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。

●縮小表示プレビューに偽装したアイコンをもつマルウエア、JPCERTが警告

https://www.jpcert.or.jp/magazine/acreport-thumbnailicon.html
http://news.mynavi.jp/news/2015/03/20/163/

このニュースをザックリ言うと・・・

- 3月19日（日本時間）、一般社団法人JPCERT/CCが新たなアイコンの偽装方法を用いたマルウェアについて警告しています。

- これまでにも、有名なソフトウェア等のアイコンによって偽装したマルウェアは出回っていましたが、今回確認されたのは、Windows Vistaから採用された「縮小表示プレビュー」での表示に偽装し、PDFファイルであることを表す偽のオーバーレイ表示も右下に付加されているものでした。

- JPCERT/CCでは、ファイルのプロパティにより、ファイルの種類やそこに表示されるアイコン（縮小表示プレビューされた画像はここでは表示されないため、もしそのような画像が表示された場合はマルウェアの可能性があります）が不審なものでないか確認することと、「フォルダーオプション」において縮小表示プレビューに関する設定を変更することを推奨しています。

AUS便りからの所感等

- 前述したものの他に、当便りから強く推奨したい対策としては、「登録されている拡張子は表示しない」を無効にすることや、エクスプローラーにおいてファイルの種類を一目で確認できるよう「詳細」「並べて表示」「コンテンツ」のいずれかの表示形式を指定することが挙げられます。

- 「誤ってマルウェアをダブルクリックしてしまわない」ことが何よりも重要ですが、そういったミスが発生する前に、マルウェアが手元に届いてしまうことを防ぐため、アンチウイルス・UTM等による防御を固めることも大事でしょう。


縮小表示プレビューに偽装したアイコンをもつマルウエア（2015-03-19）

最終更新: 2015-03-19

ツイート　メール

分析センターだより目次

縮小表示プレビューに偽装したアイコンをもつマルウエア

メールに添付されるマルウエアには、脆弱性を悪用する文書ファイルもありますが、それよりも実行ファイルもしくはその圧縮ファイルが今日では主流になっています。JPCERT/CCでも、実行ファイル形式のマルウエアをユーザが自ら実行することでマルウエアに感染した事例を確認しています。

一見して不審に見える実行形式の添付ファイルをわざわざ開いて実行してくれるほど無防備なユーザは数が限られるため、マルウエアに感染させるためには、多くの場合、添付ファイルを無害なファイルに偽装して、ユーザにファイルを開かせる手法が用いられます。その代表的な手法として、アイコンを一見無害に見える他のアイコンに偽装する方法があります。これまでの偽装は、図1のようなアプリケーションごとに定義されたアイコンによって行われてきましたが、セキュリティ教育を受けたユーザを欺くことが難しくなりつつあります。

図1: アイコンを偽装したマルウエアの例

【正しい表示の例】縮小表示プレビューが表示されている画像ファイル(左)とPowerPointプレゼンテーション(右)

オーバーレイ表示されるイラストまで含んで偽装したマルウエア

●昨年（2014年/平成26年）のサイバー犯罪相談11万8,100件、不正アクセス被害3,545件。いずれも過去最高

http://www.npa.go.jp/pressrelease/2015/03/20150312_03.html
http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000090.html

このニュースをザックリ言うと・・・

- 3月12日（日本時間、以下同様）、警察庁が「平成26年中のサイバー空間をめぐる脅威の情勢」についての発表をしました。

- 発表では、2014年サイバー犯罪等に関する相談件数は11万8,100件に上り、過去最高とされた2013年の同件数を33,237件上回るものでした。

- また、3月19日に警察庁・総務省・経済産業省が合同で行った不正アクセス行為の発生状況等の発表では、2014年に報告された不正アクセス被害が3,545件で、こちらも過去最高とされた2013年を594件上回りました。

