Searching for Smishing Triad DNS Traces

Table of Contents

Executive Report

Given the ubiquity of mobile phone usage, you'd think we'd all know by now how to tell legitimate from scammy text messages. Then again, cybercriminals are always on top of their game—learning how the latest technologies work and finding ways to abuse them.

Take phishing as an example. It has gone on to extend its reach far beyond users' computers at home and in the office to the mini computers they carry no matter where they go—their mobile phones. It's only to be expected, therefore, for smishing—Short Message Service (SMS)-based phishing—to gain popularity.

The Smishing Triad, discovered by Resecurity researchers, that plagued users all over Europe and Asia are now trailing their sights on U.S. citizens. They were most recently seen sending potential victims parcel delivery failure text messages supposedly from USPS. Users who click the embedded link and log in to the supposed USPS page are at risk of having their personal data stolen.

Resecurity published 27 indicators of compromise (IoCs) related to the ongoing campaign—two email addresses and 25 domains. The WhoisXML API researchers expanded this list through a DNS deep dive and found:

- 19 IP addresses to which the domains resolved, two of which are already classified as malicious based on malware checks
- 124 domains containing strings found among the IoCs, 34 of which are already considered malicious based on a bulk malware check
- 2,395 domains containing **usps** registered between 1 August and 13 September 2023, 595 of which are already detected as malicious based on a bulk malware check

IoC Facts

We began our in-depth investigation by taking a closer look at the IoCs.

A bulk WHOIS lookup for the 25 domains identified revealed that:

- Close to 90% of the domains were registered with NameSilo LLC between 10 April and 11 August 2023.
- Nineteen of the registrants redacted their names.
- Twenty of the registrants procured privacy protection services from PrivacyGuardian.org LLC.
- Twenty-one of the IoCs indicated the U.S. as their registrant country.

DNS Connections

We began our IoC list expansion analysis with DNS lookups for the 25 domains. We found that only 10 of them had active IP resolutions. Collectively, they resolved to 19 unique IP addresses, two of which—104[.]21[.]29[.]74 and 91[.]195[.]240[.]123—were already being detected as malicious based on malware checks.

A bulk IP geolocation lookup for the 19 IP addresses revealed that 95% originated from the U.S. and were under the purview of Cloudflare, Inc. The remaining IoC, geolocated in Germany, was administered by SEDO GmbH.

To hunt for potentially connected domains, we ran reverse IP lookups for the 19 IP addresses and found that they all appeared to be shared hosts.

Further scrutiny of the 25 domains identified as IoCs allowed us to identify six common strings, namely:

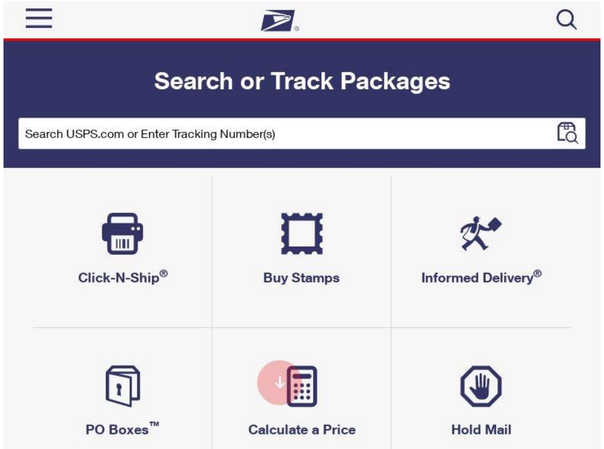
- **wangduoyu.**
- **ususnb.**
- **ususgs.**
- **uspsjh.**
- **uspoky.**
- **poczta-polska.**

According to our Domains & Subdomains Discovery searches, the strings appeared in 124 other domains, as much as 27% of which may have already figured in malicious campaigns. The artifacts containing the strings **wangduoyu.** and **poczta-polska.** could have already been weaponized in attacks targeting users in Asia and Poland, respectively. Poczta Polska is, after all, Poland’s state postal administration. Those containing variants of **usps**, meanwhile, could be used for U.S.-based attacks, with the attackers possibly impersonating the U.S. Postal Service.

