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。

●広告ブロックを回避する解析サービスが不正アクセス被害、ユーザページにてマルウェア感染の恐れ

http://gigazine.net/news/20151104-hackers-use-anti-adblocking-service/

このニュースをザックリ言うと・・・

- 11月1日（現地時間）、アドブロック等を使用しているウェブサイト閲覧者に対し、広告ブロック機能を回避する「邪魔にならない広告」を表示することによってアクセス解析を行うサービス「PageFair」が前日に不正アクセスを受けていたとして、サービスを提供するアイルランドPageFair社より発表がありました。

- 同社の発表では、標的型攻撃によって同サービスを配信するCDNのアカウントが乗っ取られ、サービスのユーザページが改ざんされたことにより、アクセスしたユーザがFlash Playerに偽装したマルウェア「Nanocore」をダウンロードさせるよう誘導されていたとのことです。

- 幸いにもNanocoreはアンチウイルスで検出される既知のものでしたが、誘導されたユーザの2～3%にあたる500人程度のユーザがこれをインストールして感染した模様です。

AUS便りからの所感等

- 被害を受けたPageFair社が8月に「広告のブロックによってメディア側に年間220億ドルの損失が生じる」とする調査結果を発表(※)し、一方では9月にリリースされたiPhoneのiOS9に広告ブロック機能が搭載される等、広告配信とそのブロック、さらにはその回避といったテーマがにわかに話題となってきており、今回の事件はある意味その延長線上に位置するものとみられます。

- 今回は以前他のケースでみられた不特定多数への不正な広告の配信はく、幸いにもマルウェアの拡散は限定的なものであり、攻撃者が大きな話題になることをあえて避けた可能性も考えられます。

- ともあれ、ユーザとしては普段利用しているサイトへのアクセスであっても、そのサイトやスクリプト等を配信する外部サイトの改ざんにより、不正なサイトに誘導される恐れがあることに常に注意し、アンチウイルスやUTM、およびブラウザのセキュリティ機能の活用による防御を怠りなく行う必要があるでしょう。

GIGAZINE

2015年11月04日 12時50分00秒

広告ブロック回避サービスがハッカーに乗っ取られてマルウェア配信

アドブロックを使用しているウェブサイト閲覧者に対し「邪魔にならない広告」を表示させ、ユーザーに無料でアナリティクスを提供するサービス「PageFair」がハッカーの攻撃に合い、ウェブサイトが乗っ取られ、いつものようにサービスを利用しようとしたユーザーをマルウェアの危険にさらす、という事態が発生しました。

Hackers use anti-adblocking service to deliver nasty malware attack | Ars Technica
http://arstechnica.com/security/2015/11/hackers-use-anti-adblocking-service-to-deliver-nasty-malware-attack/

Halloween RAT: NanoCore Served Via PageFair Service | News from the Lab
https://labsblog.f-secure.com/2015/11/02/halloween-rat-nanocore-served-via-pagefair-service/

Halloween Security Breach | Inside PageFair
http://blog.pagefair.com/2015/halloween-security-breach/

Forbes JAPAN

(※) http://forbesjapan.com/translation/post_7647.html

損失額は2兆円以上　メディアに死をもたらす「広告ブロック」ソフト

文 = レックス・サンクトゥス(Forbes)/ 編集＝上田裕資 | 翻訳記事

posted on 2015.08.15, at 08:30 am

成長を続けるオンラインメディアを横目に、密かに増殖を遂げているのが広告ブロックソフトウェアだ。

2015年には広告ブロックソフトの使用で、メディア側に220億ドル(約2兆7400億円)の損失が生まれると、アイルランドの企業PageFair社はリポートしている。今回の調査はアドビと共同で行われた。

報告によると、広告ブロックソフトは主にPC向けに世界で1億9800万人に利用されており、昨年は利用率が42%増加。特に米国では48%も増加しているという。

広告ブロックソフトはモバイルではまだ、さほどの存在感を示していないが、9月に登場するiOS9にはこの機能が実装されており、今後に大きな変化をもたらす可能性も指摘している。現状ではモバイル上の広告ブロックソフトの使用は全体の1.6%を占めるに過ぎないが、今後さらに多くのユーザーがこの手段を用いるようになるだろう。

「広告ブロックソフトはデスクトップのみならず、アジアでは既にモバイルに進出している。iOS上のコンテンツブロックが普及するにつれて、西側諸国でも同様な動きが進んでいくだろう」とPageFair社は述べている。

●Adobe、Shockwave Playerの脆弱性を修正

http://www.itmedia.co.jp/enterprise/articles/1510/28/news062.html

このニュースをザックリ言うと・・・

- 10月27日（米国時間）、Adobe Shockwave Playerのセキュリティアップデート12.2.1.171がリリースされ、1件の脆弱性が修正されました。

