— AUS（アルテミス・ユーザ・サポート）便り 2016/02/15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。

●偽Flash更新マルウェア、OS X感染を狙う手口が横行

http://www.itmedia.co.jp/news/articles/1602/05/news060.html
https://isc.sans.edu/forums/diary/Fake+Adobe+Flash+Update+OS+X+Malware/20693/

このニュースをザックリ言うと・・・

- 2月4日（現地時間）、米セキュリティ機関SANS Internet Storm Centerより、（Mac）OS Xユーザに対して偽の警告を表示してマルウェアをインストールさせようとする手口が確認されたとして、警告が発表されました。

- 偽の警告は「あなたのFlash Playerは古くなっています。アップデートをインストールして下さい」と英語で表示するもので、クリックすると、正規のFlash Playerと一緒に「スケアウェア(システムに問題があると警告して金銭を払わせようとするマルウェア)」(※)等のマルウェアをMacにインストールさせようとする不正なインストーラがダウンロードされる模様です。

- 不正なインストーラは有効なApple開発者証明書で署名されており、アンチウイルスソフトの殆どがこの時点でマルウェアを検出できなかったとされています。

- SANSでは「Flashは常に最新版に更新しておくよう呼び掛けが行われているため、ユーザはだまされてしまいやすい」と分析しています。

AUS便りからの所感等

- Macに感染するマルウェアも今では珍しくなく、Windowsと同様に注意が必要です。

-アンチウイルス・UTMの導入は必要不可欠ですが、今回のようなケースも有り得ない話ではないと念頭に置き、Flash Playerのアップデートは Adobeのサイトから行う等を改めて心がけるようにしましょう。（https://helpx.adobe.com/jp/flash-player/kb/235972.html）

ITmedia ニュース

速報　2016年02月05日 07時45分 更新

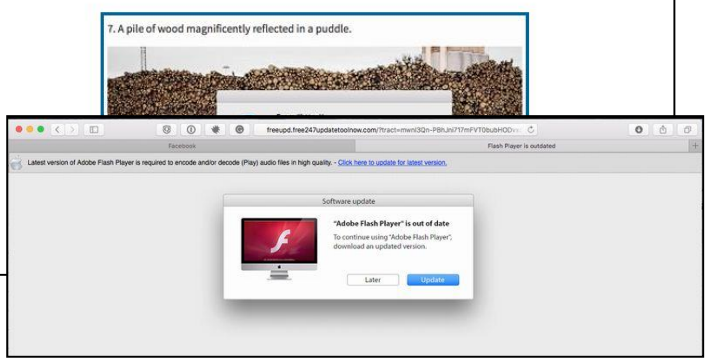
偽Flash更新マルウェア、OS X感染を狙う手口が横行

Flashは常に最新版に更新しておくよう呼び掛けが行われているため、ユーザはだまされてしまいやすいという。

[鈴木聖子, ITmedia]

OS XのユーザーにAdobe Flash Playerの更新を促すと見せかけてリンクをクリックさせ、マルウェアをインストールさせようとする手口が出回っているという。米セキュリティ機関SANS Internet Storm Centerが2月4日のブログで報告した。

SANSの研究者はFacebook上の「クリックベイト」と呼ばれる釣りコンテンツについて調べている際に、この手口に遭遇した。ポップアップ表示された画面は英語で「あなたのFlash Playerは古くなっています。アップデートをインストールして下さい」と警告する内容だった。



怪しい更新通知（SANSより）

SANS ISC InfoSec Forums

Fake Adobe Flash Update OS X Malware

Yesterday, while investigating some Facebook click-bait, I came across a fake Flash update that is targeting OS X users. Fake flash updates have been very common to infect OS X. They do not rely on a vulnerability in the operating system. Instead, the user is asked to willingly install them, by making them look like genuine Adobe Flash warnings (and we keep telling users to make sure Flash is up to date, so they are likely going to obey the warning and install the update).

