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。

●WordPressプラグイン「UpdraftPlus」に脆弱性、サイト乗っ取りに繋がる恐れ…1.22.3以降へアップデートを

https://news.mynavi.jp/techplus/article/20220221-2277143/
https://www.wordfence.com/blog/2022/02/vulnerability-in-updraftplus-allowed-subscribers-to-download-sensitive-backups/

このニュースをザックリ言うと･･･

- 2月17日(現地時間)、WordPress向けセキュリティプラグイン「Wordfence」を提供するDefiant社より、WordPressのデータバックアップ用プラグイン「UpdraftPlus」に脆弱性(CVE-2022-0633)が存在するとして注意喚起が出されています。

- 脆弱性はUpdraftPlusのバージョン1.16.7～1.22.2に存在し、管理者権限を持っていないユーザーにより、保存されているバックアップデータのダウンロードが可能になり、最悪の場合サイトの乗っ取りに繋がり得るとされています。

- 既に脆弱性を修正したUpdraftPlus 1.22.3がリリースされており、アップデートが強く推奨されています(その後、2/22時点の最新バージョンは1.22.4となっています)。

AUS便りからの所感等

- WordPressのデータバックアップ機能を提供するプラグインは他に多機能なBackWPUpが知られており、UpdraftPlusもより操作が単純とされていることから、それぞれ人気があるとされています。

- 脆弱性の悪用には、攻撃者がWordPressサイトのユーザーとしてログインし、管理者に対し標的型攻撃を仕掛ける必要があるとされていますが、最も権限の低い「購読者」権限のユーザーであっても攻撃可能とされており、管理者以外のユーザーが登録されている場合には注意が必要となります。

- WordPressでは、本体からサードパーティー製のプラグインに至るまで日々何らかの脆弱性が報告されており、インストール・有効化するプラグインはできる限り必要最小限とすること、それら全てについて随時セキュリティ情報を確認しつつ、最新バージョンに保つよう留意することが重要です。

TECH Powered by マイナビニュース

WordPress人気バックアッププラグインに脆弱性、乗っ取りの危険性

2022/02/21 09:24　　著者：後藤大地

Defiantは2月17日(米国時間)、「Vulnerability in UpdraftPlus Allowed Subscribers to Download Sensitive Backups」において、人気の高いWordPressバックアッププラグインである「UpdraftPlus」に、権限を持っていないユーザーがバックアップをダウンロードできる脆弱性が存在すると伝えた。情報窃取のみならず、結果として、影響を受けるサイトの制御権が乗っ取られる危険性もあるとされている。

●「ゲームのテストプレイをしてほしい」…exeファイルを送り付けてDiscord乗っ取りを行う攻撃の報告

https://news.denfaminicogamer.jp/news/220214g
https://togetter.com/li/1845235
https://forest.watch.impress.co.jp/docs/serial/yajiuma/1388597.html

このニュースをザックリ言うと・・・

- 2月14日(日本時間)前後から、音声チャット等のサービス「Discord」においてアカウントの乗っ取りを意図した攻撃を受けたとしてTwitter等で報告が相次いでいます。

- 挙げられている攻撃の手口は、知り合いのアカウントから「5分程で終わるからゲームのテストプレイをしてほしい」という内容のDMが届き、後からゲームのインストーラーになりすました不正なexeファイルが送られてくるというものとなっています。

- 当初、exeファイルは各社ウイルススキャンでもマルウェアと検出されなかったことから、少なからぬ被害が出ていた模様です。

AUS便りからの所感

- Emotetやビジネスメール詐欺のように、元々関係のある知り合いのアカウントから日本語で話しかけられることで安心し、マルウェアに感染しやすくなるという手口がとられており、既に乗っ取ったアカウントから知り合いのユーザーへと連鎖的に乗っ取りの攻撃を行ったものとみられます。

- exeファイルを実行したPCにおいてはボットが常駐してDiscordアカウントの認証情報等を監視するとみられ、乗っ取りを受けた後にログインした別のアカウントも、同様に乗っ取られたとの報告があります。

