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。

●なりすましメールによる国内での「Emotet」感染急増…JPCERT/CCが注意喚起

https://www.jpcert.or.jp/at/2019/at190044.html
https://blogs.jpcert.or.jp/ja/2019/12/emotetfaq.html

このニュースをザックリ言うと・・・

－ 11月27日(日本時間)、セキュリティ専門機関JPCERT/CCより、今年10月後半以降マルウェア「Emotet」への日本国内での感染事例が急増しているとして、注意喚起が出されています。

－ 次いで12月2日には同じくJPCERT/CCより、感染の有無を確認する方法および感染を確認した場合の対処等をまとめたFAQも発表されています。

－ 感染した場合の影響の例として「端末やブラウザに保存されたパスワード等の認証情報が窃取される」「窃取されたパスワードを悪用され SMB によりネットワーク内に感染が広がる」「メールアカウントとパスワードが窃取される」「メール本文とアドレス帳の情報が窃取される」「窃取されたメールアカウントや本文などが悪用され、Emotet の感染を広げるメールが送信される」を挙げています。

－ また、感染の被害を最小化するための対策として「当人にヒアリングを行う」「アンチウイルスで最新のパターンファイルを用いてPCをスキャンする」「PCで不審なプログラムが自動起動する設定になっていないか確認する」「メールサーバーや社内LANのトラフィックログを確認する」等を挙げており、特にWordファイルの不正なマクロによる感染を防ぐため、Wordの「セキュリティセンター」のマクロの設定をデフォルトの「警告を表示してすべてのマクロを無効にする」に設定することを推奨しています。

AUS便りからの所感等

－ Emotetについては10月下旬に米US-CERT等から活発化が確認されたとして注意喚起が出ており(AUS便り 2019/11/5号参照)、国内でも、実在の組織や人物になりすましているメールに添付されたWordファイルから感染するケースが目立っている模様です。

－ 実際にやり取りされたメールを奪取し、文面を似せた偽メールを送信する手口は、例えば「ビジネスメール詐欺(BEC)」でもよく使われており、IPAがBECについて注意喚起(https://www.ipa.go.jp/security/announce/201808-bec.html)した際に対策として挙げられた「取引先とメール以外の方法で確認する等、取引等に関する社内規程の整備」「普段と異なるメールに注意する」「不審と感じた場合の組織内外での情報共有」といった項目もまた、Emotetに限らない各種マルウェアや詐欺による被害の発生を抑え込む一助になることでしょう。

JPCERT CC
Japan Computer Emergency Response Team Coordination Center
JPCERT コーディネーションセンター


佐條 研(Ken Sajo) 2019/12/02

マルウエアEmotetへの対応FAQ

メール

2019年10月以降、日本国内にてEmotetの感染事例が急増しています。JPCERT/CCでは、次の通り注意喚起を発行しています。

JPCERT/CC: マルウエア Emotet の感染に関する注意喚起
https://www.jpcert.or.jp/at/2019/at190044.html

JPCERT/CC: CyberNewsFlash マルウエア Emotet の感染活動について
https://www.jpcert.or.jp/newsflash/2019112701.html

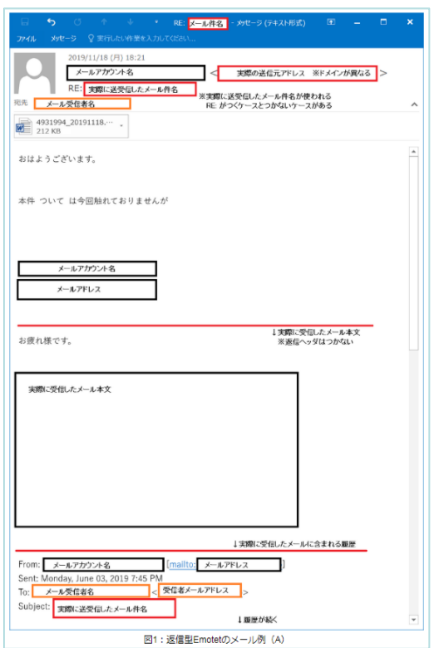

図1：返信型Emotetのメール例（A）

●ショッピングサイトで決済時だけ偽画面が…クレジット情報を盗む手口に警告

https://www3.nhk.or.jp/news/html/20191202/k10012198271000.html

このニュースをザックリ言うと・・・

- 12月2日(日本時間)、ショッピングサイトの改ざんにより、商品購入時の決済のときだけ表示される偽の画面で、クレジットカード情報を奪取する手口についてNHKで報じられています。

