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。

●豪雨災害便乗のフィッシングに注意、Yahoo募金サイトの偽物に警告

https://security.yahoo.co.jp/news/0005.html
https://www.buzzfeed.com/jp/kotahatachi/yahoo-donation

このニュースをザックリ言うと・・・

- 7月17日（日本時間）、Yahoo! JAPANより、「Yahoo!ネット募金」の「平成30年7月豪雨緊急災害支援募金」のサイトをかたるフィッシングが確認されている として注意喚起が出されています。

- 同社では15日頃から偽サイトの存在を認識しており、「Yahoo!ネット募金」の正しいURLとして https://donation.yahoo.co.jp/ にアクセスするよう呼び掛けています（一部ページについては https://docs-donation.yahoo.co.jp/ で始まるものもあるとのことです）。

- 別の情報によれば、偽サイトの一例として「yahoo-donation.●●●●」が挙げられており、本物のサイトと非常に似通ったものとなっている模様で、差異としては、本物のサイトでTポイントによる寄付を受け付けている部分が偽サイトではWebMoneyを受け付けるよう書き換えられています。

AUS便りからの所感等

- 7/20時点で上記のサイトは有効ですが、Chromeのアンチフィッシング機能によりアクセスが遮断されることを確認しています。

- Webブラウザやアンチウイルスソフト、あるいはUTMに備わっているセキュリティ機能は必ず有効にしてください。

- 加えて、疑わしいリンクが貼られたメール等を受信した場合は、
◆サイトや振込先情報が信頼できるものか検索等で確認する
◆本物のサイトの総合トップページ（Yahoo! JAPAN等）からアクセスして辿っていく
◆普段利用するサイトであればブックマークからアクセスする
等の自衛策をとることを推奨致します。

YAHOO! JAPAN セキュリティセンター

当社をかたるフィッシングメール、不正メールに関する注意喚起

更新日時：2018年07月17日

キーワード： フィッシング ， 予防と対策

当社をかたるフィッシングメール、不正メールにご注意ください。

当社名や当社ロゴを悪用し、フィッシングサイトに誘導しようとしたり、個人情報を入力させて返信させようとしたりする不正メールが確認されています。

2018年7月15日頃より、Yahoo!ネット募金の「平成30年7月豪雨緊急災害支援募金」を模倣した偽サイトを確認しています。
Yahoo!ネット募金の正しいURLは「https://donation.yahoo.co.jp/」です。
※一部のページは「https://docs-donation.yahoo.co.jp/」で始まるURLの場合もあります。

不審なメールやメッセージを受信した場合には、開かずに削除しましょう。
フィッシング詐欺かどうかの判断が難しい場合には、メール内のリンクはクリックせず、普段使っているブラウザーの「お気に入り（ブックマーク）」や検索サイトから目的のウェブサイトへアクセスしましょう

フィッシング被害に遭わないために

BuzzFeed News

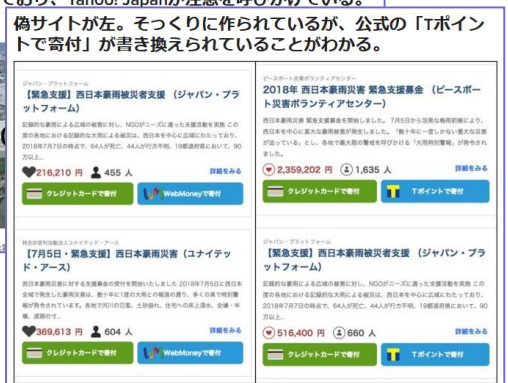
西日本豪雨「Yahoo!募金」の偽サイトにご注意　中国で取得か

フィッシング詐欺の可能性が高い。

2018/07/17 15:04

西日本豪雨災害の緊急支援をつのる「Yahoo!ネット募金」の偽サイトができており、Yahoo! Japanが注意を呼びかけている。

偽サイトが左。そっくりに作られているが、公式の「Tポイントで寄付」が書き換えられていることがわかる。



●ロシアのサイバー攻撃集団「Sandworm Team」が日本の物流企業を標的に、FireEyeが観測

https://internet.watch.impress.co.jp/docs/news/1133817.html

このニュースをザックリ言うと・・・

- 7月19日（日本時間）、セキュリティベンダーのFireEye社主催によるセキュリティカンファレンス「Cyber Defense LIVE Tokyo 2018」が開催されました。

- 同社CEOの基調講演では、今年5月初旬、ロシアのサイバー攻撃集団「Sandworm Team」によるとみられる日本国内の物流企業へのサイバー攻撃が観測されたことが発表されており、日本の企業がターゲットとなったことについては「極めて珍しい事例」とし「メインターゲットの一歩前になる中継点として攻撃された」ものと推測されています。