- この脆弱性を悪用された場合、攻撃者に任意のコードを実行され、システムを制御される恐れがあるとのことです。

- 同社では、攻撃発生の可能性が高いとして利用者に対し速やかにアップデートするよう呼びかけています。

AUS便りからの所感等

- 以前から広告やインタラクティブコンテンツで広く利用されているFlashと異なり、Shockwaveを用いるコンテンツは今日では少なく、Shockwave Playerがインストールされ ているPCの割合も2011年の時点で41%程度まで減少しています。

- もし、Shockwaveコンテンツを利用していないのにShockwave Playerがインストールされているのであれば、万が一にも悪用されないためにアンインストールするのが最も安全と思われ、また、自組織内で利用し続けているShockwaveコンテンツがある場合は、FlashやHTML5への移行も検討に値するでしょう。

- こういった対策がとれない場合は特に、アンチウイルスとUTMの導入が重要となってきます。

ITmedia エンタープライズ

2015年10月28日 06時41分 更新

Adobe、Shockwave Playerの脆弱性を修正

攻撃発生の可能性は高いとされ、Adobeではできるだけ早く更新するよう促している。

[鈴木聖子, ITmedia]

米Adobe Systemsは10月27日、Shockwave Playerの更新版を公開して1件の深刻な脆弱性に対処した。

同社のセキュリティ情報によると、更新版の「Shockwave Player12.2.1.171」ではメモリ破損の脆弱性を修正した。悪用された場合、攻撃者に任意のコードを実行され、システムを制御される恐れがある。

Adobe Security Bulletin

Security update available for Adobe Shockwave Player

Release date: October 27, 2015

Vulnerability identifier: APSB15-26

Priority: See table below

CVE number: CVE-2015-7649

Platform: Windows and Macintosh

Summary

Adobe has released a security update for Adobe Shockwave Player. This update addresses a critical vulnerability that could potentially allow an attacker to take control of the affected system.

Shockwave Playerのセキュリティアップデート

この問題はWindows版とMac版の両方が影響を受ける。攻撃発生の可能性は高いとされ、Adobeではできるだけ早く更新するよう促している。更新版は同社のダウンロードサイトから入手できる。

●ルータの管理画面に「クリックジャッキング」の脆弱性

http://internet.watch.impress.co.jp/docs/news/20151030_728285.html

このニュースをザックリ言うと・・・

- 10月30日（日本時間）、情報処理推進機構（IPA）とJPCERT/CCより、複数のメーカー製ルータのWeb管理画面に「クリックジャッキング」と呼ばれる脆弱性が存在することが発表されました。

- 管理画面にログイン済みのユーザが攻撃者によって用意されたWebページにアクセスし、ページ上の細工されたコンテンツをクリックすることにより、ユーザの権限で意図しない操作をルータ上で実行させられる可能性があります。

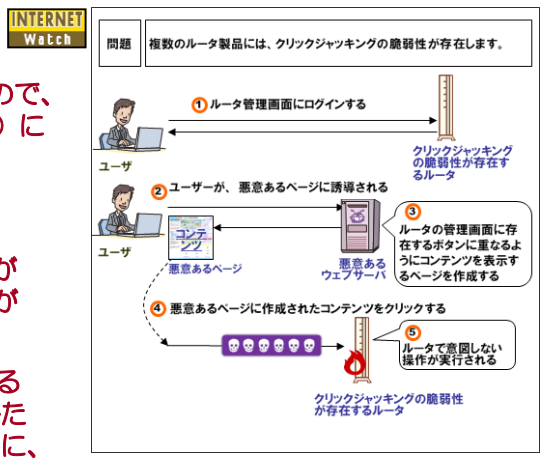
- 現時点で、「アライドテレシス」「ヤマハ」「NEC」「アイオーデータ」「バッファロー」の各社製ルータに脆弱性の存在が確認されており、一部メーカーはファームウェアの修正版をリリースしています。

AUS便りからの所感等

- クリックジャッキングは、2008年にその手法が周知にされたもので、あるページ「A」上において、透明なインラインフレーム（iframe）によって別のサイトのページ「B」を読み込み、そのページ「B」のリンクやボタンをクリックするよう誘導するという攻撃です。

- 技術的な対策として、ページB側がiframe上で表示されないよう申告する「X-Frame-Options」レスポンスヘッダを付与することが挙げられており、今回のファームウェアの修正においてもこの対策が行われていると見られます。

- クリックジャッキングはその他のWebサイトにおいても問題となる可能性があるため、現在の設定で危険ではないか？ あるいは前述した対策を既にとっているか？ について、他の項目も含め確認するために、Webアプリケーション診断を受けることが有用となるでしょう。



クリックジャッキングの脆弱性（JVN iPediaより画像転載）