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。

●Netflix配信人気ドラマのフィッシングサイト…カスペルスキーが注意喚起

https://www.itmedia.co.jp/news/articles/2110/29/news171.html
https://blog.kaspersky.co.jp/squid-game-related-threats/31880/

このニュースをザックリ言うと･･･

- 10月18日(日本時間)、カスペルスキー社より、動画サイトNetflixで配信されている**ドラマ「イカゲーム」に便乗した偽サイト**が多数確認されているとして、同社ブログにて注意喚起が出されています。

- 劇中で使われる**コスチュームの販売**、**暗号資産(仮想通貨)が獲得できるオンラインゲーム**、あるいは**本編等の動画を騙り**、**個人情報を詐取**したり、**マルウェアをダウンロード**させたりするケースが挙げられています。

- サイトは9月～10月にかけて多数確認され、偽ファイルともども**日本語以外の言語で作成・公開**されていたとのことですが、**今後日本語による類似のものが展開される可能性**もあるとしています。

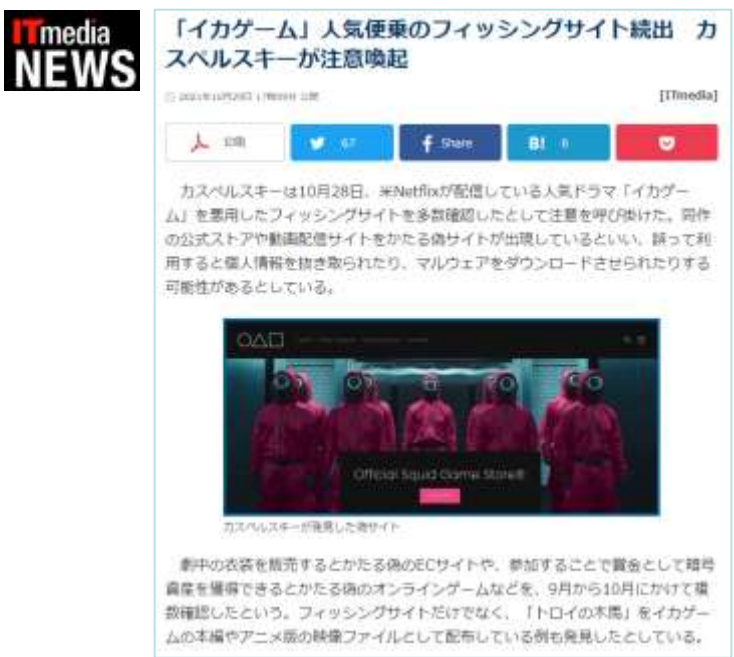
- 同社ではフィッシングの可能性に対するいくつかの回避策を呼び掛けており、例えば「**音楽や動画のファイル**ならば、**拡張子**は『.mp3』『.avi』『.mkv』『.mp4』であるはず(註：『.m4a』『.webm』等もあり)」「『.exe』や『.msi』**ということはありません**」等としています。

AUS便りからの所感等

- **Windowsの初期設定**ではダウンロードした**ファイルの拡張子が表示されず**、このときマルウェアが「***.mp4.exe」というファイル名の場合「***.mp4」と表示されてしまうため、エクスプローラーの「表示」メニューから**「ファイル名拡張子」にチェック**を入れ、**拡張子が表示されるようにする**ことを強く推奨致します(この他、**不自然に長い空白**を入れた「.mp4　　.exe」、さらには**文字が右から左に表示される**Unicode**特殊文字を利用**して偽装する場合もあることに十分注意してください)。

- また、**悪意のあるモバイルアプリ**をGoogle PlayやApp Storeといった**公式のアプリストア以外からダウンロードさせる事例**もありますが、このようなアプリのインストールは**モバイル端末のあらゆる使用権限がアプリに渡される恐れ**があり、インストール時に**不必要に多くの権限が要求される**等不審な様子がみられる場合はインストールを中止するようにし、**必要最低限のアプリのみをインストール**することを心掛けましょう。

- ともあれ、フィッシングに対しては、**公式情報やSNS等での報告を随時確認**しながら慎重に行動すること、Webブラウザー・アンチウイルスソフトおよびUTMにおいて**アンチフィッシング機能をはじめ各種セキュリティ機能を有効に**すること等が重要です。


