— AUS（アルテミス・ユーザ・サポート）便り 2018/01/22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。

●幻冬舎のWebサイト、不正アクセスで会員情報9万件以上流出か

http://itpro.nikkeibp.co.jp/atcl/news/17/011502952/?rt=nocnt
https://www3.nhk.or.jp/news/html/20180115/k10011289581000.html

このニュースをザックリ言うと・・・

- 1月15日（日本時間）、出版社の幻冬舎より、同社運営のWebサイト「幻冬舎plus」が不正アクセスを受け、会員情報の一部が流出した可能性があると発表されました。

- 発表によれば、対象となるのは、2013年11月12日～2017年8月18日の間に同サイトに登録した会員最大93,014件分のメールアドレス・ID・名前とされており、パスワード・生年月日・クレジットカード情報あるいはプレゼント応募時に入力した住所・電話番号などの情報は流出していない模様です。

- 2017年12月27日に当サイトの会員からの問合せを受けて調査を行った結果、同サイトのシステムに存在していた脆弱性を突かれ不正アクセスを受けたものとみられています。

AUS便りからの所感等

- 不正アクセスの原因となったとみられる脆弱性は、2017年3月30日に行ったシステムアップデートで発現、同8月18日にサイト上で不具合が発生したことでその存在が確認され、修正を行っていたとしており、不正アクセスはその間の5ヶ月間のどこかで発生していた模様です。

- 会員に関するあらゆる情報が抜き取られたわけではなく、クレジットカードの不正使用あるいは住所宛にDMが郵送される可能性こそ低いとみられていますが、メールアドレスは特定個人を識別できる内容となっていれば即ち個人情報に繋がりますし、そうでなかったとしてもそのアドレスを普段公開していない人にとっては、アドレスの流出は大きな痛手となり得ます。

- 仮に不正アクセス等を受けても流出しにくいよう、アクセス権限の設定等の堅牢なシステム構成、またUTM等による出口対策の実施が重要です。

- なお、同社では当該脆弱性の修正を行った際に不正アクセスの有無について調査しておらず、今回残っていた2017年7月以降のログから不正アクセスの形跡を確認できたとしており、不正アクセスが発生してから発覚までタイムラグが発生してしまう事態を防ぐため、十分に長い期間と詳細な場面におけるログの取得、そしてログからの不正アクセスの痕跡を迅速に参照できるシステム作りもまた肝心です。

ITpro

幻冬舎のサイトから最大9万3000人の情報が流出、会員の指摘まで気づかず

根本 浩之＝日経NETWORK　2018/01/15　日経NETWORK

目次一覧

シェア 17　B! ブックマーク 2　Pocket　ツイート　保存する

幻冬舎は2018年1月15日、同社のウェブサイトから会員情報が流出したことを明らかにした。最大9万3014人のメールアドレス、ユーザーID、名前の情報が流出した可能性がある。

狙われたのは同社のW
を突かれて2013年11月
報が流出した可能性があ
含まれていない。

同社の会員として登録したメールアドレス宛てにフィッシングメールが届いたユーザーが不審に思い、同社に問い合わせたことで流出が発覚。連絡を受け、残っていた2017年7月16日以降のログを確認したところ、不正アクセスの痕跡が確認された。

今回悪用された脆弱性は、2017年3月30日に実施したシステムのバージョンアップ時に発生した。その後、2017年8月18日に対策を実施し脆弱性はふさいだものの、この5カ月弱の期間に不正アクセスを受けて流出してしまった。ユーザーから問い合わせがあるまで、実際に不正アクセスがあったかどうかの調査は実施しておらず発覚が遅れただけでなく、ログが残っていない期間について不正アクセスがあったかどうかはわかっていない。

同社は流出の可能性がある会員について、お詫びと注意喚起のメールを送るという。

NHK NEWS WEB

幻冬舎ウェブサイトに不正アクセス ９万人余の会員情報流出か

1月15日 16時39分　IT・ネット

出版社の「幻冬舎」は、ウェブサイトに不正なアクセスがあり、最大で９万３０００人余りの名前やメールアドレスなどが外部に流出したおそれがあると発表しました。

発表によりますと、不正なアクセスがあったのは、幻冬舎が運営し電子書籍の購入などができるウェブサイト「幻冬舎ｐｌｕｓ」です。

先月２７日に利用者から不審なメールが届いたという連絡があったため調べたところ、不正なアクセスが確認され

この不正アクセスで、サイトが
員登録した最大で９万３０１４
れがあるとしています。

会社は、去年８月１８日に、サ
システムを修正したため、これ
います。一方、書籍の購入の際
場所に保存されていたため流出

幻冬舎のHPより

2018.01.15 [お詫び・訂正]