- 知り合いのPCに侵入している攻撃者が送信するDMをそれと確実に判別することは困難になりつつありますが、不審なファイルが送られたり、URLへ案内された場合に、Twitter等ネット上で類似した手口が報告されていないか調査・確認し、あるいはWindows 10(Pro以降、64bit版のみ)に搭載されたセキュリティ機能である「Windowsサンドボックス」上でファイルを実行する等、様々な回避策・防衛策を以て慎重に行動するよう心掛けて頂ければ幸いです。

電ファミニコゲマ

Discordでフレンドから「ゲームを開発したのでプレイして欲しい」と「exeファイル」を送り、乗っ取られる事例が多数のユーザーから報告

2022年2月14日 16:32 公開

ゲーマー向けのコミュニケーションツール「Discord」（ディスコード）にて、知り合いアカウントから「exeファイル」が送られ、それを踏んでしまうと、自分のDiscordアカウントが乗っ取られる事案が多数のユーザーからTwitterを中心に報告されている。

現在、知られている手口としては、知り合い・フレンドのアカウントからDMなどを通して「こんにちは」、「ゲームを開発したのでテストプレイして欲しい」などと日本語で言われ、その後に送られた「exeファイル」を踏んでしまうと、Discordアカウント乗っ取られるようだ。

その知り合いのアカウントはすでに乗っ取られており、リンクを貼る前に簡単な会話をしてくるため、気を許してクリックしてしまい被害にあわれるケースが多いようだ。

●米CISA、無償で利用可能なセキュリティソフト・サービスを紹介

https://news.mynavi.jp/techplus/article/20220221-2277152/
https://www.cisa.gov/free-cybersecurity-services-and-tools

このニュースをザックリ言うと・・・

- 2月18日(現地時間)、米国土安全保障省(DHS)に属するセキュリティ機関CISAより、「Free Cybersecurity Services and Tools」と題し、無償で利用可能なセキュリティソフト・サービスを紹介するWebページが同機関のWebサイトに開設されています。

- Webページでは「サイバーインシデントの被害の軽減」「侵入の可能性の速やかな検知」「組織が侵入を受けた場合の対応準備の確認」「破壊的なインシデントに対する組織の耐性の最大化」の4つのカテゴリーに分けて、CISA自体のサービスや相談窓口、あるいは大手企業が提供するものから、オープンソースのプロダクトに至るまで広範囲にわたるソフト・サービスが挙げられています。

AUS便りからの所感

- 同ページでは他にも、基本的な対策として「ソフトウェアの既知のセキュリティホールの修正」「多要素認証(MFA)の実装」「アップデートされなくなったソフトウェアの交換」「既知・デフォルト・変更不可能なパスワードに依存するシステム・製品の交換」といった事柄を挙げています。

- こういった無償ソフト・サービスの活用によっては、個人・家庭はもちろん、組織における有効なセキュリティ対策の実施においても、有償プロダクトにも匹敵する効果も期待できますが、決して安易なコスト削減のために無償ソフト・サービスだけを使い続けるのではなく、今後の有償プロダクトの導入、そしてそれとの適宜組み合せによるさらなる安全性の向上を見据え、まずは必要とされる最低限のセキュリティレベルの確保のために用いる、といった使い方も一考でしょう。

TECHF Powered by マイナビニュース

無償で使えるセキュリティソフトやサービス一覧公開、米セキュリティ当局

2022/02/21 09:48　　著者：後藤大地

サイバーセキュリティの脅威について世界中のセキュリティベンダーやセキュリティ当局が警告を行い、効果的な対策などの情報を発信している。大枠の対策に関する情報は多く発信されているが、実践の段階になると、どのようなソフトウェアやサービスが存在するのかを調査するところから始めなければならない。こうした調査や評価の必要性が組織にとって負担となっている。

こうした状況を踏まえ、米国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁(CISA: Cybersecurity and Infrastructure Security Agency)はこのほど、「Free Cybersecurity Services and Tools | CISA」において、無料で利用できるセキュリティツールおよびサービスのリストを公開した。