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。

●セキュリティソフト導入を促す銀行からの偽メール…警視庁等注意喚起

https://japan.zdnet.com/article/35111051/
http://www.itmedia.co.jp/news/articles/1711/28/news119.html

このニュースをザックリ言うと・・・

- 11月28日（日本時間）、セキュリティソフト導入を促す偽のメールによる攻撃が拡散中として、警視庁サイバー犯罪対策課のTwitterアカウントおよび日本サイバー犯罪対策センター（JC3）より警告が出されています。

- メールは、
◆件名が『【重要】不正送金・フィッシング対策ソフト「ＰｈｉｓｈＷａｌｌプレミアム」提供開始について』となっており、
◆本文が「尊敬するお客様へ いつ楽天銀行をご利用いただき誠にありがとうございます」で始まる
このメール中のリンクにアクセスすると、不審なサイトからマルウェア等がダウンロードされる可能性があるとされています。

AUS便りからの所感等

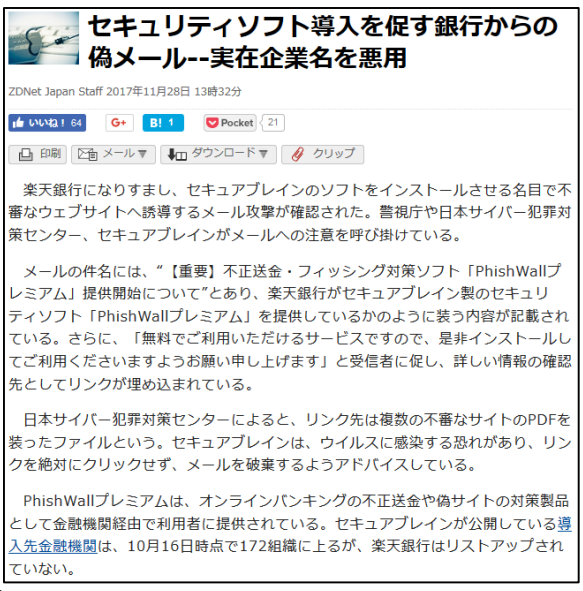
- 「PhishWallプレミアム」はゆうちょ銀行をはじめ多くの金融機関と提携している不正送金・フィッシング対策ソフトですが、現時点では楽天銀行からは提供されていません。

- しかし、実際に提供している金融機関をかたるメールも今後必ずあることでしょう。

- 偽フォームによるアカウント情報の奪取からマルウェアへの感染まで、また誘導の仕方についても、攻撃者の手口は多種多様なものであり、これまで多くとられた手口・シナリオにばかり気を取られ、今までになかった手法での誘導に騙されないよう十分注意してください。

- 警視庁・JC3のような情報源を随時チェックすること、使用している金融機関のサイトにはメールからではなくブラウザのブックマークからアクセスするよう努めること、そしてこういった不審なメールの遮断や警告のため、アンチウイルスやUTMによるメールチェックを有効にすることが重要です。

ZDNet Japan



セキュリティソフト導入を促す銀行からの偽メール--実在企業名を悪用

ZDNet Japan Staff 2017年11月28日 13時32分

いいね！ 64　G+　B! 1　Pocket 21

印刷　メール▼　ダウンロード▼　クリップ

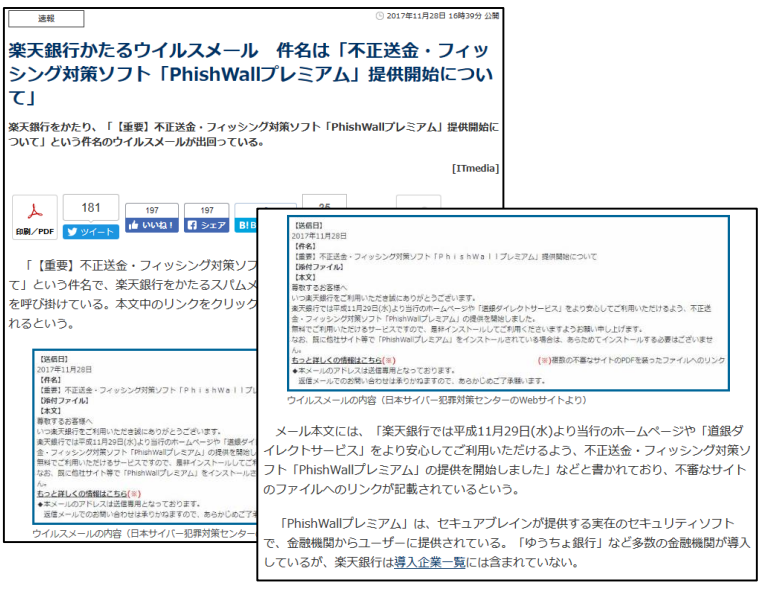
楽天銀行になりすまし、セキュアブレインのソフトをインストールさせる名目で不審なウェブサイトへ誘導するメール攻撃が確認された。警視庁や日本サイバー犯罪対策センター、セキュアブレインがメールへの注意を呼び掛けている。