ITmedia NEWS

「イカゲーム」人気便乗のフィッシングサイト続出　カスペルスキーが注意喚起

[ITmedia]

カスペルスキーは10月28日、米Netflixが配信している人気ドラマ「イカゲーム」を悪用したフィッシングサイトを多数確認したとして注意を呼び掛けた。同作の公式ストアや動画配信サイトをかたる偽サイトが出現しているといい、誤って利用すると個人情報を抜き取られたり、マルウェアをダウンロードさせられたりする可能性があるとしている。

カスペルスキーが発見した偽サイト

劇中の衣装を販売するとかたる偽のECサイトや、参加することで賞金として暗号資産を獲得できるとかたる偽のオンラインゲームなどを、9月から10月にかけて複数確認したという。フィッシングサイトだけでなく、「トロイの木馬」をイカゲームの本編やアニメ版の映像ファイルとして配布している例も発見したとしている。

●スマホゲーム会員サービス、不正ログイン2,846件…二段階認証必須に

https://www.itmedia.co.jp/news/articles/2110/28/news104.html
https://www.klab.com/jp/press/info/2021/1027/klab_id_2.html

このニュースをザックリ言うと・・・

- 10月27日(日本時間)、スマートフォン向けゲーム開発・提供するKLab社より、同社会員サービス「KLab ID」において不正ログインが発生したことが発表されました。

- 不正ログインは10月24日から26日にかけて発生、同サービスユーザー計2,846件の個人情報(メールアドレス・ひみつの質問と回答・生年月日・性別等)や連携しているアプリの情報等が閲覧された可能性があるとしています。

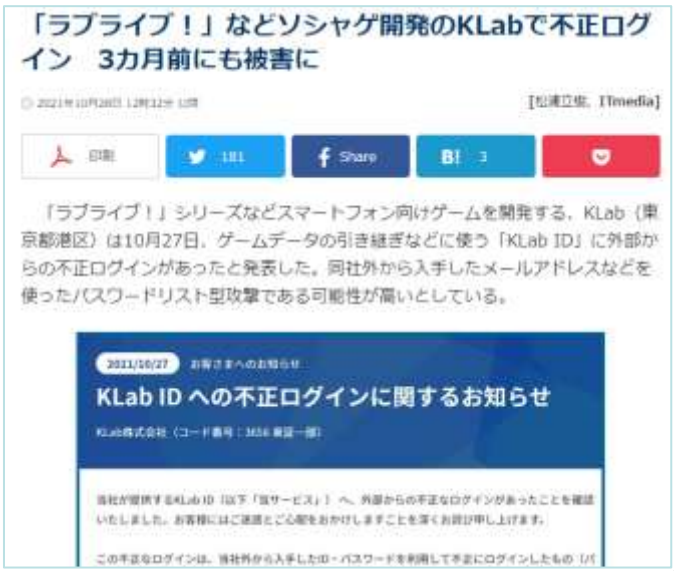
- 他のサービスで流出または不正ログインに悪用されたアカウント情報による、いわゆる「パスワードリスト型攻撃」とされており、7月にも同様のパスワードリスト型攻撃による同規模の不正ログイン被害を受けています。

AUS便りからの所感

- 同社では7月の不正ログイン発生時、ログインが成功しなかった攻撃対象ユーザーの一部も含めパスワードの変更による対応を行っていましたが、今回メールによる二段階認証を全ユーザーにて必須化する対応を行ったことが発表されています。

- パスワード管理ツール「LastPass」の調査では、世界7ヶ国・3,750人のユーザーのうち65%が依然として複数のサイト間でパスワードの使い回しを行っていると回答しているとのことです(AUS便り 2021/10/05号参照)。

- 利用しているサイトにおいてアカウント情報の流出や大規模な不正ログインの発生が発表されていない場合でも、各アカウント間でパスワードの使い回しを行ってないか点検を行い、もし使い回しがある場合は、サイト毎に異なる、推測されにくいパスワードに変更することを心掛け、可能であればLastPassやBitwarden等パスワード管理ツールによるパスワードの生成・管理も検討することを推奨致します。


「ラブライブ！」などソシャゲ開発のKLabで不正ログイン　3カ月前にも被害に

[松浦立樹, ITmedia]