AUS便りからの所感等

- 不正行為に関する件数が増加の一途をたどること以外にも、特に3月12日の発表からは、攻撃の手法にも流行り廃りがあること等を窺い知ることができ、「昨日までのセキュリティに関する常識が通用しなくなる」こともあながち大げさなこととは言えなくなってきています。

- 自分たちのPCとネットワークを守るには、各ユーザが日々のセキュリティ界隈の流行に少しでも敏感であり続けることが重要であり、一方でアンチウイルスやUTMをはじめとするセキュリティプロダクトについても新たな攻撃に対応し続けていくことにより、ユーザの努力のみでは限界があるところを十分に補ってくれることでしょう。

●Java7のサポート、4月で終了。Java8へのアップデートをIPAが呼びかけ

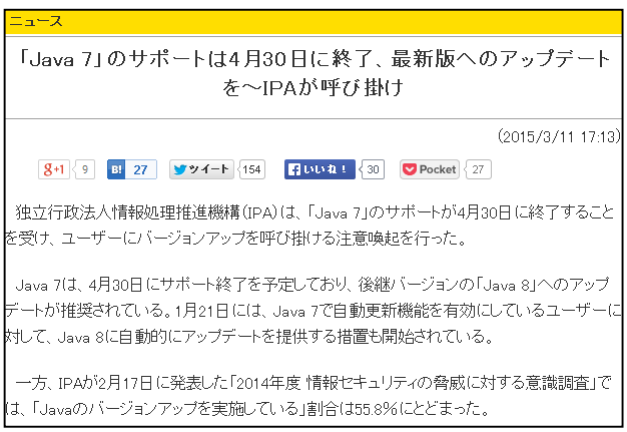
http://internet.watch.impress.co.jp/docs/news/20150311_692292.html
http://www.ipa.go.jp/about/press/20150311.html

このニュースをザックリ言うと・・・

- 4月をもってJava SE 7（Java7）のサポートが終了することを受け、独立行政法人情報処理推進機構（IPA）は3月11日（日本時間）、Java8へのバージョンアップを行うよう注意喚起を行いました。

- 注意喚起によれば、2月17日に発表した「2014年度 情報セキュリティの脅威に対する意識調査」において、Javaのアップデートを実施しているユーザが55.3%に留まっており、また2014年に発表されたJava7の脆弱性111件のうち、「危険」と判断されたものが全体の43%にあたる48件であったとされています。

- 3月4日にリリースされたJava 8 Update 40が現時点での最新バージョンであり、IPAではこのバージョンへのアップデートを強く推奨しています。


ニュース

「Java 7」のサポートは4月30日に終了、最新版へのアップデートを～IPAが呼び掛け

(2015/3/11 17:13)

g+1 9 B! 27 ツイート 154 いいね！ 30 Pocket 27

独立行政法人情報処理推進機構（IPA）は、「Java 7」のサポートが4月30日に終了することを受け、ユーザーにバージョンアップを呼び掛ける注意喚起を行った。

Java 7は、4月30日にサポート終了を予定しており、後継バージョンの「Java 8」へのアップデートが推奨されている。1月21日には、Java 7で自動更新機能を有効にしているユーザーに対して、Java 8に自動的にアップデートを提供する措置も開始されている。

一方、IPAが2月17日に発表した「2014年度 情報セキュリティの脅威に対する意識調査」では、「Javaのバージョンアップを実施している」割合は55.8%にとどまった。

AUS便りからの所感等

- Java8が必ずしも全ての場面でJava7より安全というわけではなく、Java8にのみ存在する脆弱性もあることに注意が必要ですが（これはWindowsにも当てはまることですが）、いずれにしても、サポートされているバージョンにおける最新のパッチ適用がPCを安全に保つために常に必要となります。

- さらには、アップデートまでのタイムラグの間に脆弱性を突く攻撃を受ける可能性を抑制するため、アンチウイルスやUTM等による防御も欠かせません。