— AUS（アルテミス・ユーザ・サポート）便り 2018/10/22号 —
https://www.artemis-jp.com

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。

●Facebookの情報流出、被害は3,000万人…半数はプロフィールの詳細情報に不正アクセス

https://www.nikkei.com/article/DGXMZO35922290290920180000000/
http://www.itmedia.co.jp/enterprise/articles/1810/15/news056.html
https://www.facebook.com/help/securitynotice?ref=sec

このニュースをザックリ言うと･･･

- 9月29日（日本時間）、Facebookより、同サイトの脆弱性を突かれ、ユーザ約5,000万人分の「アクセストークン」が奪取された可能性があると発表されました。

- 脆弱性は2017年7月から存在しており、アクセストークンの奪取により、そのユーザにパスワードなしでログインすることが可能な状態となっていたとのことで、脆弱性の修正とともに、最大9,000万人のユーザについてアクセストークンがリセットされています。

- 10月12日（同）に発表された続報によれば、実際に被害にあったユーザは約3,000万人で、その半数の約1,4000万人について、居住地・生年月日・検索内容などを含む詳細なプロフィール情報に不正アクセスされていたとのことです。

- Facebookでは各ユーザが被害を受けたかどうか確認する為のページを用意（10月19日現在日本語化済み）し、また実際に被害を受けた約3,000万人に対し連絡するとしています。

AUS便りからの所感等

- 脆弱性は「特定のユーザへのプレビュー」機能に存在しており、アクセストークンのリセット対象となったのは、この機能を利用したことがあるユーザとみられます。

- 「パスワードなしでログイン可能」というアクセストークンの仕様から、逆にアカウントのパスワードについては奪取できず、流出もなかった模様とのことで、このことから、今回についてはパスワードの変更は行わなくてもよいとする意見もあります。

- Facebookは実名での登録が基本とされるSNSであることから、センシティブな情報を登録していたユーザが多かったとみられ、そこが特に攻撃者の狙い目とされたと考えられ、個人情報の流出を懸念するのであれば、ごく親しい友人にも開示したくない情報は必要最低限しか登録しないよう、どのSNSであっても徹底するよう心掛けるべきでしょう。


日本経済新聞

米フェイスブック、最大5千万人に「乗っ取り」の恐れ

フェイスブック ネット・IT 北米

2018/9/29 6:16

保存 共有 印刷 その他

【シリコンバレー＝中西豊紀】米フェイスブックは28日、外部によるハッキングにより最大5000万人分のユーザーアカウントが「乗っ取り」に遭う恐れがあると発表した。具体的な被害が出ているかは調査中としている。同社は今春にも最大8700万人分の個人情報の流出が発覚したばかり。プライバシー保護の規制が世界で強まる中で、新たな火種を抱え込んだ。

プライバシー設定の一部機能に脆弱性があり、そこをハッカーに攻撃されたという。その結果、フェイスブックの交流サイト（SNS）内で第三者がユーザーアカウントを乗っ取るリスクが高まった。メッセージを第三者に読まれたり、SNS上に勝手になりすましの投稿をされたりする可能性がある。ユーザーのパスワードやクレジットカード情報が取られるリスクはないという。

問題は25日に同社の中で発覚し、26日に米連邦捜査局（FBI）に通報した。その上で27日にソフトウエアに対応のための手当てを施した。脆弱性が見つかった「View As」と呼ばれる他者から見た自分のページの外観を調べる機能は、当分の間使えないようにする。

万が一被害を受けるかもしれない人も含め、最大9000万人が同社のアカウントに再ログインする必要がある。被害を受ける恐れのあるユーザーの地域別の所在は分かっていない。


ITmedia エンタープライズ

Facebookの情報流出、被害は3000万人　プロフィールの詳細情報に不正アクセス

約1400万人については、居住地や生年月日、検索内容などを含む詳細なプロフィール情報に不正アクセスされていたことも判明した。

2018年10月15日 09時30分 公開

[鈴木聖子，ITmedia]

印刷 79 74 B! 0

米Facebookは10月12日、アカウントへのログインに使用するアクセストークンが何者かに盗まれた事件について、被害に遭ったユーザーの数は、当初の発表よりも少ない約3000万人だったと発表した。そのうち約半数については、居住地や生年月日、検索内容などを含む詳細なプロフィール情報が不正アクセスされていたことも判明した。

