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。

● Steamの無料ゲームにアカウント情報を盗むマルウェア…最大1,500人がダウンロード

https://gigazine.net/news/20250218-piratefi-game-steam-password-stealing-malware/
https://www.bleepingcomputer.com/news/security/piratefi-game-on-steam-caught-installing-password-stealing-malware/

このニュースをザックリ言うと･･･

- 2月14日(現地時間)、米IT系メディアBleeping Computerより、PCゲームプラットフォーム「Steam」においてマルウェアを含む無料ゲームが配信されていたと報じられています。

- 問題のゲームは「PirateFi」というタイトルで、インフォスティーラー系マルウェア「Vidar」の一種が含まれていたとして同12日にSteamより注意喚起が出されており、2月6日のリリースから同12日に削除されるまで最大1,500人のユーザーがダウンロードしていたとされています。

- ゲームファイルの解析を行ったSECUINFRA社のセキュリティ研究者によれば、ゲームのダウンロードにより、ブラウザー・メーラー・暗号資産(仮想通貨)ウォレット等の認証情報が漏洩した可能性があるとし、同社からは影響を受けるアカウントのパスワードを全て変更し、可能であれば多要素認証を使用するよう呼び掛けられています。

- またSteamからも、アンチウイルスソフトによるシステム全体のスキャン、身に覚えのないソフトウェアのインストールがないか確認、ないしOSのフォーマットの検討が推奨されているとのことです。

AUS便りからの所感等

- 例えばマルウェアが含まれるAndroidアプリがGoogle公式のアプリストアで配布される(そしてアップロードと削除を繰り返す)ケースは頻繁にみられますが、Steamにおいては前例はあるものの、珍しいこととされています。

- 人気ゲームの海賊版にマルウェアを仕込んで拡散させるケース(Steamとは無関係)も報告されている一方で、タイトルでユーザーが飛びつくようなものでもない、ストアを巡回してたまたま目に付くようなゲームであっても油断はできません。

- アプリやゲームの開発者に対し身元の厳格なチェックや高額な登録料等を要求したとしても、マルウェアによる情報窃取等で元手をとることを目論むような悪意のある開発者は堂々とこれをクリアするものと考えられ、決定的な対策が確立されない限りは、ユーザー側においてアンチウイルス等による防御、Webサイト等のアカウントに対する多要素認証等の強力な保護を確実に粛々と行うことが重要となるでしょう。

GIGAZINE

2025年02月18日 11時00分　ゲーム

Steamで1週間配信されていた無料ゲームに「パスワードを盗み取るマルウェア」が仕込まれていたことが判明

世界最大のPCゲームプラットフォームであるSteamで配信されていた無料ゲーム「PirateFi」に、インフォスティーラー型マルウェアが紛れ込んでいたことが、Steamからユーザーに送付された電子メールによって判明しました。

PirateFi game on Steam caught installing password-stealing malware
https://www.bleepingcomputer.com/news/security/piratefi-game-on-steam-caught-installing-password-stealing-malware/

問題のマルウェア入りゲーム「PirateFi」は、Seaworth Interactiveという開発会社によって2025年2月6日にリリースされ、12日に削除されるまでに800～1500人がインストールした無料ゲームです。

●ふるさと納税特設サイトにSQLインジェクション攻撃、413,867人分の個人情報漏洩

https://www3.nhk.or.jp/lnews/saga/20250212/5080018935.html
https://www.town.genkai.lg.jp/soshiki/19/83169.html

このニュースをザックリ言うと･･･

- 2月12日(日本時間)、佐賀県玄海町より、同町のふるさと納税特設サイトが2024年8月20日に不正アクセスを受け、個人情報が漏洩していたことが発表されました(不正アクセス自体は同27日に初報が発表されていました)。
- 被害を受けたのは、同町へ寄付を行った利用者413,865人分のメールアドレス・ログインパスワード等の情報とされています。
- Webサイトに存在していたSQLインジェクションの脆弱性を突かれたのが原因としています。

AUS便りからの所感

- 返礼品のレシピ紹介ページを2024年5月に改修した際に脆弱性が入れ込まれたとされ、不正アクセスが発覚した8月20日中にアクセス遮断・サイトの閉鎖とともに脆弱性についても修正済み(初報より)としています。
- SQLインジェクションは単にデータベースからの情報奪取のみならず、フォームに入力された個人情報・決済情報を抜き取るようWebサイトを改ざんする等にも悪用される可能性があります。
- 根本的な対策として、Webアプリケーション開発の時点でSQLインジェクション等の脆弱性が入り込まないようにすることが理想ですが、これを悪用するような不正なWebリクエストあるいは内部からの非正規な情報送信を検知、遮断するようなWAF・IDS・IPSの採用も多重防御の意味で十分検討に値します(同町でも再発防止策として同様の対策をとるとしています)。

NHK

玄海町 ふるさと納税サイトからの個人情報流出は４１万人分

02月12日　17時27分

玄海町は、去年８月に発生したふるさと納税の特設サイトへの不正アクセスを受け、寄付をした人など４１万人余りの個人情報が流出したと発表しました。

玄海町は去年８月、町のふるさと納税の窓口の１つである特設サイトが不正アクセスを受けたとして、寄付した人の個人情報が外部に流出していないかなどを調査してきました。

そして１２日、調査結果を公表し、寄付した人のメールアドレスやサイトに入る際のパスワードを暗号化したものなど４１万３８６７人分の個人情報が外部に流出していたことがわかったということです。

● SNS投稿写真からの場所・個人情報「漏れ」に注意喚起…ドコモ「ばくモレ展」

https://news.mynavi.jp/article/20250222-3134140/

このニュースをザックリ言うと･･･

- 2月22日・23日(日本時間)、NTTドコモにより、スマホ写真展「ばくモレ展」が開催されました。
- 表のテーマとしては、10人のインフルエンサーがスマホカメラで撮影した「盛れ」写真を展示するものでしたが、会場の別のスペースでは、写真から撮影した場所や撮影された人の通う学校等の情報が推測できる、即ち情報が「漏れ」るという裏テーマの展示がされています。
- スマホカメラの高性能化により、瞳の中の映り込みから居場所が特定されたり、指紋が悪用されたりしたケースも取り上げられています。

AUS便りからの所感

- 写真から読み取れる情報はもちろん、SNSにおいて出社・帰宅といった行動の投稿から在宅・不在の状態を推測され、例えば空き巣・強盗の侵入の際に情報収集されるケースもあります。
- IPAが挙げている「長期休暇における情報セキュリティ対策」(AUS便り 2024/12/19号参照)においても、「外出前や外出先でのSNS投稿」に注意を呼び掛けており、不用意な行動や写真の投稿を控えることは個人がとるべきれっきとしたセキュリティ対策といえます。

+Digital プラスデジタル　Powered by マイナビニュース

ドコモのインフルエンサー写真展、実はSNSからの情報漏洩への警鐘が目的だった！

掲載日 2025/02/22 14:49　　著者：大塚洋介

NTTドコモが2月22日・23日の2日間、東京・青山で10名のインフルエンサーのスマホカメラで撮影した写真を集めた「ばくモレ展」を開催しています。たんに"盛れている"写真を集めたように思えるこの写真展、実は裏にもうひとつのテーマがあったのでした。

会場入口のパネル。パステルカラーで明るく楽しそうな雰囲気です。実はこのロゴデザインにも裏テーマが隠れています