「ラブライブ！」シリーズなどスマートフォン向けゲームを開発する、KLab（東京都港区）は10月27日、ゲームデータの引き継ぎなどに使う「KLab ID」に外部からの不正ログインがあったと発表した。同社外から入手したメールアドレスなどを使ったパスワードリスト型攻撃である可能性が高いとしている。

2021/10/27 お客さまへのお知らせ
KLab ID への不正ログインに関するお知らせ

●プロキシ設定機能を悪用しFirefoxのアップデートを妨害するアドオン、45万人以上がインストールか…Mozillaが注意喚起

https://forest.watch.impress.co.jp/docs/news/1361/780/index.html
https://blog.mozilla.org/security/2021/10/25/securing-the-proxy-api-for-firefox-add-ons/

このニュースをザックリ言うと・・・

- 10月25日(現地時間)、米Mozillaより、Firefoxブラウザーのアップデートを妨害する悪意のあるアドオンが確認されていたとして注意喚起が出されています。

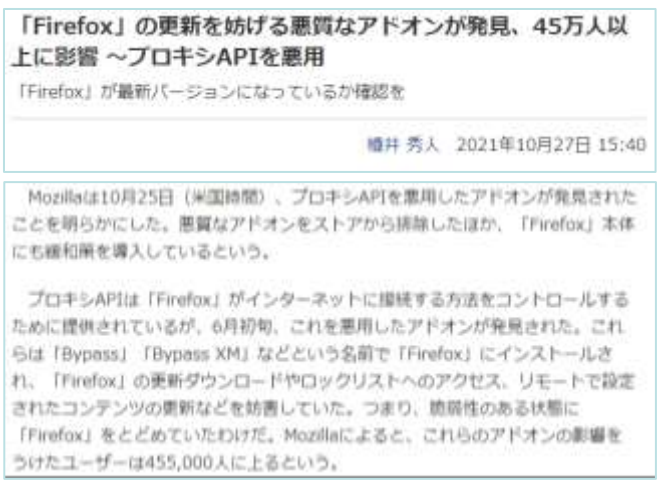
- アドオンは「Bypass」「Bypass XM」といった名前で6月初旬に存在が確認されており、インストールするとFirefoxのプロキシAPIを悪用して、Firefoxの更新ダウンロードサイト等へのアクセスを妨害していたとのことで、注意喚起によれば455,000人に上るユーザーがアドオンをインストールしていたとされています。

- Mozillaでは、最新バージョンのFirefox 93かどうか確認し、そうでない場合は自動ないし手動でアップデートすること、また身に覚えのない不審なアドオンがインストールされていないか確認すること等を呼び掛けています。

AUS便りからの所感

- Firefox 91.1において、更新ダウンロードサイト等にアクセスできない場合はプロキシを用いずに接続する挙動が追加された他、「Proxy Failover」という通常は表示されないシステムアドオンが導入され、旧バージョンも含め追加の緩和策が適用されたとのことです。

- ChromeやEdge等拡張機能に対応する他のWebブラウザーにも言えることですが、ブラウザーの拡張機能はモバイルアプリと同様、悪意のあるものはブラウザーの多くの権限を乗っ取ることも可能とされるため、こちらも不自然に多くの権限が要求される場合はインストールを取りやめ、必要最低限のアドオンのみインストールすることを推奨致します。


「Firefox」の更新を妨げる悪質なアドオンが発見、45万人以上に影響 ～プロキシAPIを悪用

「Firefox」が最新バージョンになっているか確認を

嶋井 秀人　2021年10月27日 15:40

Mozillaは10月25日（米国時間）、プロキシAPIを悪用したアドオンが発見されたことを明らかにした。悪質なアドオンをストアから排除したほか、「Firefox」本体にも緩和策を導入しているという。

プロキシAPIは「Firefox」がインターネットに接続する方法をコントロールするために提供されているが、6月初旬、これを悪用したアドオンが発見された。これらは「Bypass」「Bypass XM」などという名前で「Firefox」にインストールされ、「Firefox」の更新ダウンロードやロックリストへのアクセス、リモートで設定されたコンテンツの更新などを妨害していた。つまり、脆弱性のある状態に「Firefox」をとどめていたわけだ。Mozillaによると、これらのアドオンの影響を受けたユーザーは455,000人に上るという。