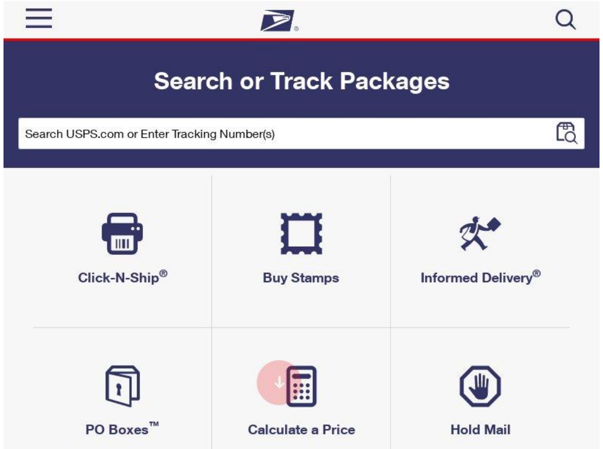
As a final step to find other artifacts possibly connected to the U.S. attacks, we looked for domains containing **usps**. We found 2,395 domains registered between 1 August and 13 September 2023. None of them were publicly attributable to the U.S. Postal Service based on their registrant email addresses.

It's also interesting to note that 595 of the **usps**-containing domains were already being detected by various malware engines as malicious. Of these, 101 remained accessible according to screenshot lookups although 15 malicious domains proved noteworthy since they mimicked not just the U.S. Postal Service's domain name but also its content.

Here's a side-by-side comparison of the official USPS website and a sample fake one.



Screenshot of the legitimate U.S. Postal Service site usps[.]com



Screenshot of the page hosted on the malicious domain uspsbt[.]com

It's also worth noting that 12 of the malicious domains hosting supposed USPS pages looked very similar. They all began with **usps** and one randomly chosen letter and used the .com TLD extension.

—

Our DNS deep dive into the Smishing Triad unveiled more than 2,500 potentially connected artifacts. Note, however, that the USPS look-alike domains and websites may not necessarily be part of the group's infrastructure but when accessed could definitely put users at risk since none of them could be publicly attributed to the company.

If you wish to perform a similar investigation or learn more about the products used in this research, please don't hesitate to contact us.

***Disclaimer:** We take a cautionary stance toward threat detection and aim to provide relevant information to help protect against potential dangers. Consequently, it is possible that some entities identified as "threats" or "malicious" may eventually be deemed harmless upon further investigation or changes in context. We strongly recommend conducting supplementary investigations to corroborate the information provided herein.*

Appendix: Sample Artifacts and IoCs

IoCs Identified by Resecurity

- mj*****@icloud[.]com
- spam@uspis[.]gov
- wangduoyu[.]site
- wangduoyu[.]shop
- wangduoyu[.]me
- ususuua[.]top
- ususnu[.]top
- ususnb[.]top
- ususmx[.]top
- usushk[.]top
- ususgs[.]top
- ususcsa[.]top
- ususcgh[.]top
- ususcac[.]top
- uspsuiu[.]top
- uspskkq[.]top
- uspsjh[.]top
- uspshhg[.]top
- uspsdg[.]top
- uspoky[.]top
- uspogumb[.]top
- uspoddp[.]top
- uspodad[.]top
- uspodaa[.]top
- uspoadc[.]top
- usplve[.]top
- poczta-polska[.]cc

Sample IP Addresses the Domains Identified as IoCs Resolved To

- 104[.]21[.]1[.]77
- 104[.]21[.]2[.]119
- 104[.]21[.]29[.]108
- 104[.]21[.]29[.]74
- 104[.]21[.]71[.]37
- 104[.]21[.]71[.]51
- 104[.]21[.]78[.]58
- 104[.]21[.]8[.]114
- 104[.]21[.]91[.]129
- 172[.]67[.]128[.]200

