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。

●6月度フィッシング報告件数は192,870件、証券会社の対策で減少か

https://www.antiphishing.jp/report/monthly/202506.html

このニュースをザックリ言うと・・・

- 7月18日(日本時間)、フィッシング対策協議会より、6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。

- 6月度の報告件数は192,870件で、5月度(https://www.antiphishing.jp/report/monthly/202505.html)の229,536件から36,666件減少しています。

- 悪用されたブランド件数は94件で5月度(91件)から3件増加、割合が多かったのはApple(約16.4%)、SBI証券(11.3%)、ANA(約10.3%)で、次いで1万件以上報告されたAmazon、NTTドコモと合わせて約50.5%、さらに1,000件以上報告された27ブランドまで含めると約94.0%を占めたとのことです。

- フィッシングサイトのURL件数は60,107件で5月度(55,940件)から4,167件増加、使用されるTLD(トップレベルドメイン名)の割合が多かったのは .cn(約26.6%)、 .com(約24.0%)、.asia(約14.1%)、.top(約8.8%)、.cc(約5.7%)で、この6つで約79.2%を占めています。

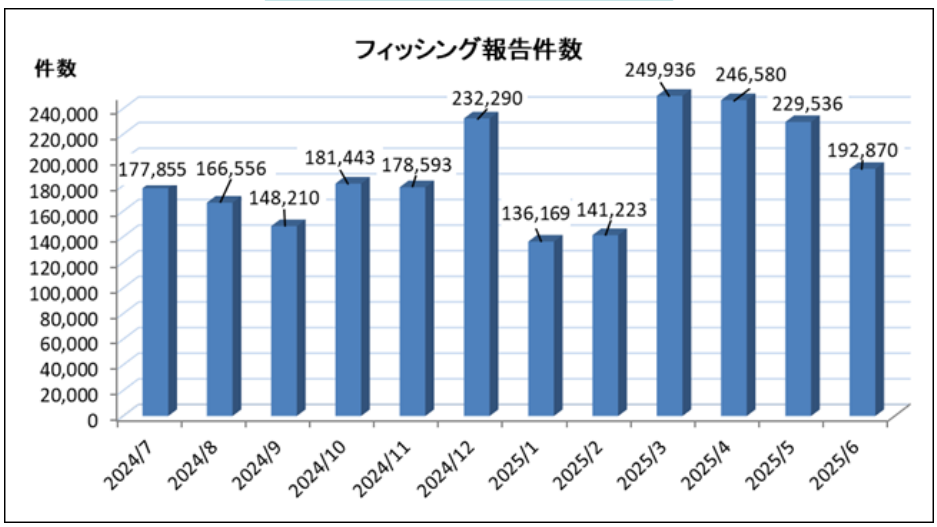
AUS便りからの所感等

- 同協議会では、各証券会社が多要素認証の必須化等といった不正利用対策の強化を行ったことがフィッシングの減少傾向の要因としている一方、各社から送られている注意喚起・多要素認証の設定依頼および補償に関するメール等を装ったフィッシングによる被害も引き続き確認されているとしています。

- フィッシングメールの送信元IPアドレスにDNS PTRレコード(IPアドレスからの逆引き)が設定されていない割合が約91.0%と高く、また設定されている場合でもこれをさらに正引きした結果(A/AAAAレコード)とは一致しないケースも頻繁に確認されており、そういったケースを判別する、いわゆるFCrDNS(Forward Confirmed Reverse DNS)認証がフィッシング・スパムメールの大幅な遮断に有用としていますが、日本国内での対応はまだ十分でない模様です。

- 毎月の報告状況ではこの他にもフィッシングメールの傾向やメールの内容で主に使われる手法、および「事業者のみなさまへ」「利用者のみなさまへ」と題した対策の呼び掛けが掲載されており、同協議会から6月3日に発表された「フィッシングレポート2025」「フィッシング対策ガイドライン」とも併せて参考とし、アンチウイルス・UTMのアンチフィッシング機構による防衛や、フィッシングサイトへ誘導されないための慎重な行動を是非とも心掛けて頂ければ幸いです。

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



● 2010年放送アニメのサイトにオンラインカジノへの誘導…第三者がドメイン名取得、偽サイト設置か

https://www.itmedia.co.jp/news/articles/2507/23/news108.html
https://togetter.com/li/2579719

このニュースをザックリ言うと・・・

- 7月22日(日本時間)頃、X(旧Twitter)において、2010年に放送されたアニメ「怪盗レーニャ」の公式サイトが、オンラインカジノへと誘導する不審な内容になっているとの指摘があり、ネットニュース等で取り上げられています。
- 当該サイトのドメイン名が2020年以降第三者のものとなっているとみられ、当時のサイトのコンテンツを引き写しながら、巧妙にオンラインカジノの紹介文を含んだものとなってる模様です。
- ドメイン名は7月28日現在も有効であり、話題を取り上げている「ITMedia NEWS」によれば、当時の主演タレントの所属事務所から制作委員会幹事のKADOKAWA社に対応が依頼されているとのことです。