INTERNET Watch

ロシアのサイバー攻撃集団「Sandworm Team」が日本の物流企業を標的に、FireEyeが観測

磯谷 智仁　2018年7月20日 11:40

日本の物流企業をターゲットにしたロシアからの攻撃も観測

2018年5月初旬にはロシアのサイバー攻撃集団「Sandworm Team」と思われるグループから、国内の物流企業を標的にしたサイバー攻撃が観測されたという。これらは、標的とされた業種や、ステージングディレクトリ設定、利用されたVPSなど、優書されたネットワーク上での活動に類似性が見られたとしている。

これまで、同グループは主にウクライナを標的とした活動を展開しており、ウクライナにおける2015年と2016年の停電事件やEternalPetya攻撃などの複数の破壊的活動に関与したとみられている。2016年以降は活動地域を米国や欧州などにも広げている。

今回、日本の企業が標的になったことに関して、ファイア・アイ株式会社最高技術責任者（CTO）の伊東寛氏は「極めて珍しい事例」としながらも、「日本はメインターゲットの一歩前になる中継点として攻撃されたのではないか」と推測する。

AUS便りからの所感等

- Sandworm Teamはこれまでウクライナを主な標的とした活動を行っており、2015年・2016年には同国内でマルウェアによる大規模な停電を引き起こしたとされています（AUS便り 2017/06/19号参照）。

- これまでにサイバー攻撃の被害に遭ったケースで主に見られた問題として、「スピア(標的型)フィッシングや悪意のある攻撃を見逃していた」「ずさんな認証情報管理」「ネットワークがセグメント化されていない」「VPNやOWAへのアクセス認証が1段階のみ」「セキュリティ保護が管理者権限から守られていない」「レスポンスに必要な重要データが集められていない」等が挙げられています。

- 何か一つソリューションを導入するだけで全ての問題をカバーできるものはなく、アンチウイルス・UTMの導入やセキュアなネットワーク構成の構成等、それぞれの対策が何を防御するのかを把握し、万一どれかが機能しなかったとしても他のソリューションで補完し、内外への攻撃や情報の流出を遮断できるような組み合わせを行うことが重要と言えます。

●6月はWindowsプロトコル「SMB」の脆弱性を悪用する攻撃が増加傾向…キヤノンITS発表

https://prtimes.jp/main/html/rd/p/000000419.000001375.html

このニュースをザックリ言うと・・・

- 7月13日（日本時間）、キヤノンITソリューションズ社より、2018年6月期のマルウェアレポートが発表されました。

- レポートでは3つのトピックとして「VBA機能を悪用したダウンローダーが4ヶ月連続で1位」「ワールドカップに関連した詐欺メール」そして「Windowsプロトコル(ファイル共有等に利用)『SMB』の脆弱性を悪用する攻撃を多数確認」が挙げられています。

- SMBの脆弱性は2017年3月に「MS17-010」としてマイクロソフトよりセキュリティパッチが出されているにも関わらず、今年4月以降攻撃の検知数が急上昇しています。


PRTIMES

2018年6月のマルウェアレポートを公開～Windowsプロトコル「SMB」の脆弱性を悪用する攻撃が増加傾向～

キヤノンITソリューションズ株式会社

2018年7月13日 12時00分

いいね！ シェア

キヤノンマーケティングジャパングループのキヤノンITソリューションズ株式会社（本社：東京都品川区、代表取締役社長：足立 正親、以下キヤノンITS）は、2018年6月のマルウェア検出状況に関するレポートを公開しました。

2018年6月 マルウェアレポート

■2018年6月のマルウェア検出状況に関するレポートをウェブで公開

キヤノンITSのマルウェアラボでは、国内で利用されているウイルス対策ソフト「ESETセキュリティ ソフトウェア シリーズ」のマルウェア検出データをもとに、2018年6月のマルウェア検出状況を分析し、以下のウェブサイトにレポートを公開しました。

AUS便りからの所感等

- MS17-010のセキュリティパッチは当時サポートが終了していたWindows XP等についても対応されたものですが、XPについては手動での適用が必要となっており、このことからも、XPが稼働し、かつパッチを適用していないPCが現在も少なからず存在すると想定して今も攻撃が続いていると推測されます。

- UTM等を用いインターネット上からファイルサーバ等のSMB関連ポートにアクセスされないようフィルタリングすべきであることは言うまでもありませんが、マルウェアに感染したPCを踏み台として社内LAN上に攻撃が行われる可能性についても決して怠ることなく対応しなければなりません。

- 全てのPCについてアンチウイルスの導入はもちろん、それぞれのPCが自由にアクセスできないよう、PC上とゲートウェイレベルでのフィルタリングをすることが望ましいでしょう。