KRAKEN IO

Malicious IP Associated with more than 60 Subdomains

47.251.33[.]8

Introduction:

In the ever-evolving landscape of cyber threats, a new sophisticated campaign has emerged, orchestrated through a malicious IP [47.251.33[.]8]. 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:

- IP Profile
- Current Status
- Forward DNS Records
- Analysis

1. IP Profile

a. IP Analytics

IP Address: 47.251.33.8
Creation Date: April 14, 2016
Update Date: April 25, 2017
Registrant: Alibaba Cloud LLC
Country: United States

b. Open Ports and Services

Port 22: Running OpenSSH 7.4 (Open)
Port 80: Running NGINX service (Open)
Port 443: Running NGINX service (Open)
Port 40029: Status unspecified
Port 21: FTP (Closed)

c. SSH Vulnerabilities in the Server

The IP has several known SSH vulnerabilities, identified by their CVE numbers, ranging from 2016 to 2023.

CVE : 2023-38408, 2021-41617, 2021-36368, 2020-15778,2020-14145,2019-6111, 2019-6110, 2019-20685, 2018-15919, 2019-15473, 2018-15906, 2016-20012.

2. Current Status

The IP is currently live and active.

3. 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.com.wtpackege.top
usps.uposnes.com
uspost.wnpackege.top
usps.afcheckadress.top
usps.wepackege.top
uspost.uponsteo.com
uspost.ipostei.top
uspost.uposnes.com
usps.com.posnis.top
usps.com.ipostei.top
uspost.posnis.com
usps.ipostei.top
usps.com.uposnes.com
usps.com.nrcheckadress.top
usps.com.nicheckadress.top
uspost.wepackege.top
usps.wipackege.top
usps.com.whpackege.top
uspost.afcheckadress.top
uspost.wtpackege.top
uspost.nicheckadress.top
usps.com.wepackege.top
usps.com.wvpackege.top
usps.wxpackege.top
uspost.wrpackege.top
uspost.wapackege.top
usps.rpostei.top
usps.com.uponsteo.com
usps.com.wxpackege.top
usps.wkpackege.top
uspost.nrcheckadress.top
usps.com.wrpackege.top
usps.com.wnpackege.top
uspost.rpostei.top
usps.com.afcheckadress.top

usps.nzcheckadress.top
uspost.wipackege.top
uspost.whpackege.top
uspost.posnis.top
usps.wrpackege.top
uspost.wkpackege.top
uspost.wxpackege.top
usps.com.nzcheckadress.top
usps.uponsteo.com
usps.posnis.com
usps.com.posnis.com
usps.com.wapackege.top
uspost.nzcheckadress.top
usps.nrcheckadress.top
usps.wvpackege.top
usps.com.rpostei.top
usps.posnis.top
usps.wtpackege.top
usps.whpackege.top
usps.nicheckadress.top
usps.com.wkpackege.top
usps.wnpackege.top
uspost.wvpackege.top
usps.wapackege.top
usps.com.wipackege.top
dizoultrawelding.com

b. Primary Domains:

These are the primary domains that are hosted in the IP:

1. wtpackege.top - 3 subdomains
2. uposnes.com - 3 subdomains
3. wnpackege.top - 3 subdomains
4. afcheckadress.top - 3 subdomains
5. wepackege.top - 3 subdomains
6. uponsteo.com - 3 subdomains
7. ipostei.top - 3 subdomains
8. posnis.top - 3 subdomains
9. posnis.com - 3 subdomains
10. nrcheckadress.top - 3 subdomains
11. nicheckadress.top - 3 subdomains
12. wipackege.top - 3 subdomains
13. whpackege.top - 3 subdomains
14. wvpackege.top - 3 subdomains
15. wxpackege.top - 3 subdomains
16. wrpackege.top - 3 subdomains
17. wapackege.top - 3 subdomains
18. rpostei.top - 3 subdomains
19. wkpackege.top - 3 subdomains
20. nzcheckadress.top - 3 subdomains
21. dizoultrawelding.com - 0 subdomains

Common subdomains:

wtpackege
uposnes
afcheckadress
wepackege
posnis
ipostei
nrcheckadress
nicheckadress
whpackege
wvpackege
wxpackege
wrpackege
wapackege
rpostei
wkpackege
wnpackege
nzcheckadress

