— AUS（アルテミス・ユーザ・サポート）便り 2025/4/4号 —
https://www.artemis-jp.com

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。

●不正なコマンドを実行させる偽CAPCHAの攻撃に注意喚起

https://www.itmedia.co.jp/news/articles/2503/26/news063.html
https://www.microsoft.com/en-us/security/blog/?p=137933

このニュースをザックリ言うと･･･

- 3月13日(現地時間)、米Microsoft社(以下・MS)より、「ClickFix」と呼ばれる攻撃の活発化が確認されているとして注意喚起が出されています。

- ClickFixはいわゆる「ソーシャルエンジニアリング」攻撃の一種で、偽のエラーページ・CAPTCHA等を表示した上で「1) Win+Rを押す」「2) CTRL+Vを押す」「3) Enterを押す」といった手順をとるよう指示し、これによりPCのマルウェア感染等に誘導するとされています。

- ClickFixは2024年3月頃に存在が確認されており(例えば6月にはProofPoint社から注意喚起が出されています)、今回のMSからの注意喚起では、12月に旅行予約サイト「Booking.com」を騙るフィッシングサイトで用いられていた事例が取り上げられています。

AUS便りからの所感等

- 前述した手順は、1)でWindowsの「ファイル名を指定して実行」のウィンドウを開き、2)で事前にクリップボード内にコピーされた不正なコマンド(PowerShellスクリプト)をペーストし、3)でそのコマンドを実行させるという流れとなっていますが、さらに1)の前段で不正なコマンドを事前にクリップボードへコピーするため、何らかのボタンのクリックを指示したり、密かに何らかの動作を行うよう仕向けたりしている模様です。

- このような、ユーザー側に過剰に協力を求める不審な手順への誘導に遭遇した場合は、それが攻撃手法の一つとして既に警告が出ていないか、ネット上で検索を行って確認すること、また常日頃からどんな攻撃手法が出回っているかの情報収集を行いつつ、ブラウザー・メーラー・アンチウイルスソフト・UTM等のセキュリティ機能により、不審なWebサイト・偽メールからの防御を図ることが肝要です。

ITmedia NEWS

この頃、セキュリティ界隈で

その「私はロボットではありません」は本物？　マルウェア感染狙う“偽CAPTCHA”出現　米Microsoftが注意喚起

2025年03月26日 08時00分 公開　［鈴木聖子，ITmedia］

Webサイトにログインしようとすると時折表示される「私はロボットではありません」の画面。不正アクセス防止を目的としたCAPTCHAの一種だが、この仕組みを偽装してユーザーのクリックを誘い、Windowsをマルウェアに感染させようとする手口が横行しているという。

「ClickFix」と呼ばれるこの手口では、普段利用しているサービスのログイン画面に見せかけた詐欺サイトにユーザーを誘導し、不正プログラムと人間のユーザーを見分ける目的で使用される「私はロボットではありません」を装うボタンを表示する。ユーザーがこのボタンをクリックすると、確認のためと称して次のようなキーボード操作を求められる。

> (1) Windowsボタンと「R」を押す
> (2) 「CTRL」と「V」を押す
> (3) 「Enter」を押す

(1) の手順ではWindowsの「ファイル名を指定して実行」のウィンドウを表示し(2)の手順で不正サイトの仮想クリップボードからコピーした悪質なコードをペースト。(3) のEnterキーを押してしまうとマルウェアが実行される。

●「Have I Been Pwned」創設のセキュリティ専門家、フィッシングによりML乗っ取り、情報流出の被害

https://codebook.machinarecord.com/threatreport/37900/
https://www.theregister.com/2025/03/25/troy_hunt_mailchimp_phish/
https://www.troyhunt.com/a-sneaky-phish-just-grabbed-my-mailchimp-mailing-list/

このニュースをザックリ言うと･･･

－3月25日(現地時間)、流出メールアドレス・パスワードのチェックサービス「Have I Been Pwned」等で知られるセキュリティ専門家トロイ・ハント氏が、フィッシング攻撃を受け、メーリングリスト管理アカウントへ不正ログインされる被害を受けたとIT系ネットメディア「The Register」で報じられました。

－同氏のブログでも経緯が報告されており、メール配信サービス「MailChimp」のアカウントが制限されたとするフィッシングメールから、誘導先のフィッシングサイトでログイン情報を入力したことにより、自身のメーリングリストに登録されたメールアドレス約16,000件等を奪取されたとしています。

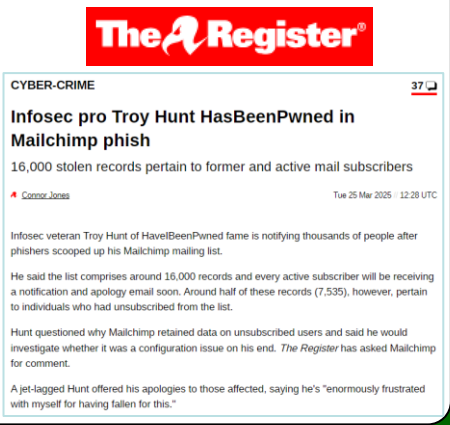
－同氏はパスワード管理ツールを使用していましたが、フィッシングサイトのため自動入力が動作しなかったにも拘らず、手動でアカウント情報の入力を行ってしまったとしています。

