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。

●ビジネスメール詐欺の添付ファイル、HTMLファイルの利用が活発化

https://www.is702.jp/news/2198/
http://blog.trendmicro.co.jp/archives/15763

このニュースをザックリ言うと・・・

- 8月28日（日本時間）、大手セキュリティベンダーのトレンドマイクロ社より、Business Email Compromise（ビジネスメール詐欺、BEC）におけるアカウント情報の奪取方法の変化に対する警告が出されています。

- 記事によれば、従来は実行ファイル形式のキーロガー（キーボードからの入力を監視して記録するプログラムやソフト）をメールに添付する形がよくとられていたものの、ユーザが警戒して添付ファイルをクリックしなくなっていることから、ユーザのメールアドレスとパスワードを外部に送信するような偽のフォームを含むHTMLファイルが添付されるケースが多く確認されるようになっているとのことです。

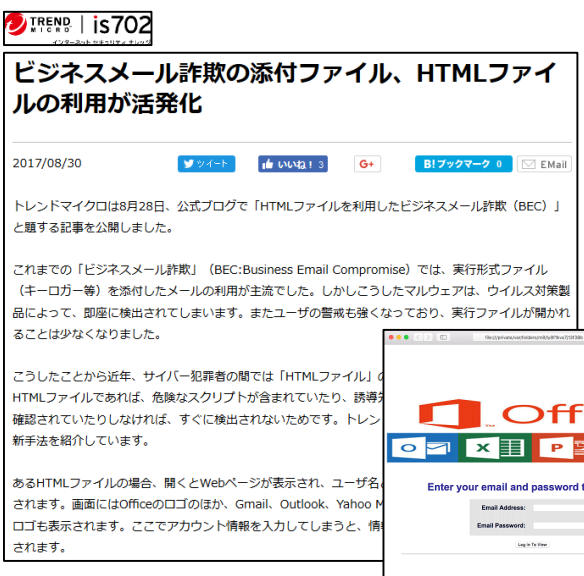
- 同社製品による統計では、2016年7月から2017年6月までの間にこのような添付ファイルが14,867件記録されている等としており、添付ファイルを不用意に開かないよう、引き続き注意が呼び掛けられています。

AUS便りからの所感等

- 前述した統計によれば、国別の攻撃件数はアメリカが8430件、次いでインド918件等となっており、日本に対する攻撃は183件確認されています。

- ただ、現状における日本への攻撃は、たびたび当AUS便りでも取り上げているようなマルウェア添付メール（AUS便り 2017/07/24号他、および https://www.jc3.or.jp/ 参照）、あるいはインターネット上のフィッシングサイトによるものが依然有力とみられます。

- トレンドマイクロ社が挙げるような動向変化の兆候があることは是非とも頭に置いておき、単に慎重な行動をとるのみならず、アンチウイルス・UTMによる防御を確実に固めておくことが肝要です。


TREND MICRO | is702

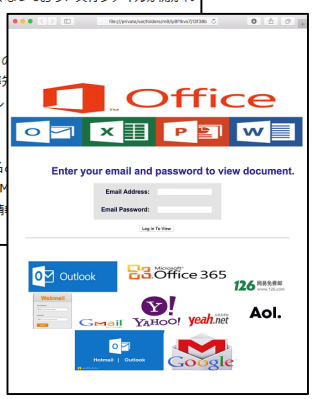
ビジネスメール詐欺の添付ファイル、HTMLファイルの利用が活発化

2017/08/30

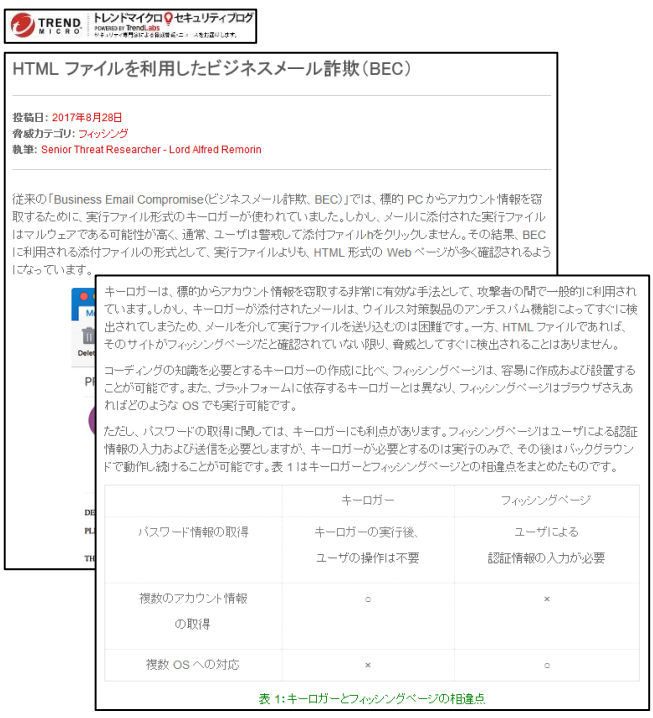
トレンドマイクロは8月28日、公式ブログで「HTMLファイルを利用したビジネスメール詐欺（BEC）」と題する記事を公開しました。

