— AUS（アルテミス・ユーザ・サポート）便り 2017/02/06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。

●Web経由の攻撃、いまだ危険な「見ただけで感染するサイト」

http://www.is702.jp/news/2097/
http://blog.trendmicro.co.jp/archives/14420

このニュースをザックリ言うと・・・

- 2月2日（日本時間）、大手セキュリティベンダーのトレンドマイクロ社より、「正規サイトを見ただけで感染する」攻撃が継続して発生しているとして同社ブログで警告が出されています。

- 同社によれば、2016年はマルウェアが添付されたスパムメールの拡散が全世界的に拡大していたとのことですが、一方で、脆弱性攻撃ツール「エクスプロイトキット」を使用した「脆弱性攻撃サイト」（「EKサイト」とも呼ばれています）によるWeb経由の攻撃が見過ごされがちになっていたと指摘しています。

- 2016年下半期（7～12月）に確認された脆弱性攻撃サイトの数は、1172件（7月）、1387件（8月）、955件（9月）、1235件（10月）、636件（11月）、550件（12月）と推移、依然少なからず存在はする一方で、10～12月は減少の方向とのことです。

AUS便りからの所感等

- 8→9月に件数が落ち込み、9→10月に再度上昇しているのは、使用されているエクスプロイトキットの移り変わりによるものとのことで、また新たなエクスプロイトキットが登場すれば、再度上昇に転じることも考えられます。

- その名のとおり、「脆弱性攻撃サイト」が攻撃するのはOSやアプリの脆弱性であり、多くはパッチが提供済みですので、利用される脆弱性がすべてアップデートにより解消されてさえいれば、「脆弱性攻撃サイト」に誘導されたとしても自動的に感染することはありません。

- 同社記事においても、ブラウザやFlash Player・Java等、インターネット利用時に使用される製品のアップデートを欠かさず行うよう呼びかけていますが、根本的な対策として、アンチウイルスやUTMによる防御以上に重要なことと言えるでしょう。

TREND MICRO | is702

ニュース

Web経由の攻撃、いまだ危険な「見ただけで感染するサイト」

2017/02/03

トレンドマイクロは2月2日、公式ブログで「『見ただけで感染』する脆弱性攻撃サイトの国内状況」と題する記事を公開しました。

従来より、不正広告や正規サイト改ざんなどにより、正規サイト利用者を不正サイトへ誘導し、マルウェア（不正プログラム、ウイルス）などに感染させる手法が存在します。こうした不正サイトは、「エクスプロイトキット」（脆弱性攻撃ツール）を使用していることから「EKサイト」（脆弱性攻撃サイト）などと呼ばれています。EKサイトの攻撃は、たくみに脆弱性を利用しており、「サイトを見ただけで感染」する攻撃を実現しています。

トレンドマイクロの監視によると、2016年下半期（7～12月）に日本からアクセスされたEKサイトは、のべ6,000件近くですが、少しずつ減少傾向を見せています。これは、EKサイト構築に利用される脆弱性攻撃ツール「Angler EK」「Neutrino EK」の2種が、活動停止した影響とのこと。現在、国内から誘導されるEKサイトは「Rig EK」を使用したものがほとんどとなっています。

また、拡散される不正プログラムについては、ランサムウェア（身代金要求型ウイルス）が主流で、10月以降にEKサイトから拡散された不正プログラムは、ランサムウェアが85%を占有していました。一方、マルウェアスパム（ウイルス付迷惑メール）で大きな量を占めているオンライン銀行詐欺ツール（ネットバンキングを狙うウイルス）は、全体の1.9%に過ぎませんでした。またランサムウェアにも偏りがあり、「CERBER」が9割以上を占め、「LOCKY」はほとんど見られませんでした。

こうした特徴の違いから、トレンドマイクロでは「Web経由とメール経由では背後にいるサイバー犯罪者が異なる」と推測しています。それぞれの攻撃手法にあわせ、個別の注意と対策が必要といえるでしょう。EKサイトに対しては、ブラウザ、Adobe Flash Player、Javaなどの定期的なアップデートが必須です。不正サイトへのアクセスを自動ブロックするWeb対策製品も有効でしょう。

TREND MICRO トレンドマイクロ セキュリティブログ

「見ただけで感染」する脆弱性攻撃サイトの国内状況

投稿日: 2017年2月2日
脅威カテゴリ: 不正プログラム、脆弱性、Webからの脅威、日本発、攻撃手法
執筆: セキュリティエバンジェリスト 岡本 勝之

「正規サイトを見ただけで感染する」攻撃が継続して発生しています。このエクスプロイトキットと呼ばれる脆弱性攻撃ツールを使用した脆弱性攻撃サイト（EKサイト）に国内のインターネット利用者を誘導する攻撃手法について、トレンドマイクロでは継続した監視を行っています。今回は、不正広告や正規サイト改ざんなどの手法で正規サイト利用者を EKサイトへ誘導して感染させる、まさに「正規サイトを見ただけで感染する」攻撃手口の、国内での現状をお伝えします。

