— AUS（アルテミス・ユーザ・サポート）便り 2016/07/25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。

●偽サイト、ブラウザで警告･･･被害防止へ警察庁が情報提供

http://www.nikkei.com/article/DGXLASDG14H0Z_U6A710C1CR0000/
http://www.jiji.com/jc/article?k=2016071400211&g=soc
http://www.asahi.com/articles/ASJ7F5DP9J7FUTIL023.html

このニュースをザックリ言うと･･･

- 7月14日（日本時間）、警察庁は、正規のショッピングサイトを装った「偽サイト」のブラックリストを米国の非営利団体アンチ・フィッシング・ワーキング・グループ（APWG）に提供することを発表しました。

- データの提供は15日以降毎週行われ、APWGを通じて、各種Webブラウザのアンチフィッシング機能に登録されることになるとしており、同庁によれば、国内で使用されているブラウザの9割がこれに対応するとのことです。

- 同庁が6月末までに国内のアンチウイルスベンダーに通告した件数は30カ国2144件で、うち84.6%が米国に置かれたサーバを使用しているため、国内での捜査が難しいことから、米国の団体に情報提供を行ったと説明しており、またアンチウイルスソフトやフィルタリングソフトを利用しなくても、ブラウザの機能のみで偽サイトに関する警告が出るようになる、としています。

AUS便りからの所感等

- 警察庁が言うところの「アンチウイルスソフトが入っていない」環境は、恐らくPCよりもスマートフォンを想定しているものと推測され、フィッシングサイトに対する防御の効果的な底上げが期待されます。

- 一方で、スマートフォンにおいても、その他の脅威からの防御の意味も含めたPCと同様の多重防衛を行うためにも、モバイル向けアンチウイルスソフトの導入や、可能な限りUTMを通してのアクセスを推奨致します。

日本経済新聞

「偽サイト」、ブラウザーで警告　被害防止へ警察庁が情報提供
2016/7/14 10:20

保存 印刷 その他

警察庁は14日、通信販売サイトなどを装った悪質な「偽サイト」の被害を防ぐため、ブラウザー（閲覧ソフト）を提供する企業などが加盟する米国拠点の非営利団体に、海外サーバーに開設された偽サイト情報を提供すると発表した。

これにより、国内で使われているブラウザーの9割以上で、偽サイトにアクセスすると警告表示が出るようになる。

非営利団体は、フィッシング詐欺対策に取り組む「アンチ・フィッシング・ワーキング・グループ（APWG）」。米マイクロソフトなど民間企業や政府機関など2千を超える団体で構成され、サイバー犯罪対策に取り組んでいる。

警察庁は15日から偽サイトのURL情報の提供を始め、以後毎週、更新された情報を伝える。

偽サイトは海外にサーバーを置くケースが目立ち、国内での捜査が難しい。同庁が今年6月末までに国内のウイルス対策ソフト会社に通告した件数は30カ国2144件に上り、うち米国が84.6%と大半を占めた。

同庁によると、マイクロソフトのインターネット・エクスプローラーやグーグルのクローム、米モジラ財団のファイヤーフォックスなど、世界的にシェアされているブラウザーが対象になる。

日本通信販売協会（JADMA、東京・中央）によると、正規の通販サイトなどにそっくりな偽サイトを含む「詐欺的サイト」を巡る相談はピークの2013年度で3829件に上り、15年度は1048件だった。

同庁によると、マイクロソフトのインターネット・エクスプローラーやグーグルのクローム、米モジラ財団のファイヤーフォックスなど、世界的にシェアされているブラウザーが対象になる。

JIJI.COM

偽サイト、ブラウザーで警告＝国際団体通じ情報提供－警察庁

警察庁は１４日、正規のショッピングサイトを装った偽サイト対策として、国際団体を通じて加盟するブラウザー事業者に対し、海外サーバーに開設された偽サイトのブラックリストを提供すると発表した。利用者が偽サイトにアクセスするとブラウザーの画面に警告表示が出る仕組みで、国内で使われているブラウザーの９割超で対策が講じられる見込み。警察庁は「一層の被害抑止が可能になる」としている。

国際団体は、サイバー犯罪撲滅を目的として米国に設立された非営利の「フィッシング対策ワーキンググループ（ＡＰＷＧ）」。２０００以上の政府機関や企業・団体が加盟し、データ収集・分析、各国政府への助言を行っている。

日本国内で被害が出ている偽サイトは取り締まりを免れるため海外のサーバーに開設されるケースも多く、警察庁は２０１３年１２月から把握したＵＲＬ延べ約１万５０００件をネットセキュリティー会社などに提供してきた。