メールの件名には、“【重要】不正送金・フィッシング対策ソフト「PhishWallプレミアム」提供開始について”とあり、楽天銀行がセキュアブレイン製のセキュリティソフト「PhishWallプレミアム」を提供しているかのように装う内容が記載されている。さらに、「無料でご利用いただけるサービスですので、是非インストールしてご利用くださいますようお願い申し上げます」と受信者に促し、詳しい情報の確認先としてリンクが埋め込まれている。

日本サイバー犯罪対策センターによると、リンク先は複数の不審なサイトのPDFを装ったファイルという。セキュアブレインは、ウイルスに感染する恐れがあり、リンクを絶対にクリックせず、メールを破棄するようアドバイスしている。

PhishWallプレミアムは、オンラインバンキングの不正送金や偽サイトの対策製品として金融機関経由で利用者に提供されている。セキュアブレインが公開している導入先金融機関は、10月16日時点で172組織に上るが、楽天銀行はリストアップされていない。

ITmedia NEWS



速報　2017年11月28日 16時39分 公開

楽天銀行かたるウイルスメール　件名は「不正送金・フィッシング対策ソフト「PhishWallプレミアム」提供開始について」

楽天銀行をかたり、「【重要】不正送金・フィッシング対策ソフト「PhishWallプレミアム」提供開始について」という件名のウイルスメールが出回っている。

[ITmedia]

印刷／PDF　181 ツイート　197 いいね！　197 シェア

「【重要】不正送金・フィッシング対策ソフト「PhishWallプレミアム」提供開始について」という件名で、楽天銀行をかたるスパムメールを呼び掛けている。本文中のリンクをクリックれるという。

【送信日】
2017年11月28日
【件名】
【重要】不正送金・フィッシング対策ソフト「ＰｈｉｓｈＷａｌｌプレミアム」提供開始について
【添付ファイル】
【本文】
尊敬するお客様へ
いつ楽天銀行をご利用いただき誠にありがとうございます。
楽天銀行では平成11月29日(水)より当行のホームページや「道銀ダイレクトサービス」をより安心してご利用いただけるよう、不正送金・フィッシング対策ソフト「PhishWallプレミアム」の提供を開始しました。
無料でご利用いただけるサービスですので、是非インストールしてご利用くださいますようお願い申し上げます。
なお、貴ご指定サイト等で「PhishWallプレミアム」をインストールされている場合は、あらためてインストールする必要はございません。
もっと詳しくの情報はこちら(※)　(※)道銀の不審なサイトのPDFを装ったファイルへのリンク
◆本メールのアドレスは送信専用となっております。
返信メールでのお問い合わせは多りかねますので、あらかじめご了承願います。

ウイルスメールの内容（日本サイバー犯罪対策センターのWebサイトより）

メール本文には、「楽天銀行では平成11月29日(水)より当行のホームページや「道銀ダイレクトサービス」をより安心してご利用いただけるよう、不正送金・フィッシング対策ソフト「PhishWallプレミアム」の提供を開始しました」などと書かれており、不審なサイトのファイルへのリンクが記載されているという。

「PhishWallプレミアム」は、セキュアブレインが提供する実在のセキュリティソフトで、金融機関からユーザーに提供されている。「ゆうちょ銀行」など多数の金融機関が導入しているが、楽天銀行は導入企業一覧には含まれていない。

●MSがサポート終了の「Office 2007」にパッチを提供

http://itpro.nikkeibp.co.jp/atcl/news/17/120102782/

このニュースをザックリ言うと・・・

- 11月29日（日本時間）、IPAおよびJPCERT/CCより、Microsoft Officeの脆弱性（CVE-2017-11882）について注意喚起が出されています。

- 脆弱性はOfficeの数式エディタに存在し、不正な文書ファイル等を開くことにより、PCを乗っ取られる可能性があるとされています。

- Microsoftでは11月15日および29日に修正パッチをリリースしていますが、10月10日にサポートが終了したOffice 2007についても特別にパッチがリリースされており、一方で、IPAではパッチ適用以外の回避策として、数式エディタを無効化することを挙げています。

