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。

● Webサイトアクセスで不審なダイアログ表示…スクリプトの削除忘れ原因

https://diskunion.net/portal/ct/news/article/1/140606

このニュースをザックリ言うと・・・

- 6月1日(日本時間)、CD・レコードショップチェーンのディスクユニオン社より、同社サイトへのアクセス時にユーザーID・パスワードの入力を求める不審なダイアログが表示されていたと発表されています。

- 発表によれば、5月31日夜から6月1日朝にかけて事象の発生を確認しており、外部サービス「Polyfill[.]io」を経由して表示されていたものとしています。

- 現在は当該サービスへの参照を削除して対応済みとしており、誤ってダイアログにID・パスワードを入力した場合は、同サイトあるいは入力したアカウント情報を使用しているサービスについてパスワードを変更するよう呼び掛けています。

- またX上では、いくつかのWebサイトで同様の事象が発生していたことが相次いで報告されており、いずれも「Polyfill[.]io」が原因とされています。

AUS便りからの所感等

- 「Polyfill[.]io」は元々は新しいブラウザーのみが対応する機能を古いブラウザーでも使用できるようにするためのJavaScriptライブラリーおよびその配布サイトで、2024年に外部からの買収を受け、スクリプトの改ざんが報告された後、サイトのドメイン名が停止される事態となっていました(「AUS便り 2024/07/04号」参照)が、そのドメイン名が第三者に取得された可能性があります。

- スクリプトの安全なバージョンをCloudFlare等が配布しているとはいえ、もはやこれを必要とする古いブラウザー(IE11およびそれ以前等)は実質使われておらず、また2年前に前述した事案が発生していたにも拘らず、問題のサイトからのスクリプトの読み込みを削除していなかったサイトが散見された点については、サイトの管理者が、このようなネット上のトレンドやニュース、そもそもサイトが閉鎖されていたことでスクリプトの読み込みエラーが発生していたこと等に無頓着であり、運用保守体制が不十分であるとするセキュリティ界隈からの指摘もみられます。

- Webサイトの開発・保守にあたっては、Webページ上からどの外部サービスにアクセスしてスクリプトやその他データ・コンテンツの読み込みを行っているかについても常に管理を怠らず、不必要となったものは確実に削除できる体制をとることが肝要です。


【重要なお知らせ】不審な認証画面について

PORTAL　ニュース

2026.06.01

disk union ディスクユニオン

DIVE INTO MUSIC.

2026年5月31日夜から6月1日朝にかけて、当サイトの一部ページにおいて、外部サービス(polyfill.io)を経由した不審な認証画面が表示される可能性がある事を確認いたしました。現在は該当サービスを削除し、対応を完了しております。

万が一、当該画面にてID・パスワード等をご入力されたお客様は、速やかに当サイトおよび同一情報を使用されている各サービスのパスワード変更をお願いいたします。

● 4月度フィッシング報告件数は151,112件…中国系ボットネット復活か

https://www.antiphishing.jp/report/monthly/202604.html

このニュースをザックリ言うと・・・

- 5月21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。

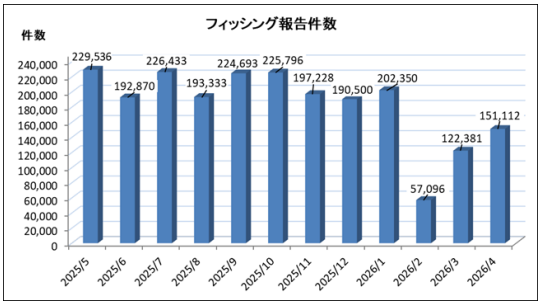
- 4月度の報告件数は151,112件で、3月度(https://www.antiphishing.jp/report/monthly/202603.html)の122,381件から28,731件増加しています。

