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。

●東京五輪に便乗した標的型攻撃が発生か…「無料チケット」で不正サイトに誘導

https://japan.zdnet.com/article/35125143/

このニュースをザックリ言うと・・・

- 9月5日（日本時間）、データ分析等を行うAntuit社より、2020年の東京オリンピックに便乗する標的型攻撃が開始された可能性があると発表されました。

- 発表によれば、同社が監視していた攻撃者のフォーラムサイトで、同3日に「日本と米国の174,000人が在籍する企業への攻撃を開始した」とし、5回にわたる攻撃を示唆する投稿を確認したとのことです。

- 攻撃メールの一例として、
◆件名が「無料チケットオリンピック」
◆本文が「親愛なる購読者/あなたは幸運な参加者として選ばれます」
で始まり、無料航空券やギフト券をプレゼントすると偽って添付ファイルやリンク先のサイトからマルウェアに感染させようとするものが挙げられています。

AUS便りからの所感等

- 大きなイベントや事件には、必ずと言っていいほど便乗してのフィッシング詐欺やマルウェア感染を狙った攻撃等が発生します。

- 今年は日本各地で立て続けに豪雨・台風そして地震による甚大な被害がもたらされていますが、例えば7月の豪雨の際には偽の募金サイトが確認されています（AUS便り 2018/07/23号参照）。

- 現在発生している攻撃の他、今までにどういった攻撃が発生したかについても情報収集し、信頼のおける公共機関・自治体等についてはブックマークやSNSアカウントのフォローを行うようにしましょう。

- また、Webブラウザやアンチウイルスソフトあるいは UTMに備わっているアンチフィッシング等のセキュリティ機能は必ず有効にし、疑わしいリンクが貼られたメール等を受信した場合は「サイトや情報が信頼できるものか検索等で確認する」等の自衛策をとることを推奨致します。

ZDNet Japan

東京五輪に便乗した標的型攻撃が発生か--「無料チケット」で不正サイトに誘導

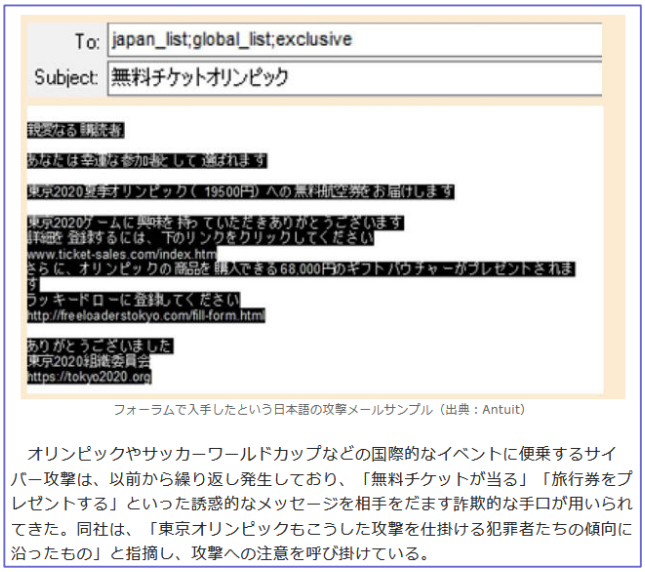
ZDNet Japan Staff 2018年09月05日 17時56分

いいね！ 42　G+　B! 12　Pocket 26

印刷　メール　ダウンロード　クリップ

データ分析のAntuitは9月5日、2020年の東京オリンピックに便乗する標的型攻撃が開始された可能性があると発表した。「無料チケット提供」をうたうメッセージから不正サイトに誘導される恐れがあるといい、日本語による偽のメール画像を公開した。

同社によると、攻撃者の狙いは、銀行のログイン情報を含む個人の機密情報を搾取して、金銭を獲得するほか、開催国の日本やオリンピック関連企業に対して風評被害を与える目的もあるという。攻撃活動は、ビジネスメール詐欺（BEC）や企業関係者などの会話の盗聴の一環として展開される可能性があるとしている。



To: japan_list;global_list;exclusive
Subject: 無料チケットオリンピック

親愛なる購読者

あなたは幸運な参加者として選ばれます

東京2020夏季オリンピック（19500円）への無料航空券をお届けします

東京2020ゲームに興味を持っていただきありがとうございます
詳細を登録するには、下のリンクをクリックしてください
www.ticket-sales.com/index.htm
さらに、オリンピックの商品を購入できる68,000円のギフトバウチャーがプレゼントされます
ラッキードローに登録してください
http://freeloaderstokyo.com/fill-form.html

ありがとうございました
東京2020組織委員会
https://tokyo2020.org

フォーラムで入手したという日本語の攻撃メールサンプル（出典：Antuit）

オリンピックやサッカーワールドカップなどの国際的なイベントに便乗するサイバー攻撃は、以前から繰り返し発生しており、「無料チケットが当る」「旅行券をプレゼントする」といった誘惑的なメッセージを相手をだます詐欺的な手口が用いられてきた。同社は、「東京オリンピックもこうした攻撃を仕掛ける犯罪者たちの傾向に沿ったもの」と指摘し、攻撃への注意を呼び掛けている。

●Office 365で「TLS 1.0/1.1」サポート打ち切り、「TLS 1.2」以上への移行を

https://internet.watch.impress.co.jp/docs/news/1141032.html

このニュースをザックリ言うと･･･

- 8月31日（日本時間）、Microsoftより、同社の「Office 365」において、10月31日をもって暗号化通信プロトコル「TLS 1.0/1.1」のサポートを打ち切ると発表されました。

