— AUS（アルテミス・ユーザ・サポート）便り 2017/06/12号 —
http://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。

●件名「日本郵便 インボイス用紙」「請求書」のウイルスメール出回る…警視庁等注意喚起

http://www.itmedia.co.jp/news/articles/1706/02/news080.html
https://www.jc3.or.jp/topics/virusmail.html

このニュースをザックリ言うと・・・

- 6月2日（日本時間）、警視庁と日本サイバー犯罪対策センター（JC3）より、日本郵便をかたった、ウイルスが添付されたメールが同1日より拡散しているとして警告が出されています。

- 警告では以下の2種類のメールが挙げられており、いずれも文書ファイルに偽装したウイルスが添付されているとのことです。

① 件名が「請求書」、本文が「お世話になっております。無事許可となりました。」で始まり、「コマーシャル・インボイス.xls」が添付

② 件名が「日本郵便 インボイス用紙」、本文が「アライバル訂正ありがとうございました。」で始まり、「(数字).zip」が添付

- その後、同7日にも以下のような同様のメールが拡散し、再度警告が出されています。

③ 件名が「請求書」、本文が「契約内容の詳細につきましては添付のファイルをご確認ください。」で始まり、「(数字).xls」が添付

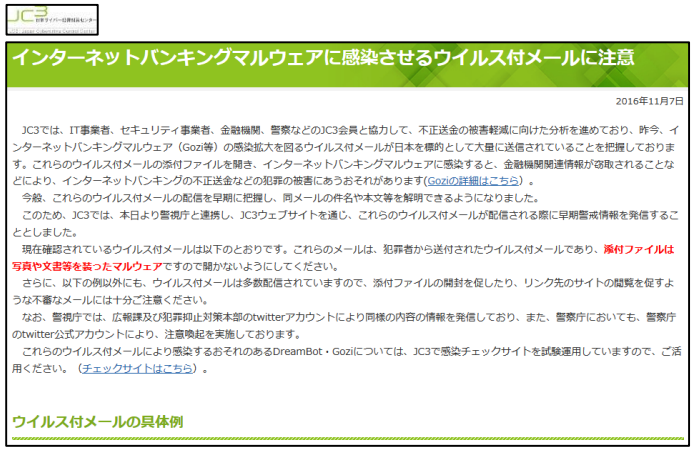
④ 件名が「請求書を添付」、本文に「12日、月曜日に支払いして下さい」という記述、「御請求書.xls」が添付

⑤ 件名が「請求書ほか」、本文に「請求書.完成届.目的物引き渡書」という記述、「請求書(完成届).xls」か「(数字).xls」が添付

AUS便りからの所感等

- これらのメールは、国内のオンラインバンキングやクレジットカード利用者を狙うマルウェア「URSNIF(gozi)」への感染を意図したものである可能性が高く、例えば、5月中旬にも大量拡散がみられていて（AUS便り 2017/5/22号参照）、JC3の情報を見る限り、それ以外の時期でも不定期に比較的短いスパンで拡散がみられており、メールの内容も件名や文面をたびたび変えられています。

- マルウェアへの感染を効果的に防ぐには、一つに随時のユーザに対する啓発と定点観測情報やSNS等での日頃の情報収集、今一つはPC等のOS・アプリ・アンチウイルスのパターンファイルを最新に保つこととUTMを設置すること等の防御策をとること、その両方を組み合わせることが大事です。



●アドウェア「Fireball」、世界中に拡散…Check Point社が警告

https://japan.zdnet.com/article/35102307/

このニュースをザックリ言うと・・・

- 6月1日（現地時間）、大手セキュリティベンダーのチェックポイント社より、世界中の2億5000万台近くのPC（WindowsおよびMac）にインストールされているマルウェア「Fireball」について、同社ブログにて警告が出されています。

- 同社によれば、Fireballは他のソフトウェアに同梱されるアドウェア（広告表示等によって収入を得るソフトウェア）としてインストールされ、ブラウザの通信をハイジャックし、例えばデフォルトのサーチエンジンへの検索リクエストを偽のサーチエンジンにリダイレクトすることにより、広告収入を得るものとされています。

- 一方でFireballには、他にもブラウザが閲覧したページ等を追跡してプライベートな情報の収集を行ったり、外部からバックドア等のマルウェアをダウンロードしてインストールしたりする機能を持っていることが判明しています。

