— AUS（アルテミス・ユーザ・サポート）便り 2018/05/07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。

●楽天をかたるウイルスメール、1日でこれまでにない量の拡散

https://mobile.twitter.com/MPD_cybersec/status/989431869786673152
https://www.jc3.or.jp/topics/virusmail.html

このニュースをザックリ言うと･･･

- 4月26日（日本時間）、警視庁と日本サイバー犯罪対策センター（JC3）より、楽天市場をかたりマルウェアに感染させようとするメールが拡散しているとして、注意喚起が出されています。

- JC3によれば27日にも同様の拡散があった模様です。

- メールは、
◆件名は、「【楽天市場】注文内容ご確認（自動配信メール）」
◆本文は、楽天の各モールからの注文内容確認を装ったHTMLファイル
で、リンクのクリックによりマルウェアをダウンロードするとみられています。
（警視庁発表ではフィッシングサイトとされており、情報が錯綜している面もあるようです。）

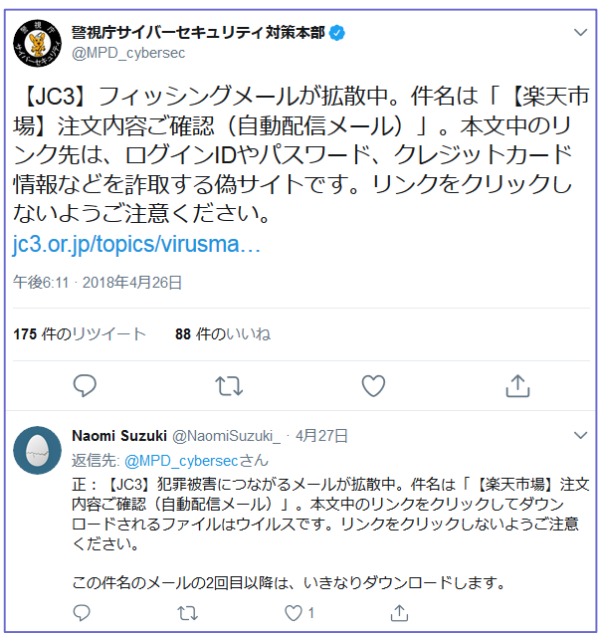
AUS便りからの所感等

- 楽天をかたるフィッシングメール・ウイルスメールはもはや珍しくありませんが、特に4月26日に確認されたものは「尋常ではない量」が送られていた模様です。

- 例えば、筆者のメールアカウントには26日だけで175通、うち168通が19:09～19:35の30分弱の間に届いています。

- このような異常な送られ方をしているメールについて、逆に興味本位でリンクをクリックしてしまうケース、あるいは自分が利用している店舗の名前がたまたま書かれていたことでそこからアクセスしようとするケースも無きにしもあらずですが、決してそのようなことはせず、削除等の対応をとりましょう。

- メーラーやメールサーバあるいはアンチウイルス・UTM等のセキュリティ機能をそれぞれ有効にすることでフィッシングメール等に引っかかる可能性を少しでも減らし、かつ注文情報等へのアクセスについても、あらかじめ登録したブックマークから辿ってアクセスするよう心がけましょう。



●プレミアム・アウトレットの会員情報最大43万件流出

https://www.nikkei.com/article/DGXMZO29150480Z00C18A4000000/

このニュースをザックリ言うと・・・

- 4月7日（日本時間）、三菱地所・サイモン社より、同社が運営するアウトレットモール「プレミアム・アウトレット」の会員情報（メールアドレス・パスワード）が流出した可能性があると発表されました。

- 海外のオンラインストレージサービスにおいて会員情報と思われるデータ42万9750件が公開されているとの通報を受けて発覚したもので、調査の結果、約24万件についてメールアドレスとパスワードが一致、約3万件についてメールアドレスのみが一致したとのことです。

- 2018年2月に様々なウェブサイトから漏洩したと思われるメールアドレス・パスワードの「組」の一覧が一斉に公開されており、今回のファイルはその中の一つとされています。

