— AUS（アルテミス・ユーザ・サポート）便り 2025/9/2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。

●不正ログイン被害の相談増加、なりすましで電話番号・SMS認証コードを奪取するケース等…IPAより注意喚起

https://www.ipa.go.jp/security/anshin/attention/2025/mgdayori20250828.html
https://www.pref.kagoshima.jp/ja13/cyber_teguchi22.html

このニュースをザックリ言うと・・・

- 8月28日(日本時間)、IPA「安心相談窓口だより」にて、インターネットサービスへの不正ログインによる被害が増加中であると発表されています。
- 発表によれば、月間の相談件数が2～6月にかけて80～90件台で推移していたところ、7月には144件に急増したとしています。
- 不正ログインに至る要因として、「単純なパスワードを推測される」「特定の(他の)インターネットサービスから漏えいしたパスワードを使われる」「フィッシングサイト等に騙されて悪意ある第三者にパスワード等を教えてしまう」が挙げられています。

AUS便りからの所感等

- 相談が多く寄せられたより具体的な手口として、Instagram上の知り合いになりすました攻撃者からDMが届き、電話番号を教えてしまう→SMSで届いた認証コードを相手に教えてしまう→不正ログインされ、パスワードの他に電話番号・メールアドレス・多要素認証のための設定を変更されてしまう、というものがあるとのことです。
- この事例は鹿児島県警のページにおいてより分かりやすい流れが掲載されています。
- 常日頃から警察・政府機関・各セキュリティ組織等の注意喚起においてどんな攻撃の手口が用いられているかの情報収集を行い、前述のように電話番号やメールアドレスの他、SMSやメールで届いた情報も随時送るよう要請するのはアカウント乗っ取りを意図したものであると心得、決して従わないことに注意してください。

IPA

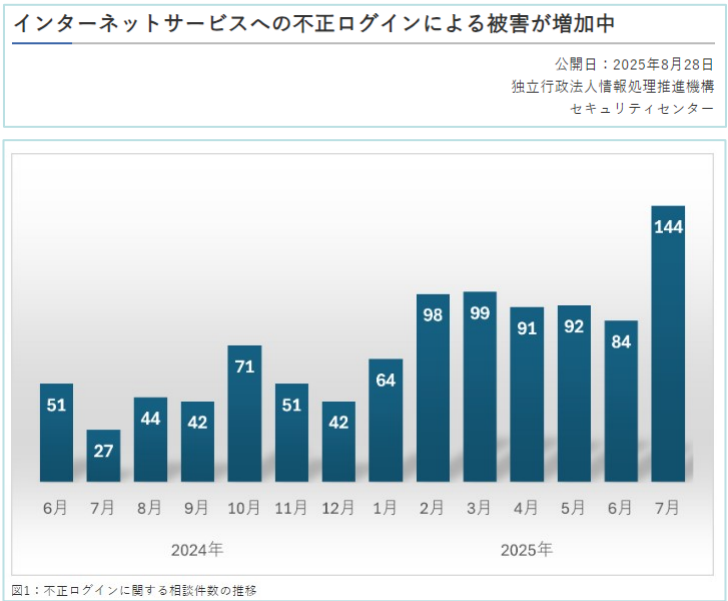
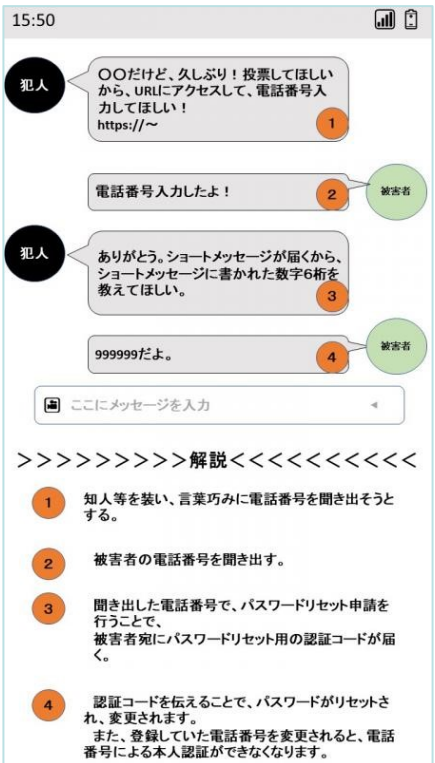