The "installer" for the fake Flash update will install various scare ware (I observed a couple different varieties when re-running the installer), and it actually installs an up to date genuine version of Flash as well.

While I wasn't able to capture the exact trigger for the popup advertising the update, I suspect it was injected by one of the many ads on the page:

NTT PC COMMUNICATIONS

（※）スケアウェア【英】scareware

スケア（scare）は、「怖がらせる」とか「おびえさせる」といった意味。そして、実際には何の機能もないのに、脅しの目的で作られたソフトウェアをスケアウェアという。典型的なのは、次のようなケース。

ちょっと怪しげなウェブサイトを興味本位でのぞいてみた。すると急にポップアップ画面が開いて、パソコンの中を検索し始めた。やがて、「あなたのコンピュータにはスパイウェアとウイルスが存在します。今すぐ、この対策ソフトをインストールしてください」といった表示が出る。驚いて、画面上のボタンをクリックして対策ソフトを購入したくなる。だけど、これがまったくのウソ。あなたを慌てさせて、偽の対策ソフトの代金やクレジットカード番号を奪い取るのが目的だ。

そして、このとき使われる偽の対策ソフトをスケアウェアと呼ぶ。しかも、スケアウェアには何の機能もない。ただ、検索しているような画面と「感染している」というウソの画面を表示するだけだ。怖いのは、普段から見ているサイトや有名サイトでも、こうした被害にあう可能性があること。そのサイトが不正な攻撃を受けていると、本来は安全なサイトにスケアウェアが仕掛けられていたり、犯人が用意した別のサイトへ勝手に移動されたりすることがある。

いずれにしてもインターネット上で、いきなり「お金を払え」といわれたら、まず疑ってかかるほうがいい。

●ヤフーのFX子会社から顧客情報18万件がネット上に、元従業員が持ち出し

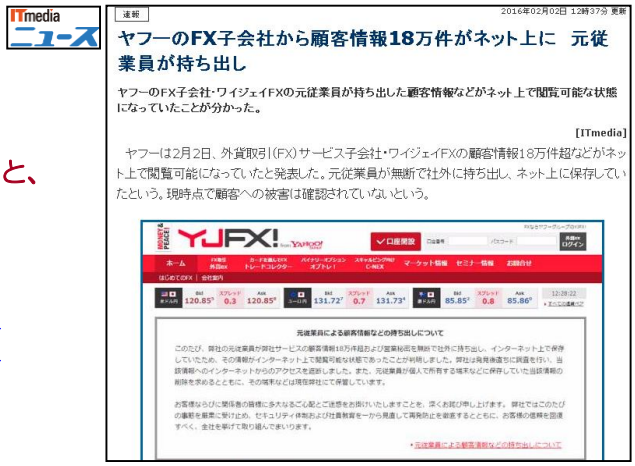
http://www.itmedia.co.jp/news/articles/1602/02/news077.html

このニュースをザックリ言うと・・・

- 2月2日（日本時間）、ヤフー株式会社は、同社のFX（外貨取引）サービス子会社であるワイジェイFX社（以下YJFX社）の顧客情報185,626件がネット上で閲覧可能になっていたと発表しました。

- 情報はYJFX社サービス「外貨ex」「MT4」「C-NEX」に関するもので、うち64,079件についてはユーザ情報（氏名、住所、銀行口座、生年月日、メールアドレス等）と取引情報が含まれていたとされています。（残る121,547件は個人情報などが含まれない取引情報のみ）

- 情報はYJFX社の元従業員が営業秘密とともに無断で持ち出し、インターネット上で保存していたものとされています。


ITmedia ニュース

速報 2016年02月02日 12時37分 更新

ヤフーのFX子会社から顧客情報18万件がネット上に 元従業員が持ち出し

ヤフーのFX子会社・ワイジェイFXの元従業員が持ち出した顧客情報などがネット上で閲覧可能な状態になっていたことが分かった。

[ITmedia]

