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。

●メールを使ったサイバー攻撃、99%は「脆弱性を悪用しない」

http://itpro.nikkeibp.co.jp/atcl/news/15/030500815/
http://www-935.ibm.com/services/jp/ja/it-services/soc-report-2014-h2.html

このニュースをザックリ言うと・・・

- 3月5日（日本時間）、日本IBMが2014年7月～12月の国内サイバー攻撃の動向をまとめた「2014年下半期Tokyo SOC情報分析レポート」を公表しています。

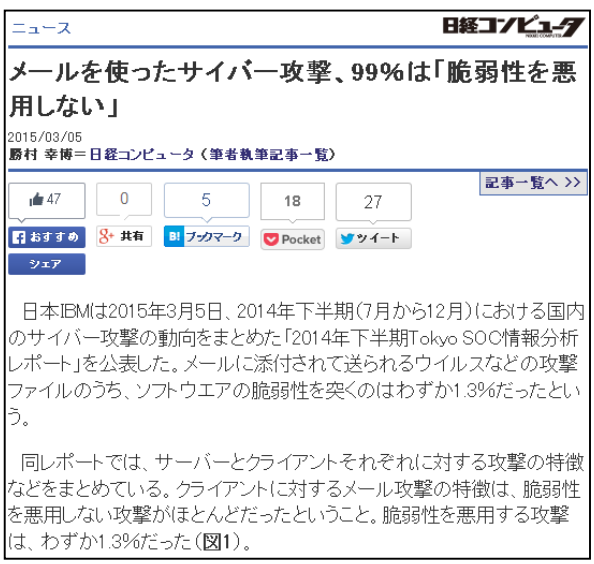
- クライアントに対し不正なメールを送りつける攻撃において、古いAdobe Reader等の脆弱性を悪用するケースは1.3%に留まり、それ以外では38.8%が悪質なマクロを含むOfficeファイル等、残る59.9%がzip形式等で圧縮された実行形式ファイルによるものだったとのことです。

- 脆弱性を悪用しないメール攻撃が多い理由として同レポートでは、「メールの添付ファイルを利用する攻撃では、脆弱性悪用の有無にかかわらず、ユーザにファイルを開かせる必要がある。脆弱性を悪用する場合でも、悪用しない場合と同様に、ユーザーをだましてファイルを開かせる必要がある。それなら、実行形式ファイルやマクロを含むファイルを使っても同じだと攻撃者は判断している」とされています。

AUS便りからの所感等

- 脆弱性を悪用するような込み入った手順をとらなくても、わざわざzipファイルを解凍して不審なexeファイルを実行したり、普段無効にしているマクロ機能を有効にしてからOfficeファイルを開いたり等して、みすみすマルウェアに感染してしまうようなターゲットユーザが依然多い、と攻撃者たちはみているものと思われます。

- ともあれ、いずれの攻撃パターンに対してもその存在を意識し、PC上のソフトウェアを最新に保ち、アンチウイルスやUTM等による防御を確実に行うことは欠かせないでしょう。


ニュース　日経コンピュータ

メールを使ったサイバー攻撃、99%は「脆弱性を悪用しない」

2015/03/05
勝村 幸博＝日経コンピュータ（筆者執筆記事一覧）

記事一覧へ >>

47　0　5　18　27
おすすめ　共有　ブックマーク　Pocket　ツイート
シェア

日本IBMは2015年3月5日、2014年下半期（7月から12月）における国内のサイバー攻撃の動向をまとめた「2014年下半期Tokyo SOC情報分析レポート」を公表した。メールに添付されて送られるウイルスなどの攻撃ファイルのうち、ソフトウエアの脆弱性を突くのはわずか1.3%だったという。

同レポートでは、サーバーとクライアントそれぞれに対する攻撃の特徴などをまとめている。クライアントに対するメール攻撃の特徴は、脆弱性を悪用しない攻撃がほとんどだったということ。脆弱性を悪用する攻撃は、わずか1.3%だった（図1）。