AUS便りからの所感

－「フィッシングサイトではパスワード管理ツールが自動入力を行わない」ことはフィッシング回避のための有効なセオリーとしてよく挙げられる一方、「アカウント情報を別のドメイン名のサイトで入力しなければならない」場面も少なからず存在します。

－同氏はMailChimpの認証で採用されていたワンタイムパスワード(OTP)等の二要素認証(2FA)はフィッシングや中間者攻撃への耐性がない(フィッシングサイトに入力されたOTPが本物のサイトに中継される等の可能性あり)と指摘、それらの攻撃に耐性のあるとされる、ハードウェアキーやパスキー等による2FAを採用すべきとしています。

－「著名なセキュリティ専門家ですらフィッシング攻撃に騙されてしまった」という今回の出来事が、単にセンセーショナルな話題のみで消化されるのではなく、いかにも見破りやすいものだけとは限らない、巧妙なフィッシングの存在への警戒や、フィッシング対策の観点からのパスキーの採用等が進む一助となるかに注目されるところです。


The Register

CYBER-CRIME 37

Infosec pro Troy Hunt HasBeenPwned in Mailchimp phish

16,000 stolen records pertain to former and active mail subscribers

Connor Jones Tue 25 Mar 2025 12:28 UTC

Infosec veteran Troy Hunt of HaveIBeenPwned fame is notifying thousands of people after phishers scooped up his Mailchimp mailing list.

He said the list comprises around 16,000 records and every active subscriber will be receiving a notification and apology email soon. Around half of these records (7,535), however, pertain to individuals who had unsubscribed from the list.

Hunt questioned why Mailchimp retained data on unsubscribed users and said he would investigate whether it was a configuration issue on his end. *The Register* has asked Mailchimp for comment.

A jet-lagged Hunt offered his apologies to those affected, saying he's "enormously frustrated with myself for having fallen for this."

●関西万博、過剰な個人情報収集に批判…一部項目削除

https://www.sankei.com/article/20250331-BBZVRA46BRLLJHRL3L56XS2S4A/
https://www.expo2025.or.jp/news/news-20250328-04-2/

このニュースをザックリ言うと･･･

－3月28日(日本時間)、2025年大阪・関西万博を運営する日本国際博覧会協会より、万博入場券のオンライン購入等に関連する個人情報保護方針の改訂が発表されました。

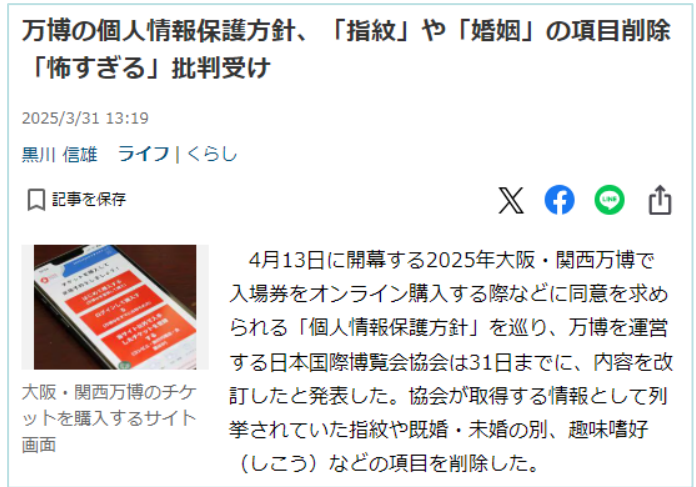
－入場券のオンライン購入やパビリオン・イベント予約のための「万博ID」登録時に収集される個人情報として、当初含まれていた「指紋」「SNSのアカウント情報」「既婚・未婚」「子供の有無」「趣味嗜好」が除外されています。

－収集される個人情報の種類が過剰であると批判を受けており、改訂により前述のものについては収集されないことになりました。

AUS便りからの所感

－個人情報提供先として当初「政府・地方自治体・外国政府」「SNS事業者・広告関係会社・データ分析事業者」が含まれていましたが、これらも除外されています。

－来場者の識別のため「パスポート番号」「顔画像」「音声」等は引き続き収集するとしていますが、個人情報をはじめとした各種情報について収集すべき種類を精査し必要最低限の収集とすることは、万が一の不正アクセスで個人情報の大量流出が発生した場合の被害を抑えることを鑑みても重要と言えます。


経済新聞 THE SANKEI NEWS

万博の個人情報保護方針、「指紋」や「婚姻」の項目削除 「怖すぎる」批判受け

2025/3/31 13:19

黒川 信雄　ライフ | くらし

記事を保存

大阪・関西万博のチケットを購入するサイト画面

4月13日に開幕する2025年大阪・関西万博で入場券をオンライン購入する際などに同意を求められる「個人情報保護方針」を巡り、万博を運営する日本国際博覧会協会は31日までに、内容を改訂したと発表した。協会が取得する情報として列挙されていた指紋や既婚・未婚の別、趣味嗜好（しこう）などの項目を削除した。