AUS便りからの所感等

- 数多の攻撃者は今回のようなメールアドレス・パスワードの流出データを入手し、あらゆるWebサービスに対し同じ情報でログインできるか即座に試してきますので、その際に他のサービスでも同じパスワードを使用していれば容易に不正ログインが成功し、さらなる不正行為に繋がり得ます。

- このような芋づる式に不正ログインを行おうとする行為が数年前に話題となったことにより、アカウントの保護のために「パスワードはサービス毎に異なるものを使う」ことが重要視されています。

- 今回のようなアカウント情報の流出が自分が利用しているサービスで発覚したときには速やかにパスワードを変更する、また、登録したきり頻繁に利用していないサービスについてこのような事態が発生したときに対応が後手後手に回ることのないようにそういったサービスへの登録状況についても常に把握しておく、などが重要です。


日本経済新聞

プレミアム・アウトレット、会員情報43万件を流出か

科学&新技術 BP速報

2018/4/9 20:00

日経XTECH

三菱地所・サイモンは2018年4月7日、同社が運営するショッピングモール「プレミアム・アウトレット」の会員情報が流出した可能性があると同社のウェブサイトで発表した。会員には、メールでも個別に同じ内容を知らせている。

流出した可能性があるのはメールアドレスとパスワード。同社は、会員が同じパスワードを使って他サイトを利用している場合は、速やかに変更するよう呼びかけている。

事実関係は調査中であり、確認が完了するまで、会員情報を管理するサーバーはネットワークから切り離し、会員サービスを停止するとしている。

きっかけは、会員情報と思われる約43万件のデータが海外のストレージサービスに公開されているとの、都内在住のセキュリティリサーチャーからの情報提供。

ストレージサービスには、「www.premiumoutlets.co.jp.txt」という名前で公開されたファイルに、42万9750件のメールアドレスとパスワードが含まれる。パスワードは暗号化されておらず、そのまま読めるようになっている。リストには、同じメールアドレスが複数登録されたものも見つかっている。

●「I'm Hacked bye2」…ネットワークカメラが不正アクセス

http://www.chiba-tv.com/info/detail/15503

このニュースをザックリ言うと・・・

- 4月25日（日本時間）、千葉県八千代市より、同市上下水道局が設置していた水位監視カメラが不正アクセスを受けたと発表されました。

- 被害を受けたのは3台設置されていたうちの2台で、カメラ画像の左上に、通常は表示されない撮影日時と「I'm Hacked bye2」と表示される改変が行われていたことが同24日17時過ぎに確認されたとのことです。

- また同26日には、埼玉県上尾市の河川監視カメラ1台も同様の不正アクセスを受けていたことが明らかになっています。

AUS便りからの所感等

- 近年IoTがブームになるとともに、PCやサーバあるいはモバイル機器ではないIoTデバイスについてもそのセキュリティについての注意が叫ばれており、2016年にはマルウェア「Mirai」が多数のWebカメラに感染する出来事がありました。

- 攻撃者は、インターネット上から接続可能な状態になっている複合機やIoT機器等を検索できるサーチエンジン「SHODAN」「Censys」等からネットワークカメラをターゲットに選んだものと推測され、画像を公開しているWebカメラにおいては、そのための機能にのみ外部からアクセスでき、かつ管理者画面等にはアクセスできないよう、UTMやファイアウォールによる適切なフィルタリングを行いましょう。


チバテレ

2018.04.25 ニュース

水位監視カメラに"不正アクセス"

不正アクセスを受けたのは、八千代台北と大和田を流れる公共下水道の水路沿いに設置されている水位監視カメラ2台です。

八千代市によりますと24日午後5時過ぎ、市の職員がインターネット上に公開されている水位監視カメラカメラ画像を職員が確認したところ、

本来表示されない現在時刻に加え、「I'm Hacked bye2」という文字が見つかりました。カメラが設置した業者が確認したところ、カメラにアクセスするためのパスワードが変更され、不正アクセスされたことがわかったということです。八千代市はカメラに接続しているLANケーブルを抜き、外部からアクセスできないよう対処するとともに、設置業者らとカメラの復旧に向けた調整を進めています。

- また、telnet等意図しないサービスポートへ外部からアクセスされないか、ネットワーク診断を受けて確認することも検討に値するでしょう。