図1：不正ログインに関する相談件数の推移

K.P. 鹿児島県警察



●複数のWordPressサイトでトロイの木馬が埋め込まれる改ざん事例、ラック社が注意喚起

https://www.lac.co.jp/lacwatch/alert/20250826_004473.html

このニュースをザックリ言うと・・・

- 8月26日(日本時間)、国内情報セキュリティ大手のラック社より、7月頃から複数のWordPressを使用したWebサイトで改ざんが確認されているとして注意喚起が出されています。

- 改ざんにおいてはページ内に「0x1c8c5b6a」といった16進数形式の文字列が不正に挿入される等が共通した特徴とされており、同社が用意したハニーポット(囮サイト)に対し、約2日に1回の頻度で複数回の攻撃が観測されたとしています。

- 改ざん行為は「Efimer」と呼ばれるトロイの木馬型マルウェアによるものと推測されており、今後も国内のWordPressサイトがターゲットとなる可能性があるとしています。

AUS便りからの所感

- ハニーポットへの攻撃にあたっては、WordPressのXML-RPC APIに対する不正アクセスで不審な文字列を挿入する投稿を試行し、またwp-jsonからユーザー一覧を取得した様子が見られたとしています。

- アクセスの際、ユーザー名に「admin」とサイトのドメイン名を使用した41パターン程度の認証情報を用いていることが確認されたとしており、admin等で非常に簡単なパスワードを設定している場合はたちどころに管理者権限を奪取され、不正なプラグインのインストール等の被害を受けることでしょう。

- 同社では「管理画面のパスワード強化」「不要なアカウントの削除・整理」「XML-RPCの無効化（不要な場合）」「サーバー上の不審なサービス・プロセスの確認」「WordPressに導入されているプラグインの精査（不審なものがないか確認）」「バックドアの有無のチェック」を呼び掛けており、これらの他にも実績のあるセキュリティ機能を提供するプラグインの導入が強く推奨されます。

●VPNサービスを提供するChrome拡張機能がスパイウェアに…10万回インストールの実績

https://forest.watch.impress.co.jp/docs/news/2041333.html
https://koi-security.webflow.io/blog/spyvpn-the-vpn-that-secretly-captures-your-screen

このニュースをザックリ言うと・・・

- 8月19日(現地時間)、セキュリティ企業のKoi Security社より、Chromeの拡張機能「FreeVPN.One」が、インストールしたPC上で不審な挙動をとるスパイウェア化していたとして注意喚起が出されています。

- 当該拡張機能は名前のとおり無料のVPNサービスを提供するものとみられますが、4月リリースのv3.0.3で拡張から任意のサイトにアクセスする権限を要求し、7月リリースのv3.1.3でサイトアクセス時のスクリーンショットを密かに外部に送信するようになったとしています。

- FreeVPN.Oneは当初は正当なVPNツールとしてGoogle公式の拡張機能ストアに登録され、10万件以上インストールされる程の実績があったとのことです。

AUS便りからの所感

- 9月1日時点で拡張機能ストアから当該拡張は削除、FreeVPN.Oneの公式サイトも繋がらなくなっていますが、スクリーンショットの送信先とされるサイトは生きている模様ですので、万が一当該拡張機能をインストールしている場合は速やかに削除してください(IDが「jobiffkllmgnkppebelchllpdbnibihel」のものが該当します)。

- ブラウザーの拡張機能を介しての攻撃の事例として、先日は「uBlock Origin」の偽物が拡張機能ストアに登録されていたことが報告されており(「AUS便り 2025/08/04号」参照)、一般論としてブラウザーへの拡張機能のインストール・有効化は必要最低限に留め、使用しない(しなくなった)ものや身に覚えのないものは削除するという自衛策をとった上で、使用中の拡張機能についてもSNS上等の評判を注視することが望ましいでしょう。

- 最初は正常な挙動を示してユーザーを安心させるケースの他に、当初マルウェア化することを意図せず、所有者が変更されて方針等が変更されるケースも多く、これらに対しGoogle側で今後有効な対策を打つことができるかが注目されます。