Smishing TriadがDNSに残した痕跡をたどる

目次

要旨

携帯電話が多くの人にいたるところで利用されるようになった今、詐欺のテキストメッセージを見分ける方法はもうわかっていると思われるかもしれません。しかし、サイバー犯罪者は常に最新の技術を学び、まだ知られていない悪用の方法を新たに見出しています。

例えばフィッシングは、自宅やオフィスのコンピューターから携帯電話にその活動の場を広げています。ショートメッセージサービス（SMS）を利用したフィッシング、すなわちスミッシングの流行は当然の成り行きと言えるでしょう。

Resecurityの研究者らによって発見された「Smishing Triad」は、かねてよりヨーロッパとアジアの全域でユーザーを悩ませていました。しかし、今はアメリカ人を標的にしています。最近、米国郵政公社（USPS）から送信されたかのように見える不在通知のテキストメッセージが確認されました。メッセージに埋め込まれたリンクをクリックし、USPSのように見えるページにログインすると、個人情報を盗まれる危険性があります。

Resecurityは、現在進行中のSmishing Triadのキャンペーンに関わっている27個のセキュリティ侵害インジケーター（IoC）（2個のメールアドレスと25個のドメイン名）を公開しています。そこで、WhoisXML APIの研究者がそのIoCリストをもとにDNSを徹底調査し、このたび以下を新たに発見しました。

- ドメイン名が名前解決した19個のIPアドレス。そのうち2個は、マルウェアチェックにより悪意あるIPアドレスと確認
- IoCに見られる文字列を含んだ124個のドメイン名。うち34個はマルウェアの一括チェックで悪意あるドメイン名と確認
- 2023年8月1日から9月13日の間に登録された、**usps**という文字列を含むドメイン名2,395個。うち595個はマルウェア一括チェックにより悪意があることを確認

IoCの実態

当社ではまず、Smishing TriadのIoCを詳しく調べることから調査を開始しました。Resecurityが特定した25個のドメイン名をBulk WHOIS Lookupで検索したところ、以下が判明しました。

- 90%近くのドメイン名は、2023年4月10日から8月11日の間にNameSilo LLC経由で登録されたもの
- 19の登録者は名前を非公開にしていた
- 20の登録者はPrivacyGuardian.org LLCのプライバシー保護サービスを利用
- 21個のドメイン名は米国で登録された

DNSのつながり

次に、IoCとして特定されている25個のドメイン名をDNS Lookupにかけました。その結果、IPアドレスへの名前解決が有効だったのは10個だけとわかりました。それらのドメイン名が名前解決したユニークなIPアドレスは合計19個ありましたが、そのうちの2個（104[.]21[.]29[.]74と91[.]195[.]240[.]123）は、すでに悪意あるアドレスとして検出されていたことがマルウェアチェックで判明しました。

その19個のIPアドレスをBulk IP Geolocation Lookupで検索したところ、95%は米国に位置しており、Cloudflare, Inc.の管理下にあることが明らかになりました。それ以外のIoCはドイツにあり、管理ISPはSEDO GmbHでした。

共通のIPアドレスを使っている可能性のあるドメイン名を探すため、19個のIPアドレスに対してReverse IP Lookupを実行したところ、全てが共用ホストのようでした。

