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。

● 1月フィッシング報告件数は136,169件、旧正月で大幅減少も高水準続く

https://www.antiphishing.jp/report/monthly/202501.html

このニュースをザックリ言うと・・・

- 2月18日(日本時間)、フィッシング対策協議会より、1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。

- 1月度の報告件数は136,169件で、12月度(https://www.antiphishing.jp/report/monthly/202412.html)の232,290件から96,121件減少しています。

- フィッシングサイトのURL件数は43,534件で12月度(120,415件)から76,811件減少(サブドメイン違いを重複として除外した件数は12,826件)、使用されるTLD(トップレベルドメイン名)の割合は .com(約47.5%)、.cn(約35.7%)で合わせて約83.2%、これに続く .shop(約3.8%)、 .goog(約3.3%)、 .net(約3.0%)等を引き離すトップ2の状態が続いています。

- 悪用されたブランド件数は89件で12月度(107件)から18件減少、最も割合が多かったブランドとしてはAmazonとPayPayがそれぞれ全体の約22.3%と13.9%、次いで三井住友カード、えきねっと、佐川急便、JAバンクと合わせて約53.4%、さらに1,000件以上報告された21ブランドまで含めると約92.6%を占めたとのことです。

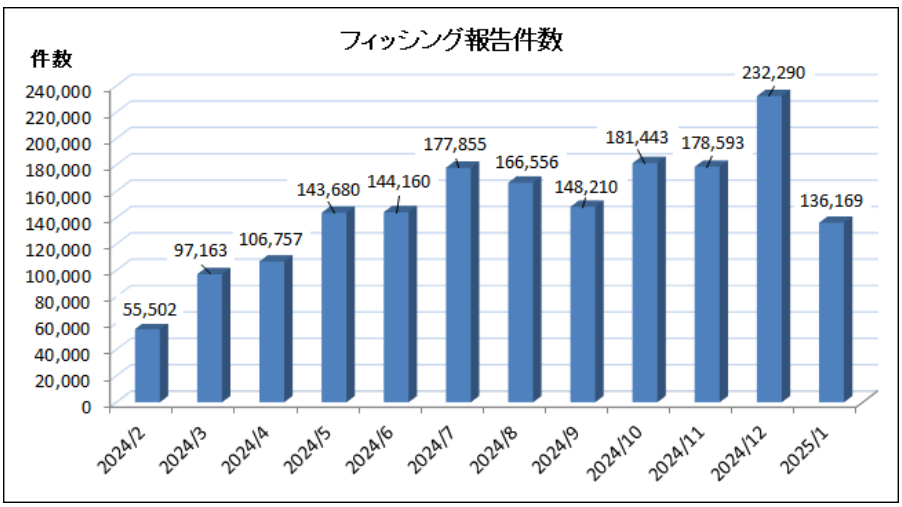
AUS便りからの所感等

- 例年1・2月における傾向の通り、報告件数は中国の旧正月が関係して大幅に減少したとはいえ、2024年5月以降14万件超が続いている流れから見れば依然として高い水準を維持しており、2月や3月以降再び20万件を超えることは確実でしょう。

- 毎月の発表においてユーザーへ行っている呼び掛けのうち、「利用者のみなさまへ」では「パスワードマネージャー」や「パスキー」の活用を推奨しており、前者は本物と異なるドメイン名では自動的に入力されない点、後者では公開鍵暗号を用い外部に機密情報を送信しない点から、フィッシングサイトへのパスワード等の入力を抑制する意味でも有用な策と言えます。

- ただしパスワードマネージャーの種類によっては、手動で他のドメイン名の情報を入力することも可能(同じサービスのサイトでもログイン画面のドメイン名が異なったり変動したりするケースに対応するものとみられます)なものもあり、表示されているサイトに対し適切な候補が提示されなかった場合でも、ドメイン名を確認せず安易にそのような入力を行わないよう十分注意が必要です。

