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。

●Clickfixの亜種か…偽のブルースクリーンからコマンド実行、マルウェア感染に誘導

https://japan.zdnet.com/article/35242455/
https://www.securonix.com/blog/analyzing-phaltblyx

このニュースをザックリ言うと･･･

- 1月5日(現地時間)、セキュリティ企業のSecuronix社より、ユーザーをマルウェア感染に誘導する新たな攻撃の手口について注意喚起が出されています。

- 「PHALT#BLYX」と名付けられたこの手口では、いわゆる「ブルースクリーン(BSoD)」に似せた全画面表示を行い、復旧のための手順と偽ってトロイの木馬「DCRat」へ感染させようとするとのことです。

- 表示されている復旧手順において「Win+R」「Ctrl+V」「Enter」を押すよう指示し、PowerShellスクリプトを実行させようとする、いわゆる「ClickFix」攻撃の亜種とされており、Securonix社では、この手口の回避のため、従業員に対しClickFix攻撃について周知させ、「ファイル名を指定して実行」やPowerShellコマンドラインに不審なスクリプトを貼り付けないよう警告すること等を呼び掛けています。

AUS便りからの所感等

- Booking.comの予約キャンセル通知を騙るメールからフィッシングサイトに誘導、「ロードに時間がかかっている」という偽のエラーダイアログ上でボタンをクリックさせることにより偽のBSoDを表示、前述の手順でPowerShellスクリプトを実行させることにより、Windowsデフォルトのアンチウイルスによる防御機構を無効化した上で、不正なファイルをダウンロードして実行させるとしています。

- 全画面表示で相手を騙し、正常な判断を失わせる手口としては、既に偽のセキュリティ警告による「サポート詐欺」が知られており、今回のものもIPAによる特集ページ(https://www.ipa.go.jp/security/anshin/measures/fakealert.html)が参考となるでしょう。

- 実際のBSoDにおいてはあらゆるキー操作が効かなくなり、そもそも「Win+R」を押しても「ファイル名を指定して実行」のダイアログは表示されず、逆に今回のケースであれば、サポート詐欺と同様に「ESCキーを一定時間押す」、もしくは「Ctrl+Alt+Del」からタスクマネージャーを起動し、ブラウザーのプロセスを強制終了するといった回避策を実行できるよう心掛けることが大切です。

ZDNET

偽の「ブルースクリーン」でユーザーをだます新たなマルウェアに注意

Lance Whitney（Special to ZDNET.com）翻訳校正：矢倉美登里 吉武稔夫（ガリレオ） 2026-01-08 09:58

「Windows」の「死のブルースクリーン」（Blue Screen of Death：BSOD）または「ブラックスクリーン」は、本来なら回復不可能なエラーや競合が発生したことを示す兆候だ。だが、サイバー犯罪者らは、ユーザーをだましてマルウェアを実行させる手段としてこの恐ろしいBSODを使うようになった。

サイバーセキュリティ企業Securonixが追跡した新たなマルウェア攻撃キャンペーンにおいて、攻撃者は悪意あるコードを被害者にコピー＆ペーストさせるために、ソーシャルエンジニアリングの「ClickFix」や、偽の「CAPTCHA」、偽のBSODを利用している。コードが実行されると、ロシアとつながりがあるRAT（リモートアクセス型トロイの木馬）が仕込まれ、犯罪者がリモートからPCを乗っ取って別のマルウェアを仕込めるようになる。

●国内サイバー攻撃、不具合による大規模障害等…JNSA「セキュリティ十大ニュース」発表

https://www.jnsa.org/active/news10/2025.html
https://ascii.jp/elem/000/004/364/4364678/

このニュースをザックリ言うと・・・

－12月25日(日本時間)、日本ネットワークセキュリティ協会(JNSA)より、「2025セキュリティ十大ニュース」が発表されました。

－サイバー攻撃によるセキュリティインシデント関連では、1位にアサヒグループホールディングス等への「相次ぐ企業へのサイバー攻撃」、2位にこの事件にも関連して「サプライチェーンに波及するサイバー被害、賠償問題に発展するケースも」、3位「金融庁、証券口座乗っ取り被害急増で注意喚起」、4位「生成ＡＩ悪用し不正アクセスの中高生3人逮捕」、7位「IIJ不正アクセス、日本取引所グループや地銀など各所に影響」が挙がっています。

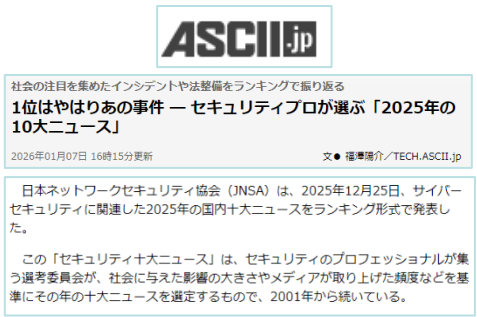
－改修や設定の不具合等で生じた障害関連も、8位「東名高速や中央道などでETC障害」や、番外編として「2025年11月18日はインターネットが壊れた日(Cloudflareにおける障害)」が挙がっています。