- フィッシングサイトのURL件数は66,574件で3月度(69,936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49.0%)、 .cn(約22.3%)、 .jp(約17.5%)で全体の約88.8%、次いで.cfd(約5.2%)、 .net(約2.0%)、.shop(約0.9%)、.info(約0.7%)、 .club(約0.6%)、 .cyou(約0.4%)と併せて、全体の約98.6%を占めたとしています。

- 悪用されたブランド件数も117件で3月度(123件)から6件減少、最も報告が多かったブランドはAmazonが約14.4%、次いでApple(約11.6%)、楽天カード、セゾンカード、PayPayカードと合わせて約47.8%、さらに1,000件以上報告された35ブランドまで含めると約91.5%となっています。

AUS便りからの所感

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



- 同協議会の調査用メールアドレス宛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、国別の割合はCN約75.1%、US約11.4%、SG約5.0%、HK約3.4%、KR約2.2%となり、1月末に激減したボットネット経由とみられるCNの一般向け回線からの配信が再び急増したと分析しています。

- また、モバイル回線以外のアクセス元では閲覧できないフィッシングサイトが増加し、稼働確認や停止調整の回避を試みているとし、こういった調査・作業のためにモバイル回線以外からPCによってアクセスする可能性が高いことを見越している他、PCからアクセスする一般ユーザーについてもターゲットとしないというケースも多々あるとみられます(この手の不審なサイトでは、検索エンジンからアクセスしてきた場合にのみ機能し、直接アクセスする場合は表示されないというケースも以前から珍しくありません)。

- また同協議会からはPayPayアプリを悪用しての不正な入金に誘導するフィッシングに度々注意喚起が出されており(「AUS便り 2026/05/18号」参照)、とにかくフィッシングの手口(どこを騙るか、どんな文面のメールやSMSを送るか、最終的な目的は何か)について十分に把握し、毎月のフィッシング報告の「利用者のみなさまへ」に記載された各種対策の実施をはじめ、慎重な行動を心掛けましょう。

● Nginx、5月は2度のセキュリティアップデート

https://rocket-boys.co.jp/security-measures-lab/nginx-rift-cve-2026-42945-heap-buffer-overflow/
https://nginx.org/en/security_advisories.html
https://my.f5.com/manage/s/article/K000161019
https://my.f5.com/manage/s/article/K000161377

このニュースをザックリ言うと・・・

- 5月13日(現地時間)、Webサーバーソフトウェア「Nginx」の6件の脆弱点を修正するセキュリティアップデート(1.31.0, 1.30.1)がリリースされました。

- 特にrewriteディレクティブの特定の状況下において任意のコード実行が可能となる脆弱点(CVE-2026-42945)について、セキュリティ企業のDepthFirst社からは「NGINX Rift」と呼称され、注意喚起が出されていました。

- しかし、同じくrewriteディレクティブにおいて任意のコード実行が可能な、別の未修正の脆弱点(CVE-2026-9256)が指摘され、同22日にはさらなるセキュリティアップデート(1.31.1, 1.30.2)がリリースされています。

AUS便りからの所感

セキュリティ対策Lab

- Webサーバーにおけるセキュリティアップデートは、5月4日にもApache HTTP Serverにおいて2.4.67がリリースされています(「AUS便り 2026/05/08号」参照)。

- 6月3日時点、Linuxディストリビューションの対応は、RHEL派生(Almalinux・Rocky Linux・Oracle Linux等)においてCVE-2026-42945にのみ対応、一方Amazon LinuxおよびDebian・UbuntuではCVE-2026-9256が未対応とされており、今後もパッケージの更新が随時行われた際は速やかに適用を行いましょう。

- 厳密には、前述した2件の脆弱点によって任意のコード実行を行うにはASLRというセキュリティ機能が無効化されている(もしくは回避される)ことが条件ですが、ASLRが有効とされる一般的なLinux環境でもNginxの子プロセスをクラッシュさせられる可能性があり、rewriteディレクティブの設定の有無ないし設定内容の確認、回避策としてその修正を行うことが推奨されます。