Sample String-Connected Domains

- poczta-polska[.]ml
- poczta-polska[.]cc
- poczta-polska[.]pl
- poczta-polska[.]de
- poczta-polska[.]eu
- poczta-polska[.]cf
- poczta-polska[.]me
- poczta-polska[.]pt
- poczta-polska[.]tk
- poczta-polska[.]gq

- poczta-polska[.]us
- poczta-polska[.]org
- poczta-polska[.]com
- poczta-polska[.]xyz
- poczta-polska[.]top
- ppoczta-polska[.]pl
- poczta-polska[.]app
- poczta-polska[.]bio
- poczta-polska[.]icu
- poczta-polska[.]net
- epoczta-polska[.]pl
- poczta-polska[.]biz
- poczta-polska[.]one
- poczta-polska[.]life
- epoczta-polska[.]com
- poczta-polska[.]live
- poczta-polska[.]info
- ipoczta-polska[.]org
- poczta-polska[.]buzz
- epoczta-polska[.]biz
- usplve[.]top
- uspoadc[.]top
- uspodaa[.]top
- uspodad[.]top
- uspoddp[.]top
- uspogumb[.]top
- uspoky[.]vg
- puspoky[.]hu
- uspoky[.]top
- uspoky[.]com
- wangduoyu[.]us
- wangduoyu[.]cn
- wangduoyu[.]me
- wangduoyu[.]io
- wangduoyu[.]cc
- wangduoyu[.]xyz
- wangduoyu[.]art
- wangduoyu[.]icu
- wangduoyu[.]app
- wangduoyu[.]vip

Sample Malicious String-Connected Domains

- poczta-polska[.]cc
- poczta-polska[.]eu
- poczta-polska[.]me
- poczta-polska[.]xyz
- poczta-polska[.]icu
- poczta-polska[.]net
- poczta-polska[.]biz
- poczta-polska[.]one
- epoczta-polska[.]com
- poczta-polska[.]info
- uspogumb[.]top
- uspoky[.]top
- uspsdg[.]top
- uspshhg[.]top
- uspsjh[.]us
- uspsuiu[.]top
- ususcac[.]top
- wangduoyu[.]me
- wangduoyu[.]cc
- wangduoyu[.]xyz

Sample Domains Containing usps Registered between 1 August and 13 September 2023

- uspsousps[.]top
- uspsoousps[.]top
- uspsousps1[.]top
- usps-usps[.]life
- usps-usps[.]work
- usps[.]kim
- uspsz[.]cn
- usps[.]bio

- uspsi[.]cc
- uspss[.]de
- uspsa[.]de
- uspss[.]ws
- usps[.]pet
- usps[.]bet
- uspsm[.]co
- uspsl[.]cc
- usps1[.]cc
- usps6[.]cc
- uspsn[.]cc
- uspsdw[.]us
- uspsne[.]us
- uspspv[.]us
- uspsek[.]us
- uspstr[.]us
- uspsre[.]us
- uspsua[.]us
- uspsrs[.]us
- uspsko[.]us
- usps-s[.]cc
- uspsgn[.]us
- uspsbt[.]us
- uspstz[.]us
- uspsxn[.]us
- uspsxw[.]us
- uspsol[.]pw
- uspsxr[.]us
- uspspn[.]us
- uspsqc[.]us
- uspske[.]us
- uspsnk[.]us
- uspsfb[.]us
- usps[.]fund
- uspsza[.]us
- uspsi[.]vip
- uspszx[.]us
- uspsnx[.]us
- uspsjk[.]us
- uspsjm[.]us
- uspsmj[.]us
- uspsmh[.]us
- uspsnf[.]us
- uspscz[.]us
- uspsrv[.]us
- uspsvr[.]us
- uspsdv[.]us
- uspsp[.]vip
- uspspx[.]us
- uspss[.]fit
- uspsyl[.]us
- uspsdk[.]us
- uspsfn[.]us
- uspsff[.]us
- uspsfe[.]us
- uspsnb[.]us
- uspskm[.]us
- uspsqa[.]us
- uspsgg[.]us
- uspsww[.]us
- uspsxv[.]us
- uspssl[.]pw
- uspss[.]win
- uspshu[.]us
- uspsdm[.]us
- uspsjb[.]us
- uspsvs[.]us
- uspsta[.]us
- uspsmv[.]us
- uspsso[.]us
- uspsgj[.]us
- uspsgm[.]us
- uspsna[.]us
- uspsjw[.]us
- uspskl[.]us
- uspspf[.]us
- uspsmc[.]us
- uspslm[.]us
- uspsnp[.]us
- uspsry[.]us