- なお、Fireballのアンインストールは「コントロールパネル」の「プログラムと機能」から簡単に実行できるようです。


ZDNet Japan

アドウェア「Fireball」、世界で2億5000万台のPCに拡散

Danny Palmer （ZDNet.com） 翻訳校正： 編集部 2017年06月06日 11時48分

いいね！ 15　G+ 4　B! 4　Pocket 25

あるアドウェアがまん延しているという。発見者であるCheck Pointのサイバーセキュリティ研究者らによると、このアドウェアは世界各地の2億5000万台あまりのPCにインストールされており、企業の社内ネットワークの20%が影響を受けているという。

「Fireball」と呼ばれるこのアドウェアは、ユーザーのブラウザをハイジャックし、ウェブトラフィックに手を加えるかたちで動作する。Fireballは、広告収入を目的としたものだと考えられているが、セキュリティ研究者らによると、任意の操作を実行できるようになっているため、PCをリスクにさらすようなバックドアの設置も可能だという。

AUS便りからの所感等

- 現時点ではFireballが大規模な損害を与える挙動は発生していないようですが、そのような攻撃を行うための機能は持ち合わせており、外部からの指令等により、一斉に活動を開始する可能性もないわけではありません。

- ソフトウェアのインストール時に別のソフトウェアのインストールを求められる場合がありますが、その殆どがアドウェアであり、インストールをさっさと終わらせようとしてうっかりアドウェアもインストールしてしまうケースは珍しくないため、インストールするソフトウェアにアドウェアが含まれていないかとそれを回避する手順とを事前に情報収集するのが良いでしょう。

- マルウェアの外部からの侵入のみならず、内部から指令サーバ等への通信を遮断する意味でも、UTMの導入が推奨されます。

●国交省の土地総合情報システムから個人情報4,000件強が流出

http://www.itmedia.co.jp/enterprise/articles/1706/06/news138.html

このニュースをザックリ言うと・・・

- 6月6日（日本時間）、国土交通省より、同省「土地総合情報システム」の「不動産取引価格アンケート回答（電子回答）」サイトが不正アクセスを受け、個人情報等が流出した可能性があると発表されました。

- 発表によれば、流出の可能性があるのは、4月7日～6月2日にサイト上で作成されたアンケート回答情報で、氏名・法人名、契約日、取引価格等の個人情報最大4,335件と、売買等を原因とする所有権移転登記情報最大194,834件（ただしこちらは登記所等で入手可能な公開情報）となっています。

- サイトで使用されていた「Apache Struts2」の脆弱性を突いて不正なプログラムが仕込まれていたことが流出の原因とみられ、同省では6月2日に電子回答システムを停止、実際の個人情報流出の有無を調査するとともに、システム監視の強化及び再発防止の為の対策を行うとしています。


ITmedia エンタープライズ

国交省の土地総合情報システムから個人情報4000件強が流出　Apache Struts2が原因

国土交通省が「土地総合情報システム」の「不動産取引価格アンケート回答（電子回答）」サイトに不正なアクセスがあったことを明らかにした。「Apache Struts2」の脆弱性を利用して、悪意のあるプログラムが仕込まれていた。

[国部毅，ITmedia]

印刷／PDF 26 ツイート　いいね！ 15　シェア 15　B! Bookmark 1　Pocket 9　G+ 1　通知

国土交通省が6月6日、同省の「土地総合情報システム」の「不動産取引価格アンケート回答（電子回答）」サイトに不正なアクセスがあったことを明らかにした。4月7日から6月2日までに情報が公開された「Apache Struts2」の脆弱性を利用して、悪意のあるプログラムが仕込まれていた。

AUS便りからの所感等

- Struts2の脆弱性が3月に発表されて以降、これを悪用した攻撃とそれによる被害は現在に至るまで続いており、当「AUS便り」でもたびたび取り上げています。

- 同省でも3月の時点で指摘を受け、管理委託していた企業に対応を指示したとのことですが、2017年度の予算による機能追加とあわせての脆弱性対策となったという情報もあり、不正プログラムの発覚等の対応に時間がかかったのはこれが要因とみられます。

- 大規模なシステムとなるとソフトウェアの改修・試験に時間とコストがかかるのは確かですが、それでも脆弱性情報の発表があったときに可能な限り短い期間と低いコストで柔軟に改修等の対応ができるような体制作りが今後新たなポイントとして求められることになるでしょう。