- 偽の画面にカード情報等が入力されると一旦エラーが表示され、本物の決済画面にリダイレクトされる手法をとるため、偽の画面だったことが気付かれにくいとされています。

- 報道内で取り上げられている日本サイバー犯罪対策センター(JC3)の注意喚起によれば、去年半ばから今年10月末までで、少なくとも約100社のサイトが改ざんされ、盗まれたカード情報は10万件に上るとされています。

AUS便りからの所感

- 前述の手口は2018年9月に「SOKAオンラインストア」で発生したケースを取り上げています(AUS便り 2018/10/15号参照)が、この時が初めて確認されたケースとされ、非常に新しい手口となります。

- 改ざんはサービスの脆弱性を突かれて、あるいは管理者のPC等を踏み台にして等で行われる可能性がありますが、たとえシステム側でカード情報を保存しない仕組みをとっていたとしても、このような改ざんをされれば結果として第三者にカード情報が送信されてしまうことになり、ユーザーにとっては「自身がフィッシングに引っかかって誘導されるケースでなくとも、本物のサイトでの決済の過程で発生してしまう」こととなります。

- サービス提供側においては、サーバー上のWebアプリケーションはじめ各種ソフトウェアを安全な状態に保ち、また改ざんのための侵入行為等を検知・遮断するソリューションを導入することを強く推奨致します。

NHK NEWS WEB

ショッピングサイト決済時だけ偽画面 クレジット情報を盗む

2019年12月2日 5時38分

インターネットのショッピングサイトが改ざんされ、商品を購入しようとすると決済のときだけ偽の画面が表示され、クレジットカードの情報を盗まれる被害が相次いでいて、サイバーセキュリティー団体が注意を呼びかけています。

●新しい検出回避機能を備えたAndroid向けアドウェアがGoogle Playから拡散

https://blog.trendmicro.co.jp/archives/22910

このニュースをザックリ言うと・・・

- 11月27日(日本時間)、トレンドマイクロ社より、Google公式のアプリストア「Google Play」においてゲームアプリやカメラアプリを偽装した49個の不正アプリを確認したと発表されました。

- モバイルデバイス内に隠れて広告を表示させる典型的なアドウェアとされる一方、アンインストールおよび検出を回避する機能も備えていた模様で、少なくとも2018年以降このようなアプリが蔓延しているとのことです。

- 既にGoogle Playからは削除されたものの、合計で300万以上のダウンロードが行われた可能性があるとしています。

AUS便りからの所感等

- 同社ではGoogle Playを監視して度々このようなアプリの存在を確認・報告し、GoogleもAndroid端末を有害なアプリから保護する「Google Play プロテクト」を提供していますが、毎回これを回避して不正なアプリがアップロードされる様子がみられ、いたちごっこが収まる気配はないようです。

- ユーザー側でマルウェアからの脅威を回避するには、インストールするアプリは最小限に留めること、事前にアプリストアでのレビューやSNS等での評判を参考として可能な限り実績のあるアプリを採用すること、Google Play以外からのインストールはさらにこのような不正なアプリに遭遇するリスクが高いため避けること等が肝要です。

TREND MICRO

新しい検出回避機能を備えたAndroid向けアドウェアがGoogle Playから拡散

投稿日：2019年11月27日
脅威カテゴリ：モバイル、攻撃手法
執筆：Trend Micro

トレンドマイクロは、Android向けの正規アプリマーケットである「Google Play」上で新たに、ゲームアプリやカメラアプリを偽装した49個の不正アプリを確認しました。これらは、モバイルデバイス内に隠れて広告を表示させる典型的なアドウェアですが、同時にアンインストールおよび検出を回避する機能も備えていました。これらのアドウェアはすでにGoogleによってGoogle Playから削除されています。ただし、削除される前には合わせて300万を超えるダウンロード回数を確認しており、多くの利用者が被害に遭ったものと考えられます。