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。

●壊れたヘッダーでアンチウイルス等を回避か…細工したZIPファイルによる攻撃手法に注意喚起

https://securityonline.info/cve-2026-0866-malformed-zip-headers-allow-malware-to-slip-past-edr-scanners/
https://kb.cert.org/vuls/id/976247
https://www.digitalsales.alsok.co.jp/col_zombie-zip

このニュースをザックリ言うと･･･

- 3月9日(現地時間)、米CERT/CCより、細工したZIPファイルにより、アンチウイルスソフトやEDRによる検知を回避する攻撃手法について注意喚起が出されています。

- 「Zombie ZIP」等と呼称されるこの手法は、ZIPファイルのヘッダーの一部を改変し、実際には圧縮されているファイルが圧縮されていない状態で格納されていると偽装することにより、当該データ部分が適切にスキャンされることを回避するものとなっています。

- Zombie ZIPによるファイルは、7-Zip等の通常の展開ツールで展開しようとしてもエラーとなるため、エラーを回避して展開するような専用のツールも用意することにより、検出を潜り抜けたマルウェア等を実行させるといったシナリオが挙げられています。

- この手法を発表したBombadil Systems社のセキュリティ研究者によれば、51種類のアンチウイルスソフトのうち50種類がZombie ZIPによるファイルを検知できなかったとし、さらにアンチウイルス用テストファイル「eicar」についても、同様に検知を回避するような細工を行うことに成功したとしています。

AUS便りからの所感等

- 細工したZIPファイルによるスキャン回避の手法はかつて2004年にも類似したものが発表されており、こちらは圧縮したファイルのサイズが0バイトであると偽装するものだったとのことです。

- 不正なZIPファイルによる攻撃は他にも大容量のサイズに展開される「ZIP爆弾」という手口も知られ、2019年には、数GB～数PBのデータとなるものも発表されています。

- 前述の通り殆どのアンチウイルスソフトが検知できなかったとしていますが、手法が公開されたことにより、今後このような不審な形式のファイルについてもデータを展開することなく検知するよう対応がとられることに期待したいものです。

Daily CyberSecurity

Vulnerability Report

CVE-2026-0866: Malformed ZIP Headers Allow Malware to Slip Past EDR Scanners

Ddos March 10, 2026 3 minutes read 0

A newly detailed vulnerability, CVE-2026-0866, is highlighting a fundamental blind spot in how many Antivirus (AV) and Endpoint Detection and Response (EDR) tools handle compressed files. By strategically "breaking" the metadata of a ZIP archive, attackers can create "shadow archives" that appear corrupted to security scanners but remain fully functional for malicious execution.

The core of the issue lies in the trust that security engines place in ZIP metadata. Standard archives contain fields that declare the version, flags, and—crucially—the compression method used.

● 2月度のフィッシング報告件数は57,096件、プロキシー・ボットネット無力化で大幅減少

https://www.antiphishing.jp/report/monthly/202602.html

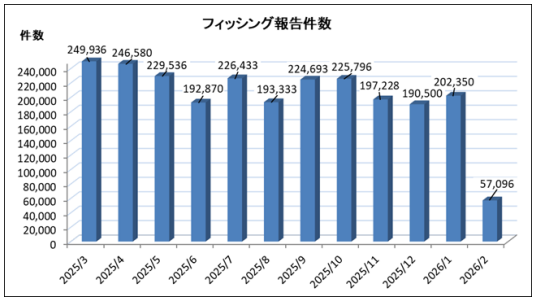
このニュースをザックリ言うと・・・

- 3月12日(日本時間)、フィッシング対策協議会より、2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。
- 2月度の報告件数は57,096件で、1月度(https://www.antiphishing.jp/report/monthly/202601.html)の202,350件から145,254件減少しています。
- フィッシングサイトのURL件数も17,037件で1月度(50,822件)から33,749件減少しています。
- 悪用されたブランド件数は96件で1月度(108件)から12件減少、最も報告が多かったブランドはマネックス証券が約23.9%、次いでAmazon(約11.7%)、VISA、三井住友カード、Appleと合わせて約52.5%、さらに1,000件以上報告された15ブランドまで含めると約75.1%となっています。

AUS便りからの所感

- 1月末に海外におけるレジデンシャルプロキシやボットネットの無力化が行われ、さらに2月後半に中国において旧正月となったことから、2025年3月以降19万件～24万件台で推移していた報告件数が一気に減少し、2024年2月(55,502件)以来の5万件台となっています。
- 同協議会の調査用メールアドレスに届いたフィッシングメールの送信元IPアドレスについて、PTRレコード(IPアドレスからの逆引き)設定なしのものは約59.1%(1月度約90.7%)、一方Google Cloudサービスが発信元のものは約34.5%(1月度約8.6%)で、Google Cloudサービスへの移行が多くあった模様です。
- 4月3日現在、手元で観測する限り、日々届いている迷惑メールの量は1月時点の2割～3割程度ながら徐々に回復の傾向が見られており、これまで同様決して油断することなく、不審なメールに対しネット上での報告等と照合し、本物のサービスのサイトへは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アクセスする、またログイン時に多要素認証を設定する等、フィッシングによってアカウントを奪取されたり、不正取引等の被害を受けないための行動をとっていくことが肝要です。

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



●バッファロー製のWi-Fiルーター等42機種に脆弱性…ファームウェア更新の有無、自動更新が有効かの確認を

https://internet.watch.impress.co.jp/docs/news/2096349.html
https://www.buffalo.jp/news/detail/20260323-01.html
https://jvn.jp/jp/JVN83788689/

このニュースをザックリ言うと・・・

- 3月23日(日本時間)、バッファロー社より、同社製Wi-Fiルーター・中継器・VPNルーター等計42機種に複数の脆弱点が存在するとして注意喚起が出されています。
- 脆弱点は6点が存在し、ログイン画面にアクセス可能な攻撃者により、設定情報の奪取・機器上での任意のコード実行および機器の強制再起動が可能とされています。
- 同27日にはIPA・JPCERT/CCが運営する脆弱性情報サイト「JVN」からも注意喚起が出されています。

AUS便りからの所感

- 多くの機種はファームウェアの更新で対策されていますが、一部Wi-Fiルーター7機種についてはサポート期間が終了しており、リプレースを行うよう呼び掛けられています。
- またファームウェアの更新が提供されている機種の一部では自動更新機能が有効でない可能性があり、必ずメーカーの情報を参照の上、管理画面でファームウェアのバージョンを確認することが肝要です。
- 脆弱性のある機器に外部から侵入され、ボットネットに組み込まれる恐れがあるため、組織内で使用している機器をすべて管理下に置き、サポート切れの機器については確実にリプレースできるような体制を必ず用意しましょう。

Impress Watch

バッファローのネットワーク製品に複数の脆弱性、ファームウェアの更新など対策方法の確認を

一部製品はサポート終了済み、買い替えの検討を

渡邊 悠太　2026年3月26日 10:20

WCR-1166DHPL

株式会社バッファローは3月23日、同社が販売するWi-Fiルーターなどのネットワーク製品において、複数の脆弱性があるとして情報を公開した。ファームウェアのアップデートで対策できる製品と、サポートが終了しているためアップデートが提供されない製品が存在する。

想定される影響は製品によって異なるが、次のような影響を受ける可能性がある。

- 当該商品のログイン画面にアクセスできる攻撃者によって、設定情報を窃取され