■「見ただけで感染する攻撃」国内での現状

しかし、EKサイトへ誘導する攻撃がすべて停止してしまったわけではありません。9月の「Neutrino EK」の活動停止以後、日本から誘導される EKサイトは「Rig EK(リグ)」の独占状態となっています。現在、国内で EKサイトの脆弱性攻撃によって拡散される不正プログラムについては、ランサムウェアが主流です。「Rig EK」の独占状態となった 10月以降に EKサイトから拡散された不正プログラムのうち、ランサムウェアが 85%を占めていました。

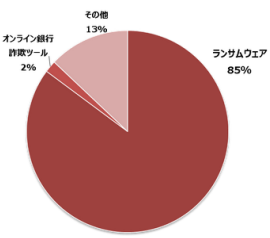

図2:国内からアクセス誘導された EKサイトから拡散された不正プログラムの種別割合
（2016年10~12月トレンドマイクロ調べ）

●マイクロソフト・Amazon・PayPalをかたるフィッシングを確認

https://www.antiphishing.jp/news/

このニュースをザックリ言うと･･･

- フィッシング対策協議会より、大手企業をかたるフィッシングについて、相次いで警告が出されています。

- 1月31日（日本時間）に出された、マイクロソフトをかたるフィッシングの警告では「OFFICEのプロダクトキーが不正コピーされています」という件名で、偽のライセンス認証サイトへ誘導する手口をとっています。

- 同じく1月31日にはAmazonについて、また2月3日にもPayPalについて、それぞれをかたるフィッシングについて警告が出されていますが、いずれも「あなたはAMAZON（あるいはPaypal）ログイン認証情報をリセットする必要があります」という件名で、個人情報やクレジットカード情報を入力させようとする偽サイトに誘導する手口とみられます。

- 同協議会では、このようなフィッシングサイトにて「アカウント情報（ID・パスワード等）」「個人情報（氏名・生年月日・住所・郵便番号・電話番号等）」および「クレジットカード情報（番号・有効期限・セキュリティコード等）」を絶対に入力しないよう呼びかけています。

AUS便りからの所感等

- AmazonとPayPalのフィッシングはメールの文面が全く同じで同一の犯行組織によるとみられていますが、日本語が洗練されたものとなっており（マイクロソフトのフィッシングはまだ一部違和感を感じるものですが、それもすぐに修正されるでしょう）、そこから人間がフィッシングと判断するのは困難になってくるでしょう。

- メールが不審なものか否かの判断のため、ブラウザやアンチウイルスあるいはUTMのアンチフィッシング機能を有効にして分析を行うことが重要であり、利用している正規のサイトのURLをブラウザのブックマークに登録し、そこからサイトにアクセスを行うことも自衛のために有用でしょう。

●偽のランサムウェアで脅して身代金を要求、被害の実態は？

https://japan.zdnet.com/article/35095582/

このニュースをザックリ言うと･･･

- 1月24日（米国時間）、シンクライアント商品などを手がける米Citrix社より、昨年11月にイギリスの企業に対し行った「ランサムウェアへの感染」に関する調査結果が発表されました。

- 調査によれば、イギリスの大企業の2/5について、実際には被害者を感染させないまま、標的となった企業にネットワークがロックされたと思い込ませる「偽のランサムウェア」による攻撃を受けたとされています。

- さらにそのうち2/3弱については、実際に脅迫者に対し身代金を支払っていたとのことで、身代金の額は平均13,412ポンド（約188万円）、さらには25,000ポンド（約352万円）を超える額を支払った企業もあるとされています。

AUS便りからの所感等

- 2015～2016年に新しい脅威として注目されるようになった「ランサムウェア」ですが、話題に便乗してか、ファイルを暗号化せず単に削除するだけのランサムウェアもどきも発生しています（AUS便り 2016/07/19号参照）。

- 今回の「偽のランサムウェア」は、以前よりあった、セキュリティソフト等をかたって金銭等を詐取しようとする「スケアウェア」の一種とみることもできますが、ランサムウェアの脅威が大きく取り上げられたことにより、企業等も過度に敏感になった結果、実際にランサムウェアでないものでも成果が挙げられるようになったということでしょう。

- アンチウイルスやUTMによる防御で「本物の」マルウェア・ランサムウェア等からの防御を十分に固めるのはもちろん、こういったニュースにも目を向け、慎重に行動できるようになることがよりセキュリティやリテラシーを高めることにつながるでしょう。