今回の事件では、Facebookのコードに2017年7月から2018年8月の間に存在していた脆弱性が悪用され、アクセストークンが盗まれた。アクセストークンは、毎回パスワードを入力し直さなくてもFacebookへのログイン状態を維持できる仕組みに使われており、これを盗めば他人のアカウントを乗っ取ることもできる。当初の発表では、約5000万人のアクセストークンが盗まれた可能性があるとしていた。

Facebookによると、攻撃者は既にコントロールを握っていた複数のアカウントを使い、友達関係でつながる計約40万人のアカウントをたどって、およそ3000万人のアクセストークンを盗み出していた。

このうち約1500万人については、氏名と連絡先情報（プロフィールに登録された電話番号や電子メール）が不正アクセスされ、約1400万人については氏名と連絡先情報に加えて、他のプロフィール情報（性別、言語、家族と交際ステータス、宗教、出身地、居住地、生年月日、Facebookへのアクセスに使うデバイスの種類、学歴、勤務先、最近訪れた場所、フォローしている相手、直近15回の検索内容など）にも不正アクセスされていたことが分かった。残る100万人については、いずれの情報にもアクセスされなかったとしている。


ヘルプセンター

Facebookの最新のセキュリティ問題に関する重要なアップデート

記事をシェア

先日お知らせしたFacebookで発生したセキュリティに関する問題について、その後の調査の結果をお知らせします。およそ3000万のFacebookアカウントの情報が、アクセストークンを使用したハッカーにより不正アクセスを受けたことが判明しました。ご迷惑をおかけして、誠に申し訳ございません。利用者の皆様のプライバシーはFacebookにとって極めて重要なことです。調査は引き続き行っておりますが、影響を受けたFaceboo アカウント、および利用者の皆様にご留意いただきたい点について、お知らせします。

Facebookによる調査の進捗、およびこれまでに判明した状況について

- 2018年9月25日、Facebookでは、システム内の3つのバグの複雑な相互作用により発生したセキュリティ脆弱性を悪用したハッカーがアクセストークンを不正に取得していたことを検知しました。デジタルな鍵のように機能するトークンは、Facebookプラットフォームから情報を引き出すために使用できます。Facebookでは、プラットフォームの情報を守るための緊急措置を講じるとともに、不正にアクセスされた情報があるか否か、および影響を受けた利用者の数の調査を開始しました。
- まず、調査を進めつつ利用者各位の情報の安全を最大限担保するため、影響を受けた可能性のあるおよそ9000万のアカウントのアクセストークンを無効とさせていただきました。利用者の皆様には、パスワードを変更するなどの手順は一切不要です。現時点でアカウントにアクセスできない場合には、対処方法をご確認ください。
- 9月28日より、アカウントのログアウト措置をとった利用者の皆様に対して、なぜ措置が必要だったのか、およびその時点で判明していた状況についての説明を開始しました。本件に関するこれまでのお知らせ、およびFacebookが当初に講じた措置についてはこちらを参照してください。安全確保のための初期的な対応を行ったものの、この時点ではFacebookでは情報に対する不正なアクセスが実際に発生したか を把握していませんでした。
- 本日までの調査の結果、9月14日から27日までの期間、特定のアカウントの情報がアクセストークンを利用したハッカーにより不正にアクセスされていた事実が確認されました。不正に利用されていたアクセストークンは既に無効化され、Facebookのアカウント情報へのさらなるアクセスのおそれはありません。不正アクセスがどのように行われたかの詳細についてはこちらを参照してください。

●仮想通貨採掘マルウェアをインストールする不正なFlash Playerインストーラー

https://crypto-times.jp/new-malware-utilises-adobe-installer-popup-to-install-xmrig/

このニュースをザックリ言うと・・・

- 10月11日（現地時間）、セキュリティベンダーの米Palo Alto Networks社より、仮想通貨採掘マルウェアが混入した不正なFlash Playerのインストーラーが確認されたと発表されました。

- 発表によれば、このインストーラーの実行により、仮想通貨「Monero」の採掘を行うマルウェア「XMRig」もインストールされ、PC上で実行されるとのことです。

- 不正なインストーラーは「AdobeFlashPlayer__(アルファベット・数字の羅列).exe」というファイル名で、「flashplayer_down.php?clickid=」という文字列を含むURLからダウンロードされるという特徴を持ち、同社では今年3月以降、このようなマルウェアを113種類検出したとのことです。