ヤフーは2月2日、外貨取引（FX）サービス子会社・ワイジェイFXの顧客情報18万件超などがネット上で閲覧可能になっていたと発表した。元従業員が無断で社外に持ち出し、ネット上に保存していたという。現時点で顧客への被害は確認されていないという。

AUS便りからの所感等

- 内部関係者による持ち出しによるケースでは、2014年7月にベネッセの個人情報2070万件が流出した事件が該当しますし、また、ヤフー社にまつわる事件となると、2004年にYahoo! BB登録者情報約450万件が流出したものもあり、これも内部関係者が関わったものでした。

- こういった情報の持ち出しが容易に行われないよう、自社社員から委託業者に至るまでのあらゆる関係者に対するモラル教育、そして、システム・ネットワーク構成の確認・UTMの導入等の見直し、これら両面からの対策が改めて問われることとなるでしょう。

●プリンタ用インク通販サイト等からのべ6,447件のクレジットカード情報、不正アクセスにより流出

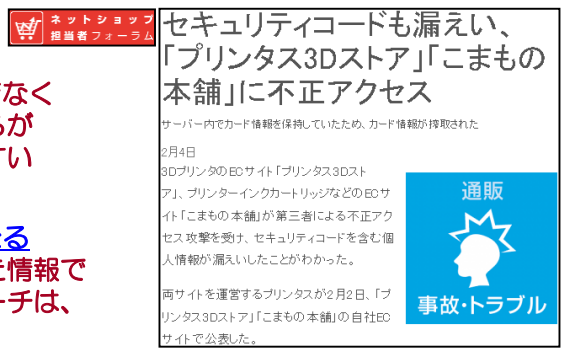
https://netshop.impress.co.jp/node/2597

このニュースをザックリ言うと・・・

- 2月2日（日本時間）、プリンタ用インク通販サイト「こまもの本舗」を運営するプリンタス社は、同サイトが不正アクセスを受け、ユーザのべ6,447人分の個人情報が流出した可能性があると発表しました。

- 流出の可能性があるのは、「こまもの本舗」の2010年4～10月注文分5件と、2015年8～12月注文分6,427件、および同社の3Dプリンタ通販サイト「プリンタス3Dストア」で2015年8～11月にクレジットカードで買い物をした15件で、カード名義人名・カード番号と有効期限・セキュリティコードおよびメールアドレスが含まれているとのことです。

- 同社では再発防止策として、今後はカード情報を自社で保有しない形式に移行する計画としています。


ネットショップ担当者フォーラム

セキュリティコードも漏えい、「プリンタス3Dストア」「こまもの本舗」に不正アクセス

サーバー内でカード情報を保持していたため、カード情報が搾取された

2月4日

3Dプリンタの ECサイト「プリンタス3Dストア」、プリンターインクカートリッジなどの ECサイト「こまもの本舗」が第三者による不正アクセス 攻撃を受け、セキュリティコードを含む個人情報が漏えいしたことがわかった。

両サイトを運営するプリンタスが2月2日、「プリンタス3Dストア」「こまもの本舗」の自社ECサイトで公表した。

通販 事故・トラブル

AUS便りからの所感等

- 多くの通販サイトは、クレジットカードの番号・有効期限だけでなくセキュリティコードもチェックするようになっていますが、これらが一緒に保存され、流出したことにより、攻撃者にとって悪用しやすい状況が発生していたと言えます。

- 同社が今後とる予定の再発防止策のように「流出したら問題になるような情報を自前で持たない」さらには一旦入力を求めて保存した情報であっても改修などで「不要になり次第破棄する」といったアプローチは、セキュリティ面で非常に有効なものとなるでしょう。

- システムの仕様上などの理由から、どうしても保存していなければならない情報は何かを十分に把握した上で、万が一外部からの攻撃や内部でのマルウェア感染が成功した場合でも流出を避けられるよう、UTM等を有効に活用したシステム・ネットワーク構成にすることを推奨します。