― AUS（アルテミス・ユーザ・サポート）便り 2015/10/13号 ―

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。

●日本のユーザを狙うマルウェア入り広告、約3,000の大手サイト・50万ユーザに影響か

http://www.itmedia.co.jp/enterprise/articles/1510/01/news106.html
http://blog.trendmicro.co.jp/archives/12293

このニュースをザックリ言うと･･･

- 10月1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、特に日本のユーザを狙って配信されている、マルウェアへの感染を狙う不正な広告について警告が出されました。
- 同社の観測によれば、約3,000の正規のWebサイト上で不正な広告が表示され、サイトを訪問した50万のユーザにおいて、攻撃者が用意した悪意のあるサイトに誘導されたとみられています。
- マルウェアが悪用した脆弱性としては、7月にパッチ「MS15-065」で修正されたIEの脆弱性（CVE-2015-2419）や、8月に修正されたFlash Playerの脆弱性（CVE-2015-5560）が挙げられています。

AUS便りからの所感等

- 今回の攻撃については、幸いにも既に修正パッチがリリースされている脆弱性に対するものであり、それに対する根本的な対策としては、やはり修正パッチを速やかに適用することです。
- 一方で、いわゆるゼロデイ攻撃（※）の脆弱性を突かれるケースも決して珍しくはなく、アンチウイルスやUTMの導入は、パッチの適用と併せていずれも欠かせない防御策となります。

ITmedia エンタープライズ

2015年10月01日 14時22分 更新

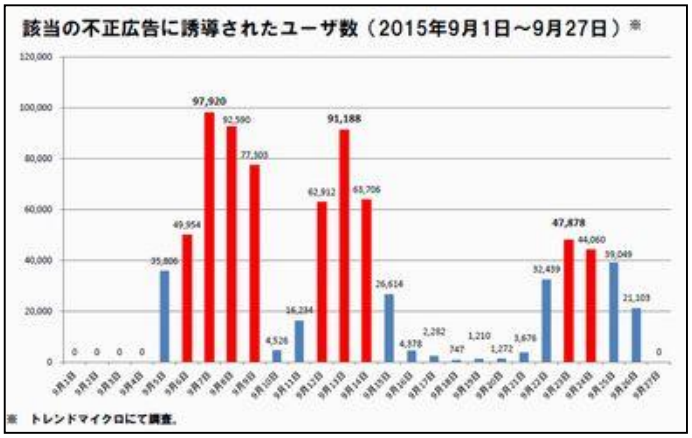
国内3000サイトに不正広告、50万人にウイルス感染の危機

9月に閲覧者のコンピュータの脆弱性を突いて不正プログラムに感染させる攻撃が発生していた。

[ITmedia]

トレンドマイクロは10月1日、Webサイトに表示される広告を悪用して閲覧者のコンピュータを不正プログラムに感染させる大規模なサイバー攻撃が国内で発生したことを明らかにした。不正な広告は約3000サイトで表示され、約50万人に影響した可能性があるという。

同社によると、この攻撃では地方の観光協会やオンラインショップが使用した広告バナーの画像を何者かが悪用し、閲覧者を不正プログラムの感染サイトに誘導する仕掛けを行って、広告配信ネットワーク経由で展開したとみられる。広告配信ネットワーク経由で約3000サイトに不正な広告が表示され、閲覧者のコンピュータに存在するソフトウェアの脆弱性を突いて、不正プログラムに感染させる手口だった。



TREND MICRO トレンドマイクロ セキュリティブログ

不正広告が約3,000 の国内大手サイトを汚染、50万ユーザに影響

投稿日: 2015年10月1日
脅威カテゴリ: 不正プログラム，サイバー犯罪，脆弱性，TrendLabs Report，Webからの脅威
執筆: Fraud Researcher - Joseph C Chen

トレンドマイクロは、2015年9月、日本のユーザを対象にした「malvertisement（不正広告）」攻撃を確認しました。攻撃者は、不正広告と脆弱性攻撃のためのエクスプロイトキットを併用し、広告が表示された正規サイトを訪問したユーザに効果的に攻撃を実行しました。

トレンドマイクロの観測では、不正広告はおよそ 3,000 の正規サイトで表示され、それらのサイトへ約 50万人のユーザが訪問しました。ユーザは脆弱性攻撃ツールである「Angler Exploit Kit（Angler EK）」を利用した攻撃サイトへ誘導されました。確認された不正広告はすべて日本語の広告であり、この攻撃は特に日本のユーザを狙って実行されたものと言えます。これらの不正広告が正規の広告と絶対に区別できないように、攻撃者は正規の広告で使用されたバナーを不正広告の画像に利用しました。

IT用語辞典 e-Words

（※）ゼロデイアタック【 zero-day attack 】ゼロデイ攻撃 / 0-day attack

ゼロデイアタックとは、ソフトウェアにセキュリティ上の脆弱性（セキュリティホール）が発見されたときに、問題の存在自体が広く公表される前にその脆弱性を悪用して行われる攻撃。