- uspsht[.]us
- usps1[.]net
- uspsuj[.]us
- uspsnm[.]us
- uspsxu[.]us
- uspssx[.]us
- uspspr[.]us
- uspsnd[.]us
- uspsjg[.]us
- uspsmd[.]us
- uspssk[.]us
- uspssr[.]pw

Sample Malicious usps-Containing Domains

- uspsoousps[.]top
- usps-usps[.]work
- usps[.]kim
- usps[.]bio
- uspsi[.]cc
- uspss[.]de
- uspss[.]ws
- usps[.]bet
- uspsm[.]co
- usps1[.]cc
- usps6[.]cc
- uspspv[.]us
- uspsre[.]us
- uspsrs[.]us
- uspsko[.]us
- usps-s[.]cc
- uspsgn[.]us
- uspsbt[.]us
- uspstz[.]us
- uspsxn[.]us
- uspsol[.]pw
- uspspn[.]us
- uspsqc[.]us
- uspsnk[.]us
- uspsza[.]us
- uspsnx[.]us
- uspsjk[.]us
- uspsjm[.]us
- uspsmj[.]us
- uspsmh[.]us
- uspsnf[.]us
- uspscz[.]us
- uspsrv[.]us
- uspsvr[.]us
- uspsdv[.]us
- uspsp[.]vip
- uspspx[.]us
- uspss[.]fit
- uspsfn[.]us
- uspsff[.]us
- uspsnb[.]us
- uspskm[.]us
- uspsqa[.]us
- uspsgg[.]us
- uspssl[.]pw
- uspshu[.]us
- uspsdm[.]us
- uspsjb[.]us
- uspsvs[.]us
- uspsmv[.]us
- uspsso[.]us
- uspsgj[.]us
- uspsgm[.]us
- uspsna[.]us
- uspsjw[.]us
- uspskl[.]us
- uspspf[.]us
- uspsmc[.]us
- uspslm[.]us
- uspsnp[.]us
- uspsry[.]us
- uspsht[.]us

- uspsuj[.]us
- uspsnm[.]us
- uspssx[.]us
- uspspr[.]us
- uspsnd[.]us
- uspsjg[.]us
- uspsmd[.]us
- uspssr[.]pw
- uspsho[.]us
- uspsri[.]us
- uspspb[.]us
- uspsmg[.]us
- uspsmk[.]us
- uspscv[.]us
- uspshe[.]us
- uspspw[.]us
- uspsnz[.]us
- uspsjv[.]us
- uspsbt[.]pw
- uspsee[.]us
- uspspp[.]us
- uspspg[.]us
- uspsfu[.]us
- uspsdx[.]us
- uspspd[.]us
- uspsgy[.]us
- uspsts[.]us
- uspsfv[.]us
- uspsjo[.]us
- uspsqg[.]us
- uspsqi[.]us
- uspsru[.]us
- uspslc[.]us
- uspswr[.]us
- uspsie[.]us
- uspstw[.]us
- uspsmz[.]us
- uspseu[.]us