AUS便りからの所感

－ランサムウェアが絡むインシデントが2021年以来5年ぶりに1位となっていますが、2024年もKADOKAWAやイセトーへの攻撃がそれぞれ3位・8位につける等、既に10年以上猛威を振るっており、その被害と影響の拡大は「今や災害級」としています。

－他にも5位「能動的サイバー防御関連法案が成立」等のセキュリティにかかわる制度の発足や世相、あるいは9位「FeliCaのセキュリティ脆弱性報道で利用者に不安広がる」のように脆弱性情報の報告と開示の問題も取り上げられています。

－年末年始にこのような振り返りが行われるのはどの分野でも定番で、セキュリティ関連でも他の団体・企業がそれぞれの立場や視野から発表する同種のランキングはそれぞれ異なった顔ぶれ・順位となるとみられ、視点や取り上げる範囲等の違いによる差異を踏まえながら複数の記事を参照することにより、情報セキュリティに関するトレンドを幅広くキャッチアップすることが大切でしょう。


ASCII.jp
社会の注目を集めたインシデントや法整備をランキングで振り返る
1位はやはりあの事件 ― セキュリティプロが選ぶ「2025年の10大ニュース」
2026年01月07日 16時15分更新　文● 福澤陽介／TECH.ASCII.jp
日本ネットワークセキュリティ協会（JNSA）は、2025年12月25日、サイバーセキュリティに関連した2025年の国内十大ニュースをランキング形式で発表した。
この「セキュリティ十大ニュース」は、セキュリティのプロフェッショナルが集う選考委員会が、社会に与えた影響の大きさやメディアが取り上げた頻度などを基準にその年の十大ニュースを選定するもので、2001年から続いている。

●ラジオ局Webサービス、AuDeeメッセージ投稿データなど流出…外部クラウドに不正アクセスか

https://ascii.jp/elem/000/004/364/4364603/
https://www.tfm.co.jp/company/about/ir/news/47630

このニュースをザックリ言うと・・・

－1月6日(日本時間)、株式会社エフエム東京より、同社が以前運営していた複数のサービスに関する個人情報が流出していたと発表されました。

－対象となるのは、2025年9月まで運営していた音声プラットフォーム「AuDee」のメッセージフォーム投稿データの一部、2023年1月まで運営していた「マイスタジオ」他番組関連サービスのユーザー情報に関する、ユーザーネーム(ラジオネーム等)・性別・年齢・職業種別・都道府県・投稿メッセージ本文およびメールアドレス等とのことです。

－年初より一部SNS等において、同社のサーバーが攻撃を受け大量の個人情報が流出したとする投稿があったことを受け調査した結果、ユーザー統計分析用に利用している外部クラウドサービス上のユーザー属性情報の一部が、何らかの原因により流出していたものとしています。

AUS便りからの所感

－同社運用サーバーにおける不正アクセスおよび情報持ち出しの痕跡、および地上波ラジオ番組のメッセージフォームへの書き込みの流出はなかったとしており、また流出したとされるデータについても分析用に加工され、氏名・住所・電話番号・ログインパスワード・クレジットカード情報等は含まれていないとのことです。

－会社が運営するサーバーについて防御を固めることはもちろん、外部サービスの利用にあたっても、アカウントの管理・強固なパスワードの設定・データへのアクセス許可設定の確認等を怠りなく実施すること、また社内PCへのマルウェア感染を踏み台にしてのアクセスの可能性も鑑み、アンチウイルス・UTMによる防衛を確実に行うこと等が肝要です。


ASCII.jp
TOKYO FMにサイバー攻撃　投稿者の情報流出
2026年01月07日 13時15分更新　文● スミーレ（@sumire_kon）
エフエム東京（TOKYO FM）は1月6日、同社が利用する外部クラウドサービス上のデータの一部が流出したことを公表した。
流出が判明した情報の概要は以下のとおり。当該データはいずれも分析用に加工されたもので、氏名、住所、電話番号、ログインパスワード、クレジットカード情報は含まれていない。
●情報流出の概要（1月6日時点）
■流出した情報（概要）
・音声プラットフォーム「AuDee」のメッセージフォーム投稿データの一部
・「マイスタジオ」他番組関連サービスのユーザー情報の一部
■流出した情報（具体例）
・ユーザーネーム（ラジオネーム等）
・一部のメールアドレス（ユーザーネームにメールアドレスを記入していた場合など）
・投稿メッセージ本文
・性別
・年齢
・職業種別
・都道府県　など