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。

●Windows 10更新促す偽メールでランサムウェア被害の恐れ

https://japan.zdnet.com/article/35145650/

このニュースをザックリ言うと・・・

- 11月19日(現地時間)、米Trustwave社より、Microsoftを騙ってWindows 10への更新を促しランサムウェアに感染させようとする偽メールについて注意喚起が出されています。

- 例に挙げられているメールは英文で、件名が「Install Latest Microsoft Windows Update now!」「Critical Microsoft Windows Update!」、本文が「PLease install the latest critical update from Microsoft attached to this email.」となり、添付された偽のアップデートファイルをクリックするよう誘導するものとなっています。

- しかし、添付ファイルのクリックにより、ランサムウェア「bitcoingenerator.exe」がダウンロードされ、PC上のファイルが暗号化された上で、500ドル相当のbitcoinを要求する脅迫文が表示されるとのことです。

AUS便りからの所感等

- まだWindows 7から10等への移行が終わっていないユーザーにとって、来年1月に迫っている7の無償サポート終了は決して無視できない重要な出来事であり、オリンピック等のイベントと同様、これに便乗した攻撃は今後も多く発生するとみられます。

- Trustwave社では、「MSがメールでパッチを送ることはなく、現在はどのWindows OSにも組み込まれている内部のアップデートユーティリティを利用する」ことを把握しておくべきだとして注意を呼び掛けています。

- 7から10へ無償でアップグレードしよう等と思って、このような不審なメールに安易に釣られるのではなくMSが提供している正式な方法について調査し、場合によってはPCの買い替えも行うことを視野に入れつつ、安全に移行する段取りをとるようにしてください。

ZDNet Japan

Windows 10更新促す偽メールでランサムウェア被害の恐れ--セキュリティ企業が注意喚起

Alison DeNisco Rayome（CNET News）翻訳校正：緒方亮 高森郁哉（ガリレオ） 2019-11-20 11:08

「Windows 7」のサポート終了を2020年1月に控え、多くのユーザーが「Windows 10」にアップグレードしてMicrosoftから引き続きセキュリティ更新とサポートを受けようとしている。セキュリティ企業Trustwaveが米国時間11月19日に発表したレポートによると、攻撃者はこうした状況を十分承知したうえで、Microsoftのサービスを利用するユーザーを狙ってWindowsの更新を呼びかける偽のメールを送り、コンピューターにランサムウェアを感染させようとしているという。ランサムウェアは、コンピューター上の貴重なデータに鍵をかけて身代金（ランサム）を要求し、払わなければデータを破壊すると脅迫する悪質なマルウェアだ。

●ネット銀行での不正送金事案、9月に急増…金融庁が注意喚起-

https://crypto.watch.impress.co.jp/docs/news/1219628.html
https://www.fsa.go.jp/ordinary/internet-bank_2.html
https://www.npa.go.jp/cyber/policy/caution1910.html

このニュースをザックリ言うと･･･

- 10月24日(日本時間)に警察庁より、11月19日には金融庁より、インターネットバンキングにおける不正送金事案が9月度に急増したとして、相次いで注意喚起が出されています。

- 警察庁発表によれば、9月度に発生した不正送金事案は436件、被害額は約4億2,600万円となっており、この1ヶ月だけでも2019年上半期(1～6月)分の183件・約1億6,600万円に比べ倍以上の被害が出ています。

- 主な手口として、「銀行を騙るSMS等から偽のログインサイトに誘導し、アカウント情報やワンタイムパスワード等を詐取する」ケースと、「利用者のPCをスパイウェアに感染させてアカウント情報を奪取する」ケースが挙げられています。

AUS便りからの所感

- 前述したような手口は、正直なところ何年もの間使われ続けているものであり、今回不正送金の成功率を上げるような決定的な手口があったのか、それとも攻撃者の活動がこれまでになく活発になったのか等は不明です。