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



●OpenSSHに2件の脆弱性、中間者攻撃・DoS攻撃の可能性

https://codebook.machinarecord.com/threatreport/37410/
https://www.bleepingcomputer.com/news/security/new-openssh-flaws-expose-ssh-servers-to-mitm-and-dos-attacks/
https://www.openssh.com/txt/release-9.9p2
https://blog.qualys.com/vulnerabilities-threat-research/2025/02/18/qualys-tru-discovers-two-vulnerabilities-in-openssh-cve-2025-26465-cve-2025-26466

このニュースをザックリ言うと・・・

- 2月18日(現地時間)、OpenSSHの2件の脆弱点を修正したバージョン9.9p2がリリースされました。
- 脆弱性の悪用により、中間者攻撃によるSSHセッションの乗っ取り等(CVE-2025-26465)、およびDoS攻撃(CVE-2025-26466)の可能性があるとされています。
- 脆弱性はセキュリティベンダーの米Qualys社によって発見・報告されたもので、同日には同社からも脆弱性に関する発表がなされています。
- 2月20日現在、主要なLinuxディストリビューションのうちDebian・Ubuntuでは提供パッケージに対するセキュリティアップデートがリリースされています。

AUS便りからの所感

codebook

- CVE-2025-26465はクライアント側で「VerifyHostKeyDNS」オプションが有効の場合に影響を受けるとされ、パッチを適用する以外の回避策としてこれを無効化することが挙げられています。
- CVE-2025-26466はOpenSSH 9.5p1(2023年10月リリース)以降にのみ存在し、Linuxディストリビューションによっては安定版においてより以前のバージョンを使用しているため影響を受けない(Debian 12、Ubuntu 22.04、RHEL 9とその派生等が該当。ただしUbuntu 24.04以降は影響)ケースもあります。
- SSHは主にLinuxサーバーをリモートから管理する目的で利用されることから、世界中の攻撃者が日々サービスポート(TCPポート22番)の探索・攻撃を行っており、OpenSSHのアップデートはもちろん、SSHサービスポートへのアクセスを特定のIPアドレスからのみに制限する等の対策をとることも強く推奨されます。

● NEC製のWi-Fiルーター11製品に脆弱性、ファームウェアアップデートを

https://internet.watch.impress.co.jp/docs/news/1663010.html
https://jvn.jp/jp/JVN65447879/index.html
https://jpn.nec.com/security-info/secinfo/nv25-003.html
https://www.aterm.jp/support/tech/2025/0115.html

このニュースをザックリ言うと・・・

- 2月14日(日本時間)、IPA・JPCERT/CCが運営する脆弱性情報サイト「JVN」より、NECプラットフォームズ社(以下・同社)提供のWi-Fiルーター「Aterm」シリーズに脆弱性が存在するとして注意喚起が出されています。
- 1月15日に同社より計11機種において3種類の脆弱点が発表されており、悪用により、クロスサイトスクリプティング(XSS)の実行、機器情報の読み取り、および機器の乗っ取りの可能性があるとされています。
- 今回の脆弱点は対象となる各機種において最新のファームウェアで対策されており、適用を強く推奨されています。

AUS便りからの所感

Impress Watch

- 同社では、発表された脆弱点はいずれも「LAN側からの不正アクセス時の脆弱性」であり、インターネット経由で外部から直接攻撃されることはないとしており、もちろん今日においてはLAN上に別の経路から侵入した攻撃者に狙われる可能性への警戒は欠かせません。
- 同社以外にも言えることですが、サポートが終了した機器については、脆弱性の影響を受けることが発表されてもファームウェアのアップデートが行われないケースもあり、サポートが続いている現行機器へのリプレースを計画すること、かつ組織内で稼働する全ての機器を確実に管理下に置き、一般的な回避策として今回も推奨されているようなWi-Fi接続キーや管理画面のパスワードを複雑なものとすることが肝要です。