ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

● 4月度フィッシング報告件数は246,580件、3月度からの高水準続く

https://www.antiphishing.jp/report/monthly/202504.html

このニュースをザックリ言うと・・・

- 5月20日(日本時間)、フィッシング対策協議会より、4月に寄せられたフィッシング報告状況が発表されました。
- 4月度の報告件数は246,580件で、3月度(https://www.antiphishing.jp/report/monthly/202503.html)の249,936件から3,356件減少しています。
- フィッシングサイトのURL件数は48,373件で3月度(51,735件)から3,362件減少、使用されるTLD(トップレベルドメイン名)の割合は .com(約32.3%)、.cn(約28.4%)、 .asia(約14.2%)、.goog(約5.1%)、 .net(約4.7%)で、この5つで約84.7%を占めています。
- 悪用されたブランド件数は100件で3月度(84件)から16件増加、Amazonを騙るフィッシングが約10.7%と減少したのに代わり、SB証券を騙るものが約11.3%と急増してトップとなっており、この2つに、1万件以上報告された野村證券、VISA、Apple、ANA、マネックス証券、東京ガスと合わせて約54.8%、さらに1,000件以上報告された31ブランドまで含めると約95.6%を占めたとのことです。

AUS便りからの所感等

- 報告件数は過去最多となった3月度に次いでいますが、4月度より迷惑メールフィルターで検知されたとみられるメール(4月度では約10.5万件)を報告件数から除外しており、これを合わせた場合は35万件を超えるとのことです。
- 大手ネット証券、特にSBI証券が標的として目立っており、証券各社が様々なセキュリティの強化策を打つ中、その告知等を装ったフィッシングも頻繁に確認されています。
- 例えば追加認証の設定時にID・パスワードの入力が要求されることがあり、くれぐれもその段階でフィッシングサイトに誘導されることのないよう、事前に登録したブラウザーのブックマークやスマホアプリから実際に使用しているサービスのサイトへアクセスすることを特に注意してください。

フィッシング対策協議会
Council of Anti-Phishing Japan

● DNS設定ミスによるドメイン名・Webサイト乗っ取り、海外でも相次いで発生

https://www.bleepingcomputer.com/news/security/hazy-hawk-gang-exploits-dns-misconfigs-to-hijack-trusted-domains/
https://blogs.infoblox.com/threat-intelligence/cloudy-with-a-chance-of-hijacking-forgotten-dns-records-enable-scam-actor/

このニュースをザックリ言うと・・・

- 5月20日(現地時間)、米セキュリティ企業Infoblox社より、「Hazy Hawk」と呼ばれる攻撃者グループによるWebサイトの乗っ取りが多発しているとして注意喚起が出されています。
- DNSのCNAMEレコード(別のドメイン名を参照する)について参照先となるクラウドサービス上のサーバーが既に存在していないものを探し、同じ名前で自分たちのサーバーを登録することにより、ドメイン名の一部(サブドメイン)等を乗っ取り、詐欺行為やマルウェア配布等に悪用するとのことです。
- 2025年2月にアメリカ疾病予防管理センターのドメイン名「cdc.gov」において乗っ取りが発生し、当該ドメイン名の不正なサイトがサーチエンジンに表示される事象が確認されたことで注目を集めたとしており、少なくとも2023年12月以降、世界中の他の政府機関・大学および国際企業が同様の攻撃を受けているとしています。

AUS便りからの所感

- Infoblox社の記事では攻撃を受けたとされるドメイン名の一覧が示されており、.govドメインのものが複数、また.jpドメインのものも一部確認されています。
- 日本国内でも昨年12月以降、同様の事例がネットワーク研究者によって多数指摘され、乗っ取りからの「保護」と称するアクションが行われていました(AUS便り 2025/01/23号参照)。
- CNAMEレコード(他にもNSレコード等も)が生きていながら、参照先のサーバーを第三者が乗っ取り可能な状態となっている、いわゆる「Dangling Record」への対策として、サービスを終了したWebサイト等のみならず、運用中のサービスにおいて設定変更があったケースについても、参照先を使用しなくなったDNSレコード情報については確実に削除することが重要です。

BLEEPINGCOMPUTER

Hazy Hawk gang exploits DNS misconfigs to hijack trusted domains

By Bill Toulas

A threat actor tracked as 'Hazy Hawk' is hijacking forgotten DNS CNAME records pointing to abandoned cloud services, taking over trusted subdomains of governments, universities, and Fortune 500 companies to distribute scams, fake apps, and malicious ads.

According to Infoblox researchers, Hazy Hawk first scans for domains with CNAME records pointing to abandoned cloud endpoints, which they determine via passive DNS data validation.

●証券口座乗っ取りによる不正取引、NHKで特集

https://www3.nhk.or.jp/news/html/20250520/k10014808601000.html

このニュースをザックリ言うと・・・

- 5月20日、NHK「クローズアップ現代」において証券口座へのサイバー攻撃による不正取引事案が取り上げられ、内容が公式Webサイトにまとめられています。
- 3月に口座の乗っ取りにあい、不正取引を行われた被害者は、普段から不審なメールやパスワードの管理には注意しているとしていたものの、PC上のメールやWebアクセス履歴の解析から、ネット証券からの約款変更告知を騙るなりすましメールから偽サイトに誘導され、ID・パスワードを入力した15分後に不正ログインが、3時間後には不正取引が行われたとされています。
- 不正取引は世界的に見ても日本が集中的に狙われているとし、中国企業の株を短時間に大量に売買した形跡や、偽サイトにおいてもソースコードの一部に中国語が用いられていることが確認され、中国語圏等の犯罪者グループが関与しているとみられています。

AUS便りからの所感

- アカウントの奪取においては、フィッシングの他にもいわゆる「インフォスティーラー」と称されるマルウェアへの感染による事例も取り上げられています。
- なりすましメールについても、これまで日本語のものは不自然な文言のものが多くみられましたが、生成AIの登場により、海外からでも自然な文章を作ることが容易になっているとしています。
- 特集では「パスワードだけでは、もはや守れなくなってきていることを認識することが重要」と結論付けており、証券各社はアカウント保護のためのセキュリティ対策を相次いで採用していますが、攻撃者がターゲットとするような海外の株に本来は目を向けないユーザーも多いと思われ、金融商品の種類毎にユーザーが同意しない限り取引を行わないようにする等の方策も適宜とっていくことに期待したいものです。

NHK

WEB特集 相次ぐ証券口座乗っ取り 被害者のパソコン解析で分かったこと

2025年5月20日 16時23分 サイバー攻撃

証券口座を乗っ取られ、株を勝手に売買される被害が急増している。

不正な取り引きによる売買はこの4か月で3000億円を超えた。

なぜ被害が拡大しているのか。

NHKは今回デジタル調査を行う会社と共同で、「デジタルフォレンジック」という技術を使って被害者のパソコンを解析。

そこから見えてきたのは、従来のパスワードだけでは、資産を守ることが難しくなってきている実態だった。