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。

●「ハリー・ポッター」新作ゲームを悪用…アドウェア入り違法配布等に注意喚起

https://news.mynavi.jp/techplus/article/20230218-2595271/
https://www.malwarebytes.com/blog/news/2023/02/fake-hogwarts-legacy-cracks-lead-to-adware-scams

このニュースをザックリ言うと･･･

- 2月16日(現地時間)、セキュリティベンダーのMalwarebytes社より、発売されたばかりのハリー・ポッターの新作ゲーム「ホグワーツ・レガシー」を悪用したサイバー犯罪について注意喚起が出されています。

- 注意喚起では、「ホグワーツ・レガシー」をクラックした海賊版を無料でダウンロードできると称し、アクティベーションキー入手のためのアンケートとして電話番号等個人情報の詐取を行うWebサイトが挙げられています。

- さらにそのサイトから「Hogwarts_Legacy_Setup.exe」という名前でアドウェアをドロップするトロイの木馬をダウンロードさせる別のサイトにリダイレクトすることも確認されているとのことです。

AUS便りからの所感等

- 先日も、ソフトウェア配布サイトにおいてある配信プラットフォームのゲームが無断配布され、無関係のソフトをダウンロードさせようとしたとして、プラットフォームの運営が批判する事例が発生しています(AUS便り2023/02/14号)。

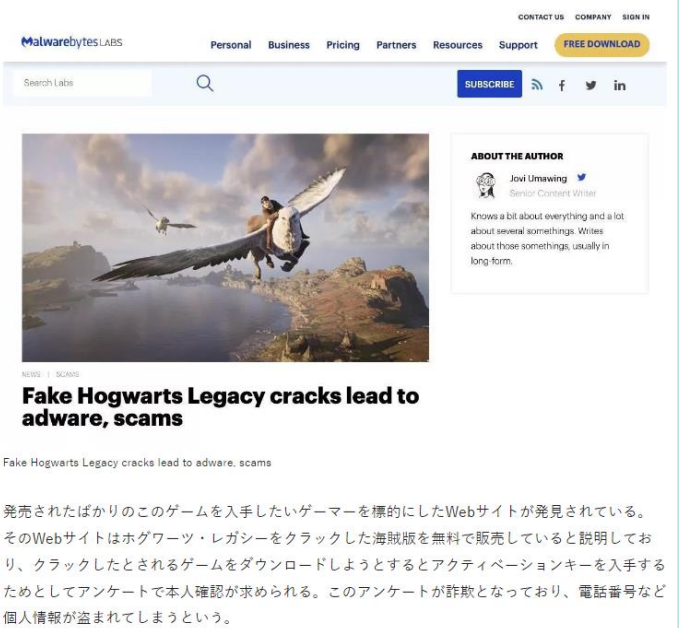
- ゲームをはじめとした有料のソフトウェアを無料で使用できるとしてユーザーを誘い、本物のソフトウェアと一緒に、あるいはまったくの偽物として不正なソフトウェアをインストールさせる手口はサイバー犯罪者にとっての常套手段であり、アンチウイルスがマルウェアを検知して警告を出した場合にこれを無視するといったことは決して行うべきではありません。

TECHF Powered by マイナビニュース

ハリーポッターの新作ゲーム、もうサイバー犯罪に悪用される

掲載日 2023/02/18 08:51　　著者：後藤大地

Malwarebytesは2月16日(米国時間)、「Fake Hogwarts Legacy cracks lead to adware, scams」において、ハリーポッターの新作ゲームソフトがサイバー犯罪に悪用されているとして、注意を呼び掛けた。ローンチされたばかりのゲーム『ホグワーツ・レガシー』がアドウェアの配布や詐欺に悪用され



Fake Hogwarts Legacy cracks lead to adware, scams

発売されたばかりのこのゲームを入手したいゲーマーを標的にしたWebサイトが発見されている。そのWebサイトはホグワーツ・レガシーをクラックした海賊版を無料で販売していると説明しており、クラックしたとされるゲームをダウンロードしようとするとアクティベーションキーを入手するためとしてアンケートで本人確認が求められる。このアンケートが詐欺となっており、電話番号など個人情報が盗まれてしまうという。

