— AUS（アルテミス・ユーザ・サポート）便り 2018/07/02号 —
https://www.artemis-jp.com

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。

●試合の日程や結果チェックのツールに偽装したマルウェア確認…W杯に便乗した攻撃に注意

https://www.checkpoint.co.jp/press/2018/pressrelease_20180622.html
https://japan.zdnet.com/article/35121291/2/

このニュースをザックリ言うと・・・

- 6月18日（日本時間）、セキュリティベンダーのチェック・ポイント・ソフトウェア・テクノロジーズ（以下チェックポイント）社より、FIFAワールドカップに便乗してマルウェア添付メールによる攻撃が確認されたと発表されました。

- 拡散されたメールは、件名が「World_Cup_2018_Schedule_and_Scoresheet_V1.86_CB-DL-Manager」で、添付されたファイルを開くことにより、マルウェアをダウンロードする仕組みになっていた模様で、試合の日程や結果チェックのツールに偽装し、興味を引いたユーザをマルウェアに感染させる意図があったとみられます。

- チェックポイント社ではこのような攻撃に対し、
「ソフトウェアを最新の状態に維持する」「偽のWebサイトに注意する」「心当たりのない差出人からの電子メールに注意する」「Wi-Fiホットスポットの使用に注意する」
ことを呼び掛けています。

- この他、チェックポイント社以外のセキュリティベンダー等からも、この手のイベントに便乗する攻撃への警戒が呼び掛けられています。

AUS便りからの所感等

- 前述のメール攻撃は5月30日に初めて確認されていましたが、大会が開幕してから再度活発化したとのことです。

- 今年は2月の平昌オリンピックにおいても、公式サイトのハッキングや会場内のシステムあるいは開会式の演出において障害が出るなどの問題が発生しています（AUS便り 2018/02/19号参照）。

- ともあれ、先日にはKaspersky社が注意喚起を出した（AUS便り 2018/06/18号参照）のと同様、この時期に増加するであろう攻撃にどういったものが確認されているか情報収集を行いつつ、安易に攻撃者の仕掛ける罠に飛びつかないよう慎重に行動することを改めて意識しましょう。

Check Point SOFTWARE TECHNOLOGIES LTD

チェック・ポイント、サッカー・ワールドカップ人気に便乗したフィッシング・キャンペーンを確認

試合の日程や結果チェックのツールをダウンロードさせ、マルウェアに感染させる新たな攻撃が発生

2018年6月22日

PDF 版のダウンロード (426KB)

カルフォルニア州 サン カルロス - 2018年6月18日
ゲートウェイからエンドポイントまで、包括的セキュリティを提供するチェック・ポイント・ソフトウェア・テクノロジーズ(Check Point® Software Technologies Ltd. NASDAQ: CHKP) は本日、先ごろ開幕したサッカーのFIFAワールドカップに便乗するフィッシング・キャンペーンを発見したと発表しました。このキャンペーンでは、試合の日程や結果をチェックするツールをダウンロードさせ、マルウェアに感染させるという手口が用いられています。

フィッシング・メールに添付されたファイルを開くと、好ましくないプログラム（PUP）をダウンロードする既知のダウンローダ「DownloaderGuide」の亜種が実行されます。このダウンローダは、ツールバーやアドウェア、システム最適化ユーティリティなどのアプリケーションのインストーラとして広く使用されています。チェック・ポイントの研究者が確認したところによると、このキャンペーンでは、合計9種類の実行可能ファイルが使用されており、

「World_Cup_2018_Schedule_and_Scoresheet_V1.86_CB-DL-Manager」

という件名の電子メールで送信されています。

このキャンペーンは、2018年5月30日に初めて観測され、6月5日に最初のピークを迎えました。ただし、大会が開幕した先週から再び勢いを増し、新たな攻撃の発生が確認されています。

ZDNet Japan

熱戦のW杯、サイバー犯罪者も別の意味で盛り上がる - (page 2)

Danny Palmer （ZDNet.com） 翻訳校正： 石橋啓一郎 2018年06月25日 06時30分

いいね！ 38　G+　B! 6　Pocket 36

印刷　メール▼　ダウンロード▼　クリップ

また、国家によるハッキングに関しては、ワールドカップの舞台がロシアであることが、通常とは異なる要因として働いている。

欧米諸国の政府は、ロシア政府が後援するハッキンググループを非難することが多いが、ロシア国内でイベントが開催されている場合、標的になるのはイベントのインフラではなく、訪れている観客になるかもしれない。

米連邦捜査局（FBI）の高官は12日、ワールドカップを観戦しに行く旅行者に対して、持ち込んだスマートフォンやノートPCがロシアのハッカーやサイバー犯罪者の標的になる可能性があると警告した。

FBI捜査官兼国家防諜安全保障センターのディレクターであるWilliam Evanina氏は、Reutersの取材に対して「もっともリスクが高いのは企業の役員や政府職員だが、自分は重要人物ではないため標的にはならないと考えるべきではない」と述べた。