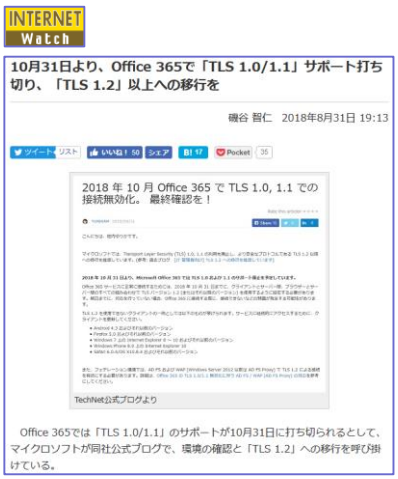
- 同社ではより新しい「TLS 1.2」以降を使用するよう呼びかけており、TLS 1.2非対応の古いクライアント（「Windows 7上のInternet Explorer 10以前」「Safari 6.0.4/OS X 10.8.4以前」等）といったクライアントについては11月以降アクセスできなくなるため、クライアントを更新するよう求めています。

AUS便りからの所感等

- 暗号化通信や証明書において今も「SSL」という単語が使われますが、実際にはその後継である「TLS」の方が一般的に利用されており、SSLやTLS 1.0/1.1にはプロトコル自体に暗号化通信を解読され得る等の脆弱性が発見されていることから使用しないことが推奨されており、多くのWebサイトやWebサービスがTLS 1.2以降のみ受け付けるようになっています。

- 既にサポート切れのXPやVistaはTLS 1.0までしか対応しておらず、Windows 7についてはTLS 1.2を使用しない設定になっている可能性があるため、「インターネットオプション」において設定を確認してください。

- 前述したようなWebサイトでの設定や「常時HTTPS化」の流れもあり、古すぎるクライアントでは今後まともにインターネットにアクセスできなくなる可能性も考えられ、やむを得ない事情から使い続ける場合、それによるリスクを十分に考慮し、インターネットあるいはLANから隔離する等の処置をとることも視野に入れなければならないでしょう。


INTERNET Watch

10月31日より、Office 365で「TLS 1.0/1.1」サポート打ち切り、「TLS 1.2」以上への移行を

磯谷 智仁　2018年8月31日 19:13

2018 年 10 月 Office 365 で TLS 1.0, 1.1 での接続無効化。最終確認を！

TechNet公式ブログより

Office 365では「TLS 1.0/1.1」のサポートが10月31日に打ち切られるとして、マイクロソフトが同社公式ブログで、環境の確認と「TLS 1.2」への移行を呼び掛けている。

●Windowsタスクスケジューラに未修正の脆弱性…悪用コード・マルウェアも確認

http://www.itmedia.co.jp/enterprise/articles/1809/06/news062.html

このニュースをザックリ言うと･･･

- 8月27日（現地時間）、米セキュリティ機関のCERT/CCより、Windowsに未修正の脆弱性が確認されたとして注意喚起が出されています。

- 脆弱性はWindowsタスクスケジューラの「Advanced Local Procedure Call(ALPC)」に存在し、PCにログインしているユーザが悪用することにより、システム権限を奪取される恐れがあるとされています。

- 発表の時点で脆弱性を悪用するコードが出回っていた他、その2日後にはこのコードを参考にしたとみられるマルウェアが確認されたとして、9月5日にセキュリティベンダーのESET社より発表されています。

AUS便りからの所感等

- 9月12日（日本時間）には月例のセキュリティパッチのリリースが予定されており、脆弱性はここで対策されるものと考えられます。

- 当日の情報で実際に修正されたかどうか確認することは大事ですが、いずれにせよセキュリティパッチの適用は必ず行うようにしましょう。

- ESETの発表によれば、「PowerPool」と呼ばれる攻撃者グループにより、マルウェアを添付したメールによる攻撃が行われている模様です。

- 多くのアンチウイルスソフトやUTMでは対応済みとみられていますので、これらによる防御を十分に行うこともまた忘れてはいけません。


ITmedia エンタープライズ

Windowsタスクスケジューラに発覚した脆弱性、たった2日で悪用マルウェアが出回る

この脆弱性を突くコンセプト実証コードのソースコードも公開されていて、誰でもこれに手を加え、自分のコードに取り込むことができてしまう状態にあるという。

[前本梨子, ITmedia]

Windowsのタスクスケジューラに発覚した未解決の脆弱性について、セキュリティ企業のESETは9月5日、この脆弱性を突くマルウェアが出回っているのを発見したと伝えた。

Windowsタスクスケジューラ「Advanced Local Procedure Call（ALPC）」の脆弱性に関する情報は、8月27日にGitHubに掲載された。現時点でMicrosoftの修正パッチは公開されていない。

ESETによると、GitHubに掲載された情報の中には、この脆弱性を突くコンセプト実証コードのソースコードも含まれていた。つまり、誰でもこれに手を加えて、自分のコードに取り込むことができてしまう状態にあった。

ESETはそれからわずか2日後に、このコードを使ったマルウェアが出回っているのを発見。このマルウェアを開発している集団を「PowerPool」と命名した。

Windowsタスクスケジューラに発覚した脆弱性は、GitHubに悪用コードが掲載され、SNSなどを通じて瞬く間に広がった（出典：ESET）