One domain that does not fit the USPS pattern:
dizoultrawelding.com

c. Domain Lifespan

Domain	Created	Updated	Expires	Registrant Name
wtpackege.top	9/21/23	9/22/23	9/21/24	Henry
uposnes.com	9/04/23	9/22/23	9/04/24	Alibaba
wnpackege.top	9/21/23	9/22/23	9/21/24	Henry
afcheckadress.top	9/25/23	-----	9/25/24	Complete Tech
wepackege.top	9/21/23	9/22/23	9/21/24	Henry
uponsteo.com	9/04/23	9/22/23	9/04/24	Alibaba
ipostei.top	9/04/23	9/22/23	9/04/24	Bush
posnis.top	9/04/23	9/22/23	9/04/24	Bush
posnis.com	9/04/23	9/22/23	9/04/24	Alibaba
nrcheckadress.top	9/25/23	-------	9/25/24	Complete Tech
wipackege.top	9/21/23	9/22/23	9/23/24	Henry
whpackege.top	9/21/23	9/22/23	9/21/24	Henry
wvpackege.top	9/21/23	9/22/23	9/21/24	Henry
wxpackege.top	9/21/23	9/22/23	9/21/24	Henry
wrpackege.top	9/21/23	9/22/23	9/21/24	Henry
wapackege.top	9/21/23	9/22/23	9/21/24	Henry
rpostei.top	9/04/23	9/22/23	9/04/24	Bush
wkpackege.top	9/21/23	9/22/23	9/21/24	Henry
nzcheckadress.top	9/25/23	----	9/25/24	Complete Tech
dizoultrawelding.com	7/15/20	7/15/23	7/15/23	Alibaba

The domains were registered around late 2023 and have expiration dates, mostly in 2024. Registrant names include 'Henry,' 'Alibaba,' 'Bush,' and 'Complete Tech,' suggesting that multiple entities may be involved or fictitious names are used to register these domains.

d. Distinguished Domains

nzcheckadress.top: This domain appears to have higher activity with directories flagged as malicious.
uspost.nzcheckadress[.]top/go/TrackConfirmAction
uspost.nzcheckadress.top/admin

canadapost-postescanada.nhcheckadress.top: Hosted on a different IP (43.135.163[.]174), this domain mimics the Canada Post, indicating the campaign targets users in multiple countries.

4. Analysis:

The tactics employed by the bad actor in this campaign are a classic example of phishing through domain and subdomain manipulation. By creating domain names that closely resemble the official USPS website, the attacker is betting on a typical user behavior: not scrutinizing the URL in the address bar. This is particularly effective because the fraudulent domains and subdomains are constructed to give the impression of authenticity. For instance, a user seeking to track a package might not notice that they have navigated to "usps.com.wtpackege.top" to understand how the user might be deceived:

"usps.com": This URL part is the most recognizable. Users expect to see it when looking for the official USPS website. Attackers include it to catch the user's eye and make the rest of the URL seem trustworthy by association.

".wtpackege": This section is a subdomain of the following domain. It's strategically placed to maintain the illusion of a legitimate USPS service, suggesting a specific function or department, such as 'weight package' or 'where's my package.'

".top": This is the top-level domain (TLD). Unlike the expected ".com" TLD, ".top" is less common and might be overlooked by users not paying close attention. It's the key to the attacker's domain and the destination where the user's browser is headed.

When put together in "usps.com.wtpackege.top," the URL creates an interactive illusion. The user, likely focused on the beginning of the URL, assumes they are navigating to the safe, official "usps.com" domain. In reality, they are being subtly redirected to a malicious site controlled by the attacker — "wtpackege.top." Once there, any interaction, such as attempting to track a package, could compromise the user's personal information.

This kind of attack, often referred to as "typo-squatting" or "URL hijacking," takes advantage of typographical errors internet users make when entering a website address into a web browser. By exploiting such errors, the attacker can divert traffic intended for the legitimate site to a malicious one, where victims might be tricked into disclosing personal information, downloading malware, or being defrauded.

The campaign's analysis indicates a high level of sophistication and adaptability. Utilizing the infrastructure of Alibaba Cloud LLC adds a veil of legitimacy to the operation, complicating the task of detection systems that might otherwise flag unfamiliar traffic sources. The wide range of subdomains allows for a robust and resilient campaign, minimizing the risk of disruption from domain blocklisting.

The global scope of this operation, targeting not only USPS but also mimicking Canada Post, demonstrates the attackers' ambition and highlights the potential for international impact. This approach will likely continue evolving, extending beyond postal services to other trusted brands, expanding the pool of potential victims.

The appropriate professional response encompasses both reactive and proactive measures. Reactive measures include reporting and blocking known malicious domains and subdomains. Proactive measures involve user education campaigns to raise awareness of phishing tactics and the implementation of sophisticated threat detection systems that employ heuristic and behavior-based analytics to identify and mitigate such threats preemptively.

Overall, this operation represents a significant and cleverly designed threat, leveraging the subtleties of domain naming to bypass user vigilance and security measures. A comprehensive cybersecurity strategy, combining education, advanced detection, and swift incident response, is paramount to defend against these phishing operations and safeguard against data breaches and identity theft.

Resources:

Analysis 47.251.33.8
https://threatbook.io/ip/47.251.33.8

Fake USPS Emails
https://www.uspis.gov/news/scam-article/fake-usps-emails

The Inspector tool -KrakenIO
https://github.com/TheKrakenIO/The_Inspector

Overview 47.251.33.8
https://hunt.io/domains/47.251.33.8