AUS便りからの所感等

- 11月下旬にこの脆弱性を悪用してマルウェア感染を狙うメール攻撃が確認されましたが、このことがIPA等が注意喚起を出した一因とみられます。

- サポート切れプロダクトへのパッチのリリースは、今年WannaCry/WannaCrypt対策のためにWindows XPに対しパッチがリリースされた例がありますが、その時と同様にあくまで特例に過ぎないものと認識し、今後もパッチが出ることに期待するのではなく、必ずより新しいバージョンへのアップグレードを行うようにしましょう。

- この他、外部からOffice文書ファイルをダウンロードする際には、必ずアンチウイルスやUTMによるスキャンが行われるようにすることも重要です。


ITpro
MSがサポート終了の「Office 2007」にパッチを提供
島田 優子＝日経SYSTEMS　2017/12/01　SYSTEMS
目次一覧
シェア 0　B!ブックマーク 9　Pocket　ツイート　保存する
日本マイクロソフトは2017年11月に2回、10月10日にサポートが終了した「Office 2007」向け
ターの脆弱
の脆弱性を
日本マイクロソフトが修正プログラムを提供したのは11月の月例セキュリティ更新となる11月15日と、その後の11月29日。CVE-2017-11882の影響を受けるのはOffice 2007に加え、Office 2010、Office 2013、Office 2016となる。Office 2007以外のバージョンに対しても修正プログラムが公開されている。
JPCERTコーディネーションセンター（JPCERT/CC）は「脆弱性が既に悪用されていることや、本脆弱性を実証するコードが既に公開されており、動作することを確認している。早期の適用を強く推奨する」としている。情報処理推進機構（IPA）は、CVE-2017-11882の脆弱性の解消策として、修正プログラムを適用するほか、数式エディターの無効化を提示している。

●米Uber、5700万人分の個人情報が2016年10月に流出

https://japan.cnet.com/article/35110808/

このニュースをザックリ言うと・・・

- 11月21日（米国時間）、自動車配車サービスを提供する米Uber社より、2016年10月に同社が不正アクセスを受け、5700万人分の個人情報が流出していたことが発表されました。

- 発表によれば、流出した個人情報は同社サービスユーザとドライバー（60万人）の氏名・メールアドレス・運転免許証番号等で、社会保障番号やクレジットカード情報は含まれていなかったとのことです。

- 流出が発生した当時、同社は不正アクセスを行った攻撃者に対し10万ドルを支払って、情報を削除させたとしています。

AUS便りからの所感等

- 大手ネットサービスからの大規模な個人情報流出という点以上に、今回の件では発生から1年以上公表や連邦取引委員会（FTC）への報告を行っていなかった疑いで批判を受けています。

- Uberのエンジニアがコード共有サイト「github」にアップロードしていたソースコードに、Uberのシステムが利用するAWSのアカウント情報が含まれていたことが不正アクセスを受けた原因とされています。

- しかしこういったことで、AWS等のクラウドサービスの利用は自前のネットワークでサービスを構築する（オンプレミス）より安全ではないとするのは正しくなく、それぞれにおいて求められるセキュリティ対策を確実に意識し、実行することこそが重要です。


CNET Japan
Uber、5700万人分の個人情報が2016年10月に流出
Laura Hautala Dara Kerr （CNET News） 翻訳校正： 編集部 2017年11月22日 10時39分
シェア 38　ツイート　B! 18　Pocket　46　G+　印刷　メール　保存　クリップ
米国時間11月21日、Uber Technologiesは、ドライバーとユーザーを含む5700万人分のデータがハッカーに盗まれる事件が約1年前の2016年10月に発生していたことを明かした。このデータには、氏名や電子メールアドレス、運転免許証番号などの個人情報が含まれていたが、社会保障番号やクレジットカード情報は含まれていなかった。
同社の最高経営責任者（CEO）のDara Khosrowshahi氏は声明の中で、同氏自身がこのデータ流出について知ったのは最近のことだが、Uberがそれを最初に知ったのは2016年11月だった、と述べた。Bloombergの報道によれば、Uberは当時、データを盗んだハッカーらに10万ドルを支払って、情報を削除させたという。
そのデータはクラウドサービスに保存されていたが、「社外の2人の人間」がその情報にアクセスしダウンロードした、とKhosrowshahi氏は述べた。そのデータはその後削除されたとUberは考えており、このデータ流出に起因する詐欺行為が行われた兆候はない、と同氏は言い添えた。
Uberにはこのデータ流出について情報を開示する法的義務があった、と同社は現在考えている。