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。

●EC-CUBEバージョン4.2.1リリース…クロスサイトスクリプティング脆弱性修正など

https://www.dreamnews.jp/press/0000276160/
https://www.ec-cube.net/info/weakness/weakness.php?id=87
https://jvn.jp/jp/JVN04785663/

このニュースをザックリ言うと･･･

- 2月28日(日本時間)、株式会社イーシーキューブ(以下・同社)より、ECサイト構築用ソフトウェア「EC-CUBE」最新バージョン4.2.1がリリースされています。
- 同時に、バージョン4系および3系・2系に確認され、当該バージョンで修正されたクロスサイトスクリプティング(XSS)の脆弱性(CVE-2023-22438・CVE-2023-25077・CVE-2023-22838)についての注意喚起が同社およびIPA・JPCERT/CCより出されています。
- 脆弱性により、ECサイトや管理画面にアクセスしたユーザーのブラウザー上で不正なスクリプトを実行される可能性があるとされ、4.2.1へのアップデート、あるいは3系・2系についてはパッチの適用が推奨されています。

AUS便りからの所感等

- バージョン4.2.1では、XSSの対策の他にも、クレジットマスター攻撃(大量のクレジットカード番号を送信することにより、実在するカードの不正利用を図る攻撃)への対策等が採用されています。
- 今回報告されたXSSの脆弱性は、管理者の権限で不正な内容の商品登録等を行う必要があるとみられ、幸いにも致命的なものではないようですが、いわゆる「Stored XSS(格納型・持続型XSS)」と呼ばれるもので、過去には不正な注文内容を管理者が閲覧した場合に脆弱性が発動するケースもEC-CUBEには存在していました。
- 近年、ECサイト構築に用いられるソフトウェアの脆弱性を悪用されることにより、入力フォーム等の改ざんが行われ、クレジットカード情報を含む個人情報が流出する事案が多数発生しており、使用しているあらゆるソフトウェアについて更新情報を随時チェックし、速やかにアップデートを行う体制を整えることが肝要です。

● Mac向け動画編集アプリにマルウェア入り海賊版…密かに仮想通貨の採掘

https://gigazine.net/news/20230224-macos-cryptojacking-malware-pirated-software/
https://www.jamf.com/blog/cryptojacking-macos-malware-discovered-by-jamf-threat-labs/

このニュースをザックリ言うと・・・

- 2月23日(現地時間)、MacやiPhone等Apple製品の管理ツールを提供する米Jamf社より、macOS向け動画編集アプリ「Final Cut Pro」にマルウェアが含まれた海賊版が存在すると発表されました。
- 海賊版の実行により、暗号資産(仮想通貨)のマイニングツール「XMRig」がバックグラウンドで動作、匿名通信プロトコルを使用してコンポーネントのダウンロードや採掘した暗号資産の送信を行うとのことです。
- Jamf社では、Apple開発のARMプロセッサの進歩により、これを搭載したMacが大量の計算機リソースを使用するマイニングに悪用される可能性があると警告しています。

AUS便りからの所感

- これまでのmacOSを狙うマルウェアは殆どがアドウェアでしたが、PC上で密かにマイニングを行う「クリプトジャッキング」を狙うものが蔓延しつつあるとしています。
- macOSにはXProtectやGatekeeperといったセキュリティ機構があり、最新版のmacOS Venturaでは海賊版Final Cut Proのインストールはブロックされたものの、マルウェアはその時点でインストールされたことが確認されているとのことです。
- ネットメディアやその取材を受けたAppleはマルウェアが含まれている可能性が高い海賊版をインストールせず、Mac App Storeから正式なソフトウェアをインストールするよう推奨しています。


2023年02月24日 14時00分 セキュリティ

Macに感染して無断で仮想通貨をマイニングするマルウェアが海賊版「Final Cut Pro」に仕込まれている

macOSの動画編集ソフトウェアである「Final Cut Pro」の海賊版に、ユーザーに無断でデバイスのリソースを使用して仮想通貨をマイニングするクリプトジャッキングマルウェアが仕込まれていることを、サイバーセキュリティ企業のJamf Threat Labsが報告しました。今回発見されたマルウェアは巧妙な検出回避システムを備えており、ほとんどのセキュリティソフトでは検出されなかったとのことです。

Beware of macOS cryptojacking malware.
https://www.jamf.com/blog/cryptojacking-macos-malware-discovered-by-jamf-threat-labs/

Pirated Final Cut Pro infects your Mac with cryptomining malware
https://www.bleepingcomputer.com/news/security/pirated-final-cut-pro-infects-your-mac-with-cryptomining-malware/

Mac cryptomining malware found in pirate copies of Final Cut Pro
https://9to5mac.com/2023/02/23/mac-cryptomining-malware/

クリプトジャッキングマルウェアとは、感染したデバイスのコンピューティングリソースを無断で利用し、ユーザーが気づかないうちに仮想通貨をマイニングするマルウェアです。仮想通貨のマイニングにはかなりの処理能力が必要であるため、Appleが開発するMac向けチップが継続的に進歩するにつれ、macOSデバイスはクリプトジャッキングマルウェアの標的として魅力的になっているとのこと

●娯楽施設運営会社のWebサイト、改ざんの被害…一部ページからアダルトサイトへリダイレクト

https://nlab.itmedia.co.jp/nl/articles/2302/28/news173.html
https://www.round1.co.jp/news/pdf/news_20230227.pdf

このニュースをザックリ言うと・・・

- 2月27日(日本時間)、ボウリング場等の娯楽施設を運営するラウンドワン社より、同社Webサイトが不正アクセスを受け、一部ページが改ざんされていたと発表されました。
- 同社の発表およびSNSでの報告によれば、2月25日22時53分～2月26日11時10分において、店舗料金案内ページが改ざんされ、外部のアダルトサイト等にリダイレクトされる状態になっていたとのことです。
- 復旧作業の実施により、現在は正常に表示されるようになっており、個人情報の流出等も確認されていないとのことです。

AUS便りからの所感

- Webサイト改ざんの目的は、単なる愉快犯的行為から、フィッシングサイト等への誘導、マルウェアのダウンロード、さらにはフォームへ入力される情報の奪取に至るまで多岐にわたります。
- 改ざんに至る経路も、サイトへの直接侵入、CMSへの攻撃、管理者が使用するPCへの侵入によるアカウントの乗っ取り等様々です。
- 少しでもそういった経路での攻撃を食い止められるよう、CMSへのログインや、ファイルアップロードに使用するサービスへのログインを適宜制限すること、クライアント側でも可能な限りアンチウイルスやUTMの導入等による防御を固めることが重要です。


2023年02月28日 15時42分 公開

ラウンドワン公式サイト→アダルトサイトに飛んだとの報告多数　運営元「第三者からの不正アクセスによるもの」と説明して謝罪

ページ改ざんによる公式サイトからの個人情報などの流出は起きていないとしています。

[ねとらぼ]

ボウリング場やスポッチャなどを運営するラウンドワンは、第三者からの不正アクセスにより同社の店舗料金案内ページが改ざんされ、不適切なWebページに誘導されるようになっていたとして、公式サイトで謝罪しました。