これまでの「ビジネスメール詐欺」（BEC:Business Email Compromise）では、実行形式ファイル（キーロガー等）を添付したメールの利用が主流でした。しかしこうしたマルウェアは、ウイルス対策製品によって、即座に検出されてしまいます。またユーザの警戒も強くなっており、実行ファイルが開かれることは少なくなりました。

こうしたことから近年、サイバー犯罪者の間では「HTMLファイル」



HTML形式のフィッシングページの例→


TREND MICRO トレンドマイクロ セキュリティブログ

HTML ファイルを利用したビジネスメール詐欺（BEC）

投稿日: 2017年8月28日
脅威カテゴリ: フィッシング
執筆: Senior Threat Researcher - Lord Alfred Remorin

従来の「Business Email Compromise(ビジネスメール詐欺、BEC)」では、標的 PC からアカウント情報を窃取するために、実行ファイル形式のキーロガーが使われていました。しかし、メールに添付された実行ファイルはマルウェアである可能性が高く、通常、ユーザは警戒して添付ファイルをクリックしません。その結果、BEC に利用される添付ファイルの形式として、実行ファイルよりも、HTML 形式の Web ページが多く確認されるようになっています。

キーロガーは、標的からアカウント情報を窃取する非常に有効な手法として、攻撃者の間で一般的に利用されています。しかし、キーロガーが添付されたメールは、ウイルス対策製品のアンチスパム機能によってすぐに検出されてしまうため、メールを介して実行ファイルを送り込むのは困難です。一方、HTML ファイルであれば、そのサイトがフィッシングページだと確認されていない限り、脅威としてすぐに検出されることはありません。

コーディングの知識を必要とするキーロガーの作成に比べ、フィッシングページは、容易に作成および設置することが可能です。また、プラットフォームに依存するキーロガーとは異なり、フィッシングページはブラウザさえあればどのような OS でも実行可能です。

ただし、パスワードの取得に関しては、キーロガーにも利点があります。フィッシングページはユーザによる認証情報の入力および送信を必要としますが、キーロガーが必要とするのは実行のみで、その後はバックグラウンドで動作し続けることが可能です。表 1 はキーロガーとフィッシングページとの相違点をまとめたものです。

	キーロガー	フィッシングページ
パスワード情報の取得	キーロガーの実行後、ユーザの操作は不要	ユーザによる認証情報の入力が必要
複数のアカウント情報の取得	○	×
複数 OS への対応	×	○

表 1：キーロガーとフィッシングページの相違点

●約300本のAndroidアプリからDDoS攻撃…Google、公式ストアから削除

http://news.mynavi.jp/news/2017/08/31/059/

このニュースをザックリ言うと・・・

- 8月29日（現地時間）、DDoS対策機能等に対応したCDN（Contents Delivery Network）を提供する米CloudFlare社より、約300本のAndroidアプリがDDoS攻撃を行う大規模なボットネットを構築していたと発表されました。

- 同社の他、AkamaiやGoogleといった大手ベンダーの研究者が連携して調査を行った結果、問題となったアプリにはマルウェア「WireX」が含まれており、これをインストールした100ヶ国以上のAndroid端末が踏み台となってDDoS攻撃が行われたとのことです。

- アプリはGoogle公式アプリストア「Google Play」において、メディアプレイヤーや着信音、ストレージ管理といったカテゴリーで確認されており、画面ロックあるいはスリープ中の状態でもバックグラウンドで動作するようになっていたとされており、報告を受けてGoogleではこれらのアプリをブロックし、インストールされた端末からアプリを削除する措置を講じているとのことです。