コンピュータシステムを外部からの攻撃から守るには、メーカーや開発者が公開するパッチを、公開後即座に適用するのが基本だが、ゼロデイアタックの場合は対応策が公表される前に攻撃が行われるため、このような対策では防ぎきれない。

実際、開発者が対応を取る前に、発見された脆弱性の情報がクラッカーコミュニティで流通したり、攻撃用ツールが配布されたりする事例が報告されており、この「時間差」が問題となっている。

攻撃に使用されるパケットの特徴を分析し、発見されていない脆弱性を利用した攻撃を認識して遮断するソフトウェアの研究も行われているが、有効で万能な解決策は今のところない。

●「著名人の名前+無料mp4」検索でマルウェア感染サイトへ誘導の恐れ･･･マカフィー

http://ascii.jp/elem/000/001/061/1061608/

このニュースをザックリ言うと･･･

- 10月1日（日本時間）、大手セキュリティベンダーのインテル セキュリティ（日本での事業会社：マカフィー株式会社）から、2015年版「インターネット検索で最もリスクの高い有名人」の調査結果が発表され、有名人の名前を含むキーワードの検索における危険性について警告しています。

- 同社は、攻撃者がさまざまな賞の授賞式・TV番組・新作映画・音楽アルバムのリリースあるいは有名人カップルの破局といった有名人にまつわるイベントへの関心を悪用し、ユーザをマルウェアを潜ませたサイトに誘い込んで個人情報を盗む、と説明しています。

- 今回の調査では、音楽の無料ダウンロードやミュージックビデオの検索、特に「有名人の名前+無料mp4」「有名人の名前+HDダウンロード」「有名人の名前+Torrent(P2Pソフトウェア)」といったキーワードでの検索が攻撃者に狙われるリスクが特に高いことが判明したとのことです。

- 同社では、こういった検索を安全に行う注意点として、「外部リンクのクリックには慎重になる、コンテンツのダウンロードは公式サイトなどから行う」「疑わしいサイトから動画をダウンロードしない」「『無料ダウンロード』は、ウイルスが最も好む検索用語であることに注意する」「不審なサイトにて、ログインしたり、その他の情報を入力したりしない」等を挙げています。

AUS便りからの所感等

- トップ10に出た有名人を含め発表された調査結果はアメリカのインターネットに関する調査とみられますが、日本を含めた世界各国のユーザが同様に狙われている可能性も皆無とは言えません。

- 万が一不審なサイトへの誘導や偽のファイルを開くことにより、マルウェアに感染してしまう可能性を抑止するためにも、ブラウザの機能と併せてアンチウイルス・UTMを有効活用することが重要です。

●Linuxルータ約10,000台に感染、セキュリティアップデートを行うマルウェア

http://gigazine.net/news/20151002-hacked-routers-secure/

このニュースをザックリ言うと･･･

- 10月1日（米国時間）、大手セキュリティベンダーのシマンテック社より、OSにLinuxを用いているルータ約10,000台に感染したとされるマルウェアについて、同社ブログにて紹介されました。

- 「Linux.Wifatch」と呼ばれるマルウェアは2014年に発見され、感染したルータ同士でP2Pネットワークを構成することが知られていましたが、同社が今年4月以降調査を行ったところ、悪意のある行動を取る様子はなく、むしろP2Pネットワークからルータのセキュリティアップデートを受け取る行動をとることが判明したとのことです。

- これが話題になった数日後には、マルウェアの作者を名乗るメンバーがソースコードを公開、さらに経済誌のインタビューにメールで応じ、あくまで勉強のため、理解のため、あるいは面白いから、そしてセキュリティ啓発のためにマルウェアを作成したこと等を語っています。

AUS便りからの所感等

- 悪意はないとは言え、マルウェアに不正に侵入されるような状況だったということは、攻撃者次第で、その気になればルータをDDoS攻撃のボット（※）に仕立て上げることも可能だった状況にあると言えます。

- 今回の出来事がPCと同様ルータやUTM等のあらゆる機器についても、確実にセキュリティアップデートの確認を行うよう注意をはらうきっかけとなれば幸いです。

IT用語辞典 e-Words

（※）ボット【 bot 】ロボット / robot

ボットとは、「ロボット」の略称で、もともと人間がコンピュータを操作して行っていたような処理を、人間に代わって自動的に実行するプログラムのこと。検索エンジンなどが導入している、Webページを自動的に収集する「クローラ」や、オンラインゲームでキャラクターを人間に代わって自動的に操作するプログラムなどのことを言う。

コンピュータウイルスの一種にもボットと呼ばれるプログラムがあり、感染したコンピュータを攻撃者が用意したネットワーク（IRCサーバなど）に接続して攻撃者からの指令を待ち、指令通りの処理を感染者のコンピュータ上で実行する。

他のウイルスと違い、感染者のコンピュータが攻撃者の意のままに動いてしまう点で悪質である。ボットに感染したコンピュータによって構成されたネットワークは「ボットネット」（bot net）と呼ばれ、攻撃者はボットネットに接続したコンピュータに対して一斉に同じ指令を与えることができるため、DDoS攻撃やスパム送信などに利用されることもある。