IoCと特定された25個のドメイン名をさらに精査した結果、共通する文字列として以下の6つを特定することができました。

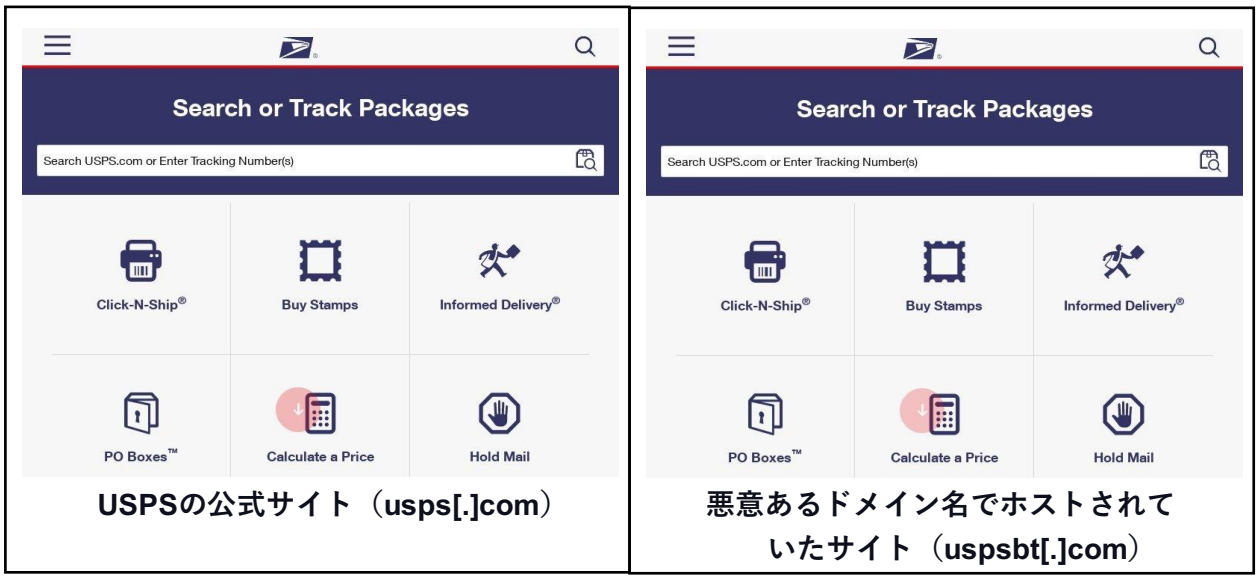
- **wangduoyu.**
- **ususnb.**
- **ususgs.**
- **uspsjh.**
- **uspoky.**
- **poczta-polska.**

Domains & Subdomains Discoveryでの検索結果によると、これらの文字列は別の124個のドメイン名に含まれており、そのうちの27%はすでに悪意のあるキャンペーンに関与した可能性があります。**wangduoyu.**と**poczta-polska**という文字列を含むドメイン名は、それぞれアジアとポーランドのユーザーを標的とした攻撃ですでに使われたことが疑われます。Poczta Polskaはポーランドの郵便局です。他方、**usps**のバリエーションを含むドメイン名は、脅威アクターがUSPSになりすまして米国での攻撃に使用したかもしれません。

米国における攻撃に関連している他のアーティファクトを特定するため、**usps**を含むドメイン名を探したところ、2023年8月1日から9月13日の間に登録された2,395個のドメイン名が見つかりました。登録者のメールアドレスを見る限り、USPSへの帰属を確認できるドメイン名はありませんでした。

uspsを含むドメイン名のうち595個は、すでに様々なマルウェアエンジンによって悪意あるドメイン名として検出されていました。それらにScreenhot Lookupを実行したところ、101個のドメイン名がアクセス可能な状態のままでしたが、15個については、USPSのドメイン名のみならずUSPSのコンテンツも模倣していたことが判明しました。

以下は、USPSの公式ウェブサイトと偽サイトのサンプルを並べて比較したものです。



USPSの公式サイト（usps[.]com）

悪意あるドメイン名でホストされていたサイト（uspsbt[.]com）

USPSのように見えるページをホストしている悪意あるドメイン名のうち12個は、見た目がUSPSのドメイン名と非常によく似ていました。全て**usps**と無作為に選ばれたらしい1文字で始まる.comドメイン名でした。

—

今回DNSでSmishing Triadを詳しく調査した結果、関連性が疑われるアーティファクトが2,500個以上見つかりました。USPSに見た目が似ているドメインやウェブサイトの全てがSmishing Triadのインフラの一部とは限りません。しかし、いずれもUSPSへの帰属がWHOIS情報から確認できないため、アクセスしたユーザーを危険にさらす可能性はあります。

同様の調査をご希望のお客様、または本調査で使用された当社の商品にご興味をお持ちのお客様は、こちらまでお気軽にお問い合わせください。

免責事項： *当社は、潜在的な危険から企業を守るために役立つ情報の提供を目指しており、脅威の検出に対して厳格な姿勢で臨んでいます。そのため、当初「脅威」または「悪意がある」とみなされたエンティティが、さらなる調査やその後の状況の変化により最終的に無害と判断される可能性があります。ここで提供されている情報を確認する補足調査の実施を強くお勧めします。*

付録：アーティファクトとIoCの例

Resecurityが特定したIoC

- 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

IoCとして特定されたドメイン名が名前解決したIPアドレスの例

- 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

共通の文字列を含むドメイン名の例

- 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

共通の文字列を含む悪意あるドメイン名の例

- 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

2023年8月1日～9月13日に登録された*usps*を含むドメイン名の例

- 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

*usps*を含む悪意あるドメイン名の例

- 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