investing in emerging security technologies, and fostering a culture of cybersecurity resilience.

In conclusion, the usps.otognluguws.top attack is a complex challenge that demands a dynamic and multi-faceted response, reminding us that vigilance and collaboration are vital to safeguarding our cyber world in the digital age.

6. Sources

Alien vault review IP: 43.252.172.35. (n.d.). Retrieved from Alien vault : https://otx.alienvault.com/indicator/ip/43.252.172.35

Fake USPS Emails. (2023, 04 12). Retrieved from uspis.gov: https://www.uspis.gov/news/scam-article/fake-usps-emails

Review the Mirai file: Unix.Trojan.Mirai-5607483-0. (n.d.). Retrieved from Virus Total: https://www.virustotal.com/gui/file/251ecd1ac492fb7da375937888a5115e5271ed9f922ca5acdc28e012694507e9/detection

Review URL: usps[.]otognluguws[.]top. (n.d.). Retrieved from Virus Toral: https://www.virustotal.com/gui/url/af72bdb3476444b4121cb6c0019862caafa4809d3c5ff53873865cf56fdb186a/details

The Inspector tool. (n.d.). Retrieved from Kraken.IO: https://github.com/TheKrakenIO/The_Inspector