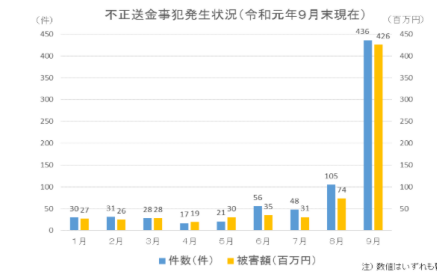
- しかしだからこそ、これまでフィッシングへの対策として推奨されてきたこと、例えば金融庁等も挙げているような「各銀行がパスワード等をSMS等で求めることはない」といった情報をWebサイトで確認する「心当たりのないSMS等は開かない」「事前に正しいウェブサイトのURLをブックマークに登録しておく」こと、あるいはフィッシングサイトへのアクセスやマルウェア感染を遮断するようブラウザー・アンチウイルスおよびUTMのセキュリティ機能を有効にすること等に改めて気を配ることが肝要です。

金融庁 Financial Services Agency

令和元年11月19日更新
金　融　庁

インターネット・バンキングによる預金の不正送金事案が多発しています。

メールやショートメッセージ（SMS等）を用いたフィッシングや、スパイウェア等の不正プログラムを用いた手口により、インターネット・バンキング利用者のＩＤ・パスワード等を盗み、預金を不正に送金する事案が多発しています。



注）数値はいずれも暫定値

（出典：警察庁HP「フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（注意喚起）」）

●トレーディングカードショップよりクレジットカード情報4,982件が流出

https://kai-you.net/article/69482
https://cybersecurity-jp.com/news/34301
https://cardshop-serra.com/user_data/cxk46J3ZV6rw.php

このニュースをザックリ言うと･･･

- 11月21日(日本時間)、トレーディングカード等の売買を行う「カードショップ セラ」より、同サイトが不正アクセスを受け、クレジットカード情報が流出したと発表されました。

- 流出した可能性があるのは、2017年9月17日～2018年11月8日に同サイトで決済に使用されたクレジットカード情報(名義人名、番号、有効期限およびセキュリティコード(CVV))4,982件とされています。

- 2018年11月8日にクレジットカード会社からカード情報流出の懸念について連絡を受けて決済を停止、今年9月30日までに第三者調査機関による調査が行われ、流出の事実が確認されたとしています。

AUS便りからの所感等

- 流出の原因については「システムの一部の脆弱性をついたことによる第三者の不正アクセス」としており、現時点でそれ以上の詳細は不明ですが、ペイメントモジュールの改ざんにより、例えばフォームから入力されたクレジットカード情報が攻撃者に送信されるよう仕向けられた可能性が一部で指摘されています。

- クレジット取引セキュリティ対策協議会が策定した「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画」により、2020年3月までに「加盟店におけるカード情報の非保持化」の完了を目指す動きが進んでいるためか、攻撃者側の手口もこれまでの「サーバー上に保存・蓄積されていたカード情報を奪取する」パターンから「カード情報の入力フォームを改ざんし、入力されたカード情報を奪取する」パターンへの移行が2018年以降目立っています。

- Webサーバー・アプリケーションの脆弱性を突かれてこのような改ざんが行われることは、サービスを信頼して重要な情報を入力するユーザーを裏切ることに繋がり得ますので、根本的対策として、使用するソフトウェアを最新のバージョンに保ち、またSQLインジェクション等が発生しないよう安全なWebアプリケーションの開発に注意すること等を心がけ、併せてIDS・IPS・WAF等により、脆弱性の悪用を許す不正なリクエストを検知・遮断する体制を整えることを推奨致します。

Cardshop Serra

個人情報流出に関するお詫びとお知らせ

2019年11月21日

お客様各位

株式会社　英宝

弊社が運営する「Cardshop Serra」への不正アクセスによる
個人情報流出に関するお詫びとお知らせ

このたび、弊社が運営する「Cardshop Serra」におきまして、第三者による不正アクセスを受け、お客様のクレジットカード情報（4,982件）が流出した可能性があることが判明いたしました。
お客様をはじめ、関係者の皆様に多大なるご迷惑およびご心配をおかけする事態となりましたこと、深くお詫び申し上げます。
なお、個人情報が流出した可能性のあるお客様には、本日より、電子メールおよび書状にてお詫びとお知らせを個別にご連絡申し上げております。

弊社では、今回の事態を厳粛に受け止め、再発防止のための対策を講じてまいります。
お客様をはじめ関係者の皆様には重ねてお詫びを申し上げますとともに、本件に関する概要につきまして、下記の通りご報告いたします。