AUS便りからの所感

- 失効したドメイン名が第三者に「ドロップキャッチ」される事案は、6月にもJR東日本およびアトレが運営していた「マイアトレ」に関する発表がありました(AUS便り 2025/07/07号参照)。
- 15年前のアニメ作品ではあるものの、同じURLで本物と誤認させるような内容の偽サイトが設置されたことにより、古いWebページのリンクや資料掲載のURL・QRコードから、さらにはサーチエンジンでも上位に表示され、誘導される危険性が指摘されています。
- ドメイン名の「終活」をどうすべきかについては、2024年末に技術資料が公開(同 2024/11/14号参照)されてから話題となっていますが、対策の一つに挙げられる「閉鎖後にドメイン名を長期間(10年以上等)保持する」について、今回と同様の事案が頻発することで「永久に保持しなければならない」となる可能性や、最初の取得時点で「既存のドメイン名やそのサブドメインを用いる」ことの検討がより重要となる等、既存の知見の更新が今後起き得るとみられます。

ITmedia NEWS

アニメ公式サイトがいつの間にか“オンカジ誘導サイト”に変わっていた？　事務所「すでに対応をお願いしている」

2025年07月23日 19時33分 公開　[芹澤隆徳，ITmedia]

懐かしいアニメの公式サイトを見たら、なぜかオンラインカジノの宣伝サイトになっていた――と、X上で話題になっている。そのアニメは2010年に放送した「怪盗レーニャ」。モーニング娘。の田中れいなさんをモチーフにしたコメディアニメで、田中さん本人が声優を務めたことでも知られる。

そのWebサイトは一見、一般的なアニメ公式サイトにみえる。ストーリーやキャラクター紹介などのメニューがあり、DVD販売情報なども掲載している。

しかし、スクロールした先には「アニメの次はオンラインカジノ！」「貴方の心を鷲掴み！な、怪盗レーニャとネットカジノ」といったコンテンツが並んでいた。何らかの理由で手放したドメインを第三者が入手し、怪盗レーニャ公式サイトを模したオンラインカジノ誘導サイトを作ったとみられる。

● Apache HTTP Server 2.4.64でアクセス制限回避の恐れ…2.4.65で修正

https://httpd.apache.org/security/vulnerabilities_24.html#2.4.65
https://www.cve.org/CVERecord?id=CVE-2025-54090
https://security.sios.jp/vulnerability/apache-security-vulnerability-20250724/

このニュースをザックリ言うと・・・

- 7月25日(日本時間)、Apache Software Foundationより、Apache HTTP Server(以下・Apache)の最新バージョン2.4.64にセキュリティホールが存在すると発表されました。
- 2.4.64は同11日に出たばかりのセキュリティアップデート(AUS便り 2025/07/22号参照)でしたが、mod_rewriteモジュールにバグが存在し、アクセス制限等を行っていた場合に迂回される恐れがあるとされています。
- 既に修正バージョン2.4.65がリリースされており、2.4.64をインストールしている場合はアップデートが推奨されています。

AUS便りからの所感

- mod_rewriteのバグは、RewriteCondディレクティブによる条件分岐において、本来false(否)とすべきケースでも全てtrue(真)になるというものとされ、許可しないアクセス元に対するエラーやリダイレクトの実行が行われなかったり、逆に常時エラーが発生したりする等の可能性が考えられます。
- 脆弱性が存在するのは2.4.64のみで、主にこれをソースコードからコンパイルした場合にのみ影響するとされ、主要なLinuxディストリビューションでは影響しないと発表されています。
- 一方で2.4.64で修正された複数の脆弱性については、Ubuntuで修正パッケージがリリースされていますが、RHEL系(Almalinux・Rocky Linux等)やDebianではまだリリースされておらず、更新され次第速やかに適用するよう引き続き用意を推奨致します。

APACHE HTTP SERVER PROJECT

Apache HTTP Server 2.4 vulnerabilities

This page lists all security vulnerabilities fixed in released versions of Apache HTTP Server 2.4. Each vulnerability is given a security impact rating by the Apache security team - please note that this rating may well vary from platform to platform. We also list the versions the flaw is known to affect, and where a flaw has not been verified list the version with a question mark.

Please note that if a vulnerability is shown below as being fixed in a "-dev" release then this means that a fix has been applied to the development source tree and will be part of an upcoming full release.

Please send comments or corrections for these vulnerabilities to the Security Team.

The initial GA release, Apache httpd 2.4.1, includes fixes for all vulnerabilities which have been resolved in Apache httpd 2.2.22 and all older releases. Consult the Apache httpd 2.2 vulnerabilities list for more information.

Fixed in Apache HTTP Server 2.4.65

moderate: Apache HTTP Server: 'RewriteCond expr' always evaluates to true in 2.4.64 (CVE-2025-54090)

A bug in Apache HTTP Server 2.4.64 results in all "RewriteCond expr ..." tests evaluating as "true".

Users are recommended to upgrade to version 2.4.65, which fixes the issue.

Reported to security team	2025-07-16
Update 2.4.65 released	2025-07-23
Affects	