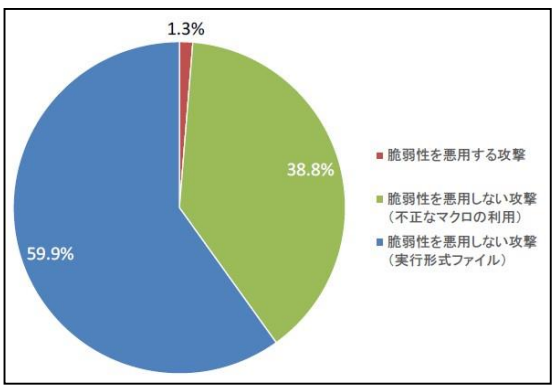


図1●脆弱性を悪用する攻撃と脆弱性を悪用しない攻撃の割合（日本IBM「2014年下半期Tokyo SOC情報分析レポート」から引用）


IBM　ソリューション　サービス　製品　サポート & ダウンロード　My IBM

ITサービス > セキュリティー・サービス >

2014年下半期 Tokyo SOC 情報分析レポート 公開

「2014年下半期 Tokyo SOC 情報分析レポート」を公開しました。

「Tokyo SOC 情報分析レポート」とは？

本レポートは、IBMが世界10拠点のセキュリティー・オペレーション・センター（SOC）にて観測した2014年下半期（7月～12月）のセキュリティー・イベント情報に基づき、主として日本国内の企業環境に影響を与える脅威の動向を、Tokyo SOCが独自に分析し、まとめたものです。

●フィッシング報告件数、1月に2000件越す

https://www.antiphishing.jp/report/monthly/201501.html
https://www.antiphishing.jp/report/monthly/201502.html

このニュースをザックリ言うと・・・

- フィッシング詐欺に関する調査・啓発を行っているフィッシング対策協議会が2月2日（日本時間、以下同様）に1月度の、3月2日に2月度のフィッシング報告状況に関する月次報告書を発表しています。

- 2014年10月の648件から12月の503件へと減少傾向にあった月間のフィッシング報告件数は1月に4倍以上の2156件に増加しましたが、2月は498件とそれまでの水準に戻っています。

AUS便りからの所感等

- 1月のみ報告件数が突出した理由は特に説明されていませんが、楽天の偽サイトが2月に多数確認されたという情報があるなど、今後もある程度の波が起こり得るもので、油断は禁物でしょう。

- 必要以上に一喜一憂するのではなく、常日頃からフィッシングに引っ掛からないための様々な行動（※）をとることが肝心です。

（※）普段利用するサイトにはブラウザのブックマークからアクセスする、ブラウザやアンチウイルス・UTMのアンチフィッシング機能を有効利用する等

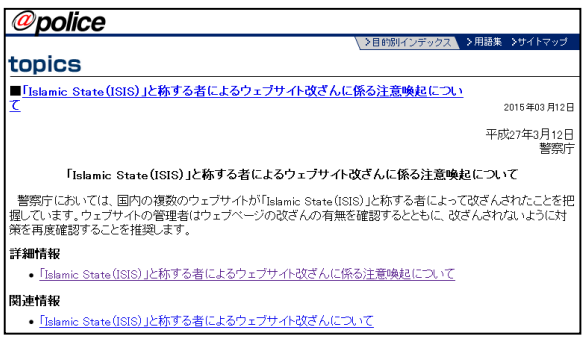
●ISISを称する者によるWebサイト改ざんが続発、WordPressプラグインの脆弱性を悪用か

http://www.npa.go.jp/cyberpolice/topics/?seq=15671

このニュースをザックリ言うと・・・

- 3月12日（日本時間）、警察庁より、国内複数のWebサイトが「Islamic State(ISIS)」を称する攻撃者によって改ざんされる事件が続発していると発表されました。

- 被害にあったWebサイトのいくつかでブログツール「WordPress」が使用されており、また2月には当該ツールにおいて複数のプラグインにおいて脆弱性が確認されていたことから、改ざんにあたってこれらの脆弱性が悪用された可能性が指摘されています。



AUS便りからの所感等

- 今回の改ざんがISIS自身によるものか、便乗した無関係の攻撃者によるものかは不明ですが、インターネット上では、メディアやネット上で騒がれる時事問題に便乗するサイバー攻撃が絶え間なく発生しており、いつどこの組織や個人がWebサイト改ざん等の被害を受けるか、到底予測できるものではありません。

- 警察庁も呼びかけるように、ブログツールをはじめとするCMS（コンテンツ管理システム）からサーバにアクセスするための各種ソフトウェアに至るまで常日頃から脆弱性についての情報をチェックし随時安全なバージョンに保つこと、同時にサーバにログインするアカウントの管理を適切に行うこと等が必要不可欠です。

- また、Webサイトを閲覧する側についても、改ざんされたWebサイトへのアクセスにより何らかのマルウェアを仕込まれる可能性があるため、こちらもブラウザや各種ソフトウェアを最新に保ち、アンチウイルスやUTMも含めた多重の防御策をとることが重要です。