●6国公私大、フィッシング被害…情報流出のべ1万件超

https://this.kiji.is/385035736119952481

このニュースをザックリ言うと・・・

- 今年4月から6月にかけ、6つの国公私立大学でフィッシング被害による個人情報等の流出が相次いで発生しています。

- 流出が発表されたのは（以下発表日と流出件数）、立命館大（5月2日・264件）、富山県立大（5月30日・275件）、横浜市立大（6月7日・5794件）、沖縄県立看護大（6月20日・330件）、島根大（6月22日・573件）および弘前大（6月27日・3151件）となっており、合計で延べ1万件超の被害が出ています。

- 6月27日（日本時間）には文部科学省より、全国の大学に対して対策を強化するよう注意喚起が出されています。

AUS便りからの所感等

- 殆どのケースがフィッシングメールによって誘導された偽サイトにおいてアカウント情報が奪取され、不正なメール転送設定が行われた結果、個人情報が記載されたメールが外部に転送されるという形での流出となっており、この他、島根大では約2800件の迷惑メールを送信させられる事態にもなっています。

- いずれもMicrosoftが提供するクラウドサービス「Office 365」を利用していたことから、攻撃者は各大学が使っているメールサーバ情報を調査し、フィッシングの準備を行ったものと考えられます。

- フィッシングへの対策として、アンチウイルスやWebブラウザあるいはUTMのセキュリティ機能を有効にすることと、本物のサービスサイトに確実にアクセスするようブックマークに登録すること、またOffice 365に備わっている2段階認証（多要素認証）も可能な限り有効にすることを推奨致します。


KYODO

6国公私大、フィッシング被害

情報流出1万件超、文科省

2018/6/28 20:54

©一般社団法人共同通信社

文部科学省は28日までに、弘前大（青森県弘前市）など六つの国公私立大が、今年4月から6月にかけて、偽サイトに誘導してID、パスワードを盗む「フィッシング」メールの被害に遭い、結果として大量の個人情報流出につながったとして、全国の大学に対して対策を強化するよう注意喚起した。

サイバー犯罪者は盗んだID、パスワードで不正ログインし、学生らのメールを勝手に外部転送するよう設定していたとみられる。文科省によると、6大学では、合計約1万2千人分の個人情報が漏えいしていた。

弘前大のほか被害が判明したのは、横浜市立大、富山県立大、立命館大、島根大、沖縄県立看護大。

文部科学省

●IPA、主要なサーバ向けOSSの「更新まとめ」を開設

https://japan.zdnet.com/article/35121571/

このニュースをザックリ言うと・・・

- 6月27日（日本時間）、情報処理推進機構（IPA）より、主要なサーバ向けオープンソースソフトウェア（OSS）の更新やセキュリティに関する情報を集約して配信するWebサイトが公開されました。

- 対象となるOSSは、「Apache HTTP Server」「Apache Struts」「Apache Tomcat」「BIND」「Joomla!」「OpenSSL」および「WordPress」となっています。

- IPAでは今後週一回程度のペースで情報を更新し、Webサイトの運営者や構築者（SIerなど）、組織内のシステム管理者向けに情報提供するとしています。

AUS便りからの所感等

- 対象とされているOSSはいずれも国内でサーバ・Webサイト構築の際に広く用いられており、またそのため攻撃者からも脆弱性を狙われることが多い一面を持っています。

- 中には頻繁に脆弱性が報告され、修正バージョンがリリースされるものもあり、管理者にとっては是非とも定期的な巡回を行い、各ソフトウェアを安全な状態に保つ体制を整えるために参考とすべきサイトといえるでしょう。

- なおLinuxで構築したサーバではこういったソフトウェアをインストール・アップデートするにあたり、ソースコード等を入手して自分でインストールするケースとディストリビューションが提供するパッケージを使用するケースがありますが、それぞれ一長一短があり、前述のIPAの情報等をもとに確実にアップデートするのでなければ、後者の方法を用いることにより、パッケージのアップデートを一括で行う方が良いでしょう。


ZDNet Japan

IPA、主要なサーバ向けOSSの"更新まとめ"を開設

ZDNet Japan Staff 2018年06月28日 10時05分

いいね！ 95　ツイート　G+　B! 17　Pocket 65

印刷　メール　ダウンロード　クリップ

情報処理推進機構（IPA）は6月27日、主要なサーバ向けオープンソースソフトウェア（OSS）の更新やセキュリティに関する情報を集約して配信するウェブページを開設した。ウェブサイトの運営者や構築者（SIerなど）、組織内のシステム管理者向けに情報提供する。

提供対象のOSSは、Apache HTTP Server、Apache Struts、Apache Tomcat、ISC Bind、Joomla!、OpenSSL、WordPress。開発者やダウンロードページ、脆弱性などのセキュリティ関連、最新バージョンの情報と注意喚起などの参考情報を一覧で表示し、詳細情報を掲載しているコミュニティーページなどへのリンクも提供する。