●Windows 10上のIE11デスクトップアプリ無効化。非公式な実行方法あり

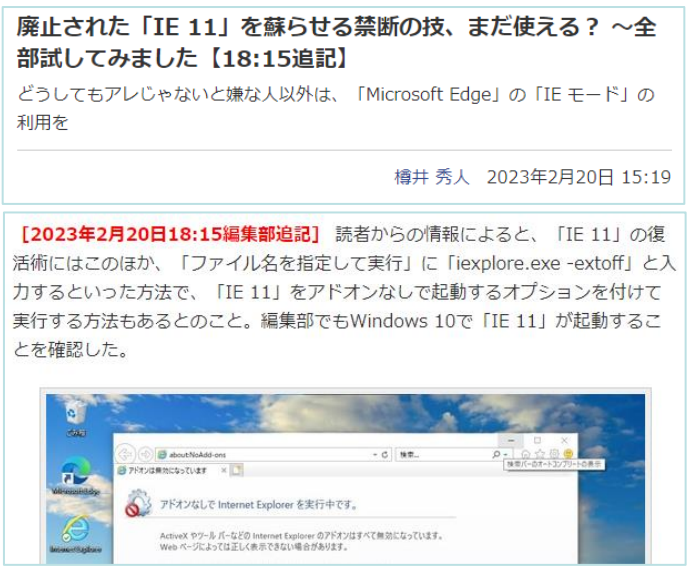
https://forest.watch.impress.co.jp/docs/serial/yajiuma/1480018.html

このニュースをザックリ言うと･･･

- 2月15日(日本時間)にリリースされたマイクロソフト月例のセキュリティアップデートにより、Windows 10上のInternet Explorer(IE) 11 デスクトップアプリの実行が無効化され、実行しようとするとEdgeが代わりに実行されるようになりました。
- 代替策として、Edge内で実行されるIEモードが2029年まで提供される予定です。
- 一方で、インプレス「窓の杜」では、VBScriptやツール、あるいは特別なオプション等により、Windows 10や11でもIE11を起動する方法が紹介されています。

AUS便りからの所感

- IE11のサポートは2022年6月に終了、既に大手Webサイトの多くも対応外としており、表示が崩れる等実用に耐えないケースもあり、上記の記事でも通常はモダンなブラウザーを、また一部例外のサイトについてIEモードを使うよう推奨しています。
- あくまで理論上ですが、攻撃者がVBScriptからIE11を実行してサイトへアクセスするよう指示することにより、IE11で修正されていない脆弱性を悪用される可能性もあるため、そういった指示に決して従わず、システム管理者等に指定された特定のサイトについてのみIEモードでアクセスすることを心掛けるようにしてください。



●ECサイトから9,416件のカード情報流出、不正利用も報告か

https://netkeizai.com/articles/detail/8139
https://www.the-sankyo.com/f/officialdocument

このニュースをザックリ言うと･･･

- 2月20日(日本時間)、アパレル業の三京商会より、同社ECサイトが不正アクセスを受け、クレジットカード情報を含む個人情報が流出したと発表されました。
- 発表によれば、不正アクセスにより、2020年7月28日～2021年12月20日にかけて当該サイトでクレジットカード決済を行った8,794人について、カード情報(名義・番号・有効期限・セキュリティコード)およびサイトのログイン情報(メールアドレス・パスワード※ハッシュ化の有無は不明)が流出したとしています。
- また、2020年7月28日までに当該サイトに登録ないし商品購入を行った最大46,614人の個人情報(氏名・住所・電話番号・メールアドレス・性別・生年月日・職業)、サイトのログイン情報(同上)および注文情報が、および同日までに電話注文を行った2,716名についても個人情報(氏名・住所・電話番号)および注文情報が流出したとのことです。

AUS便りからの所感

- 2月14日に発表されたソースネクスト社からのカード情報等流出(AUS便り 2023/02/14号)同様、サイトの脆弱性を悪用したペイメントアプリケーションの改ざんが流失の原因とされています。
- ここ最近頻発するセキュリティコードも含めたカード情報の流出事故に対し、ネット上では「今時セキュリティコードも保存していたのか？」という批判が毎回散見されますが、フォームを改ざんし、カード情報を詐取・第三者に送信する手口がサーバー上にカード情報を保存しているか否かに拘わらず有効で、近年ほぼ全てのケースについてとられているとされています。
- システム管理側において攻撃者による侵入や改ざんの余地をなくすための対策(Webアプリケーションや OS・各種ソフトウェアを最新に保つ、IDS・IPS・WAFの設置、等)をとることは必要不可欠ですが、のみならず、ユーザー側の行動においても今後さらなる新たな手口に対処できるよう、知識の適切なアップデートが同じく重要と言えます。