しかし、ウイルス対策ソフトを利用していなければ被害を防止できない恐れがあり、世界的ネットワークを持つＡＰＷＧと協定を締結。情報提供は１５日の約７００件を手始めに、週１回実施する。（2016/07/14-10:13）

朝日新聞 DIGITAL

詐欺を未然に防げ　警察庁、偽サイト情報をNPOに提供
2016年7月14日18時32分

偽のショッピングサイトや偽ブランド品を売るサイトなどの情報について、警察庁は2013年12月、ウイルス対策ソフトやフィルタリングの事業者に提供を始め、警告画面が表示される仕組みを整えた。今年6月末までに計約1万5千件の情報を提供した。今回新たにAPWGに情報提供することで、ウイルス対策ソフトやフィルタリングを導入していなくても、「インターネット・エクスプローラー」や「グーグル・クローム」など主要なブラウザーで、偽サイトなどの警告が出るようになるという。

●MMSを受け取るだけでiPhoneの各種認証情報・パスワードを抜き取れる脆弱性が明らかに

http://gigazine.net/news/20160720-ios-mms-vulnerability/

このニュースをザックリ言うと・・・

- 7月19日（現地時間）、米Ciscoのセキュリティ部門Talosより、iOSおよびOS Xの古いバージョンに存在する脆弱性について警告が発表されました。

- 脆弱性は特定の画像フォーマットの処理において存在し、MMS（マルチメディアメッセージングサービス）やiMessageおよびWebページに含まれる不正な画像を読み込むことにより、iOS端末上に保存されたパスワード等の認証情報が抜き取られる可能性があるとされています。

- Appleでは7月18日に脆弱性が修正された「iOS 9.3.3」「OS X 10.11.6」をリリースしており、アップデートが推奨されています。

AUS便りからの所感等

- 2015年7月にはAndroidでもやはりMMSの受信だけでデバイスを乗っ取られるような脆弱性が報告されています（AUS便り 2015/08/03号参照）が、Appleによれば、iOSやOS Xのセキュリティ機構により、デバイス全体を乗っ取られるような事態にはならないと説明しています。

- それでも保存されている認証情報の奪取は決して見過ごせない問題であり、アップデートは可能な限り速やかに、欠かさず行うべきものです。

- 今後も、iOSやOS XであってもWindowsと同様の脆弱性が発生する可能性に備え、それらに対応したアンチウイルスおよびUTMの導入による防御を意識しましょう。

●CGIを利用するWebサーバの脆弱性、中間者攻撃や不正なホストへの接続に悪用の恐れ

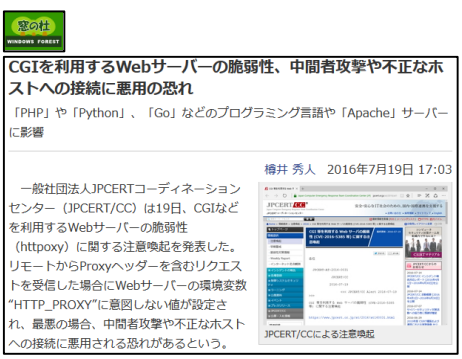
http://forest.watch.impress.co.jp/docs/news/1010961.html

このニュースをザックリ言うと・・・

- 7月19日（日本時間）、CGIやPHP等あるいはそれらが動作するWebサーバに脆弱性が存在することが報告されています。

- 「httpoxy」と名付けられたこの脆弱性は、Webアプリケーション側で特定の条件を満たしている場合、攻撃者が不正なリクエストヘッダを含むリクエストを送信することにより悪用が可能で、Webサーバを踏み台にして第三者ホストに接続される等の恐れがあるとされています。

- JPCERT/CC等が対策法等を含め警告を出している他、警察庁では、19日の時点でこの脆弱性の悪用が目的とみられるWebアクセスを確認していると発表しています。



AUS便りからの所感等

- httpoxyについて簡単に説明することは困難ですが、Webアプリケーション上から別の「WebサーバA」にアクセスする場面があるときに、攻撃者が不正なリクエストヘッダを送信した場合、Webアプリケーションがヘッダで指定された「サーバB」をプロキシサーバとみなして接続しようとする、というのが動作原理です。

- 結果として、Webアプリケーションが本来のアクセス先であるサーバAに送信しようとするリクエストが攻撃者が指定したサーバBを通過することになり、そこで機密情報等を奪取される恐れ、あるいはリクエストやレスポンスの改ざんといった、いわゆる「