不正アクセスによる会員情報の流出に関するご報告とお詫び

このたび、弊社が運営するウェブサイト「幻冬舎plus（以下、当サイトといいます）」において、第三者による不正アクセスにより、会員情報の一部が流出した可能性があることが判明いたしました。
現在把握している事項を以下にご報告するとともに、お客様ならびに関係者の皆様に多大なるご迷惑とご心配をおかけすることとなったことを深くお詫び申し上げます。

1.経緯

2017年12月27日に当サイトの会員の方から、会員登録の際に入力したメールアドレス宛にフィッシングメールが届いたとの報告を受け、サーバーログ等の調査を開始しました。その結

●脆弱性「Spectre」「Meltdown」のパッチを偽装したマルウェアに注意

https://news.mynavi.jp/article/20180116-571898/

このニュースをザックリ言うと・・・

- 1月12日（現地時間）、アンチウイルスソフトベンダーの米Malwarebytes社より、CPUの脆弱性「Spectre」「Meltdown」に対するパッチを偽装したマルウェアが確認されたとして警告が出されています。

- 警告では、偽パッチはドイツの政府機関関係サイトをかたるサイトで配布され、実行すると「Smoke Loader」と呼ばれるマルウェアをダウンロードする仕組みになっていたとのことです。

- 既に同社の働きかけにより、サイトは閉鎖されているとのことです。

AUS便りからの所感等

- スポーツ等の大きなイベントに便乗してスパムメールやマルウェアが拡散するのと同様、今回のケースも「多くのCPUに影響する脆弱性」というニュースに便乗した攻撃の一環と言えます。

- 対策をとるべき箇所はどこか、適用すべきパッチはどれか（CPUやOS等のメーカーが公式にリリースしているパッチをダウンロードすべきなのは言うまでもありません）、そしてどんな攻撃が発生しているか、日々情報収集を行い、正しい情報をもとに慎重に行動することが重要です。


マイナビニュース

2018/01/16 09:46:54 印刷

脆弱性「Spectre」「Meltdown」のパッチを偽装したマルウェアに注意

後藤大地

関連キーワード：脆弱性

昨今のサイバー攻撃は時事ネタを巧みに悪用して行われる。脆弱性を修正するパッチなどを偽装してマルウェアが配布されることも多く、今回Malwarebytesに掲載された記事も同様の内容を指摘している。

Webサイトから更新プログラムやアプリケーションをダウンロードする際、これまではまずそのサイトがHTTPSを使っているかどうか、証明書は適切なものであるかを確認することが推奨されていた。しかし、HTTPSは通信内容の漏洩を防止する機能を提供するが、HTTPSを提供している側が悪用する意図を持っているかどうかまでは保証していない点に注意が必要。

今回取りあげられている偽パッチはドイツの政府機関に関係していると見せかけたサイトを用いて、感染を促している。

●サイバーセキュリティクイズの賞品として提供されたUSBメモリからマルウェアが見つかる

https://security.srad.jp/story/18/01/12/0621229/

このニュースをザックリ言うと・・・

- 1月10日（現地時間）、イギリスのBBC等にて、台湾のイベントで配布されたUSBメモリにマルウェアが混入している事例が確認されたと報じられています。

- USBメモリは2017年12月11日～15日に、サイバーセキュリティに関するクイズイベントの賞品として250個が配布されていましたが、少なくとも54個が「XtbSeDuA.exe」と呼ばれるマルウェアに感染していたとみられており、台湾の警察によれば、54個のうち34個が未回収とのことです。

- 「XtbSeDuA.exe」は中国の古いウイルスサイトで配布されていたとされ、32ビットマシンから個人情報を盗み出すものとされています。

AUS便りからの所感等

- USBメモリから接続したPCにマルウェアが感染するケースは枚挙にいとまがなく、そういったUSBメモリを郵便でばら撒く等の攻撃も存在します。

- また2015年には、300個のUSBメモリを放置したところ、約半数が拾われてPCに接続されたという調査結果もあります。


スラド

サイバーセキュリティクイズの商品として提供されたUSBメモリからマルウェアが見つかる

ストーリー by hylom 2018年01月13日 7時00分 裏 部門より

あるAnonymous Coward曰く、

サイバーセキュリティ関連のクイズイベントで商品として提供されていたUSBメモリにマルウェアが混入していたそうだ（BBC、The Register、Slashdot）。

このイベントは昨年の12月11～15日に開催されたもの。感染していたウイルスは中国の古いウイルスサイト「Liberty Times」で配布されていた「XtbSeDuA.exe」で、32ビットマシンから個人情報を盗み出すタイプのものだという。クイズの受賞者に提供された250個のうち少なくとも54台がウイルスに感染していたものとみられている。まだ回収されていないものが34台ほどある模様。

45 コメント セキュリティ security

- USBメモリやDVD-ROM等から何らかのプログラムを自動実行させないよう可能な限り設定を行うこと、アンチウイルスによるUSBメモリのスキャンおよびPCへの感染防御を確実に行うこと、またそもそもの感染回避策として出所が不明なUSBデバイスは接続しないよう努めること等が肝要です。