AUS便りからの所感等

- Flash Playerに偽装するマルウェアは既に珍しくはありませんが、今回は本物のFlash Playerをダウンロードしてインストールする挙動の他、ポップアップ通知も本物そっくりなものとなっており、巧妙にマルウェアへの感染を隠蔽しているようです。

- Flash Playerのインストーラーは必ずAdobe公式のサイトからダウンロードするようにし、また不正なファイルのダウンロードや実行を食い止められるよう、アンチウイルスやUTMによる防御を確実に行うようにしてください。


CryptoTimes

Adobe Flashのアップデートを巧妙に装ったマイニングマルウェアが発見される

2018-10-19

Adobe Flash Playerのアップデートを装いモネロ($XMR)のCPUマイナーを仕込むマルウェアが今年8月ごろから確認されていることが、Palo Alto Networks社のセキュリティチーム・Unit 42による発表からわかりました。

Windows OSをターゲットにした同マルウェアに感染すると、暗号通貨・モネロのCPUマイナー「XMRig」がユーザーに通知されることなくインストールされ、バックグラウンドで同通貨をマイニングし続けるといいます。

マイニングされた通貨はハッカーのものとみられるアドレスに送られるようになっており、マルウェアに感染したコンピューターには全体的なパフォーマンスの低下がみられるとされています。

- なお、ChromeにはFlash Playerが同梱、Windows 8以降のIE・Edgeで使用されるFlash PlayerはWindows Updateで更新されるため、これらを利用する場合はこのようなインストーラーではインストール・アップデートしないことにも注意してください。

●PDFリーダー「Foxit Reader」最新バージョンリリース…13件の脆弱点修正

https://forest.watch.impress.co.jp/docs/news/1147621.html

このニュースをザックリ言うと・・・

- 10月12日（日本時間）、PDFリーダー「Foxit Reader」およびPDF作成・編集ツール「Foxit PhantomPDF」の最新バージョン9.3がリリースされています。

- このバージョンでは、不正なPDFファイルを開くことにより、PCを乗っ取られたり情報が漏えいしたりする等の可能性がある13件の脆弱点が修正されています。

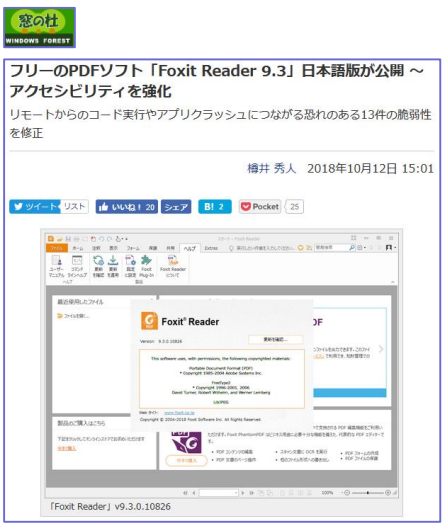
AUS便りからの所感等

- Adobe社の「Acrobat Reader」については、「動作が重い」「脆弱性が多い」等と感じることから、Foxit Readerをはじめ他のPDFリーダーを利用するユーザは以前から多く存在します。

- ただし、他のソフトウェアに乗り換えたからと言って、必ずしも脆弱性にわずらわされなくなるとは限らないことには注意が必要です。

- それぞれのソフトで独自に脆弱性が発生することはもちろん、例えばPDF形式自体の問題等が原因で、あらゆるPDFリーダーに影響する脆弱性が発表されることも考えられます。

- OSにも他のアプリケーションにも言えることですが、セキュリティを確実に保つための根本的な対策として、最新のバージョンに保つことが最も重要であり、そしてアップデートまでの間に脆弱性を突かれる可能性を少しでも抑制する意味でも、アンチウイルスやUTMによる防御も併せて行うことが肝要です。


窓の杜 WINDOWS FOREST

フリーのPDFソフト「Foxit Reader 9.3」日本語版が公開 ～アクセシビリティを強化

リモートからのコード実行やアプリクラッシュにつながる恐れのある13件の脆弱性を修正

樽井 秀人　2018年10月12日 15:01

ツイート リスト いいね！20 シェア B！2 Pocket 25