AUS便りからの所感等

- Googleでは7月にAndroid端末を有害なアプリから保護する「Google Play プロテクト」をリリースしていますが、今回削除されたもの以外にも、将来的な攻撃に備えてまだ活動を行っていないマルウェアを含むアプリがまだGoogle Playに登録されていることが考えられ、今後もそういった不正なアプリとの戦いは続きそうです。

- モバイル端末からのDDoS攻撃による大容量のパケット送信は、無料通信や高速通信分の使用量を早々に使い尽される恐れもあり、ユーザの経済的な損害にもつながり得ます。

マイナビニュース

Google、DDoS攻撃を仕掛けていた300の不正アプリをGoogle Playから削除

後藤大地
[2017/08/31]

Cloudflareは8月29日(米国時間)、「The WireX Botnet: How Industry Collaboration Disrupted a DDoS Attack | Cloudflare」において、大規模なボットネットを構築して分散型サービス妨害（DDoS)攻撃を仕掛けていた数百のAndroidアプリがGoogle Play Storeから削除されたと伝えた。

Akamai、Cloudflare、Flashpoint、Google、Oracle Dyn、RiskIQ、Team Cymruなど複数のベンダーの研究者が、この攻撃に対応するために協力して作業を実施した。各社の発表によると、Google Play Storeで配信されたアプリにマルウェア「WireX」が仕込まれ、それをダウンロードした100カ国以上のAndroid端末が踏み台となって、DDoS攻撃が発生したという。

- 可能な限りこういったアプリをインストールしてしまう可能性を減らすためにも、インストールするアプリの数は最小限とし、事前にアプリストアでのレビューやTwitter等の評判を参考とすること、Play Protectの他にもアンチウイルスアプリを導入し、また可能な限りUTMへのVPN接続を経由してインターネットにアクセスする等、モバイル端末においても各種セキュリティ対策を行うことを推奨致します。

●米国180万人の有権者情報がクラウド上に…設定ミスが原因

http://www.itmedia.co.jp/enterprise/articles/1708/21/news054.html

このニュースをザックリ言うと・・・

- 8月17日（現地時間）、米国セキュリティ企業のUpGuard社より、米シカゴの有権者約180万人の個人情報がクラウドサービス「Amazon Web Service(AWS)」上でアクセス可能な状態にあったと同社ブログで発表されました。

- 記事によれば、同社の研究者がAWSのサーバ上に保存されていた有権者情報のバックアップデータを発見し、シカゴ選挙管理委員会に8月12日に通報したもので、有権者の氏名・住所・生年月日・社会保障番号(下4桁)・免許証等の情報が含まれていたとのことです。

- データは委託業者が保存していたものとされ、通報を受けて対策を行い、現在はサーバを閉鎖していますが、AWSのデフォルトの設定では許可されたユーザのみがデータにアクセス可能であったところ、設定ミスにより不特定多数がアクセス可能な状態になっていた模様です。

AUS便りからの所感等

- 先週は大手旅行業者HIS社で約12,000人分の個人情報流出事故が発生していますが、これもサイト移行作業のために抽出したデータが外部からアクセス可能な場所に保存されたままになっていたことによるもので、オペレーションミスによる発生という意味では似たものとなっています。

- 既にクラウドの利用は一般的なものとなり、企業ネットワーク外のサーバ等に機密情報を保持することも珍しくなくなっている一方で、「企業ネットワーク内でサーバを運営するオンプレミスの方が安全」とする主張も依然根強いものがありますが、さしたる根拠も適切な対策もなくオンプレミスでの運用を行っているのであれば、一たび侵入したマルウェアや攻撃者等に対し脆弱なものとなるでしょう。

ITmedia エンタープライズ

180万人の有権者情報が露呈、AWSの設定ミスに警鐘

2017年08月21日 08時30分 公開

有権者情報のバックアップファイルが保存されていたAWSのAmazon S3バケットは、一般にアクセスできる設定になっていた。

[鈴木聖子，ITmedia]

印刷／PDF　209 ツイート　114 いいね！　114 シェア　31 B! Bookmark　48 Pocket　G+　通知

米シカゴの有権者180万人あまりの個人情報が保存されていたAmazon Web Services（AWS）のサーバ設定に不備があり、有権者情報が一般にアクセスできる状態で露呈されていたことが発覚した。

- サーバの適切な設定とその確認、出口対策を含めた安全なネットワーク構成、特にオンプレミスであればUTMの設置による適宜サーバの分離等、いずれにおいてもとるべき対策は存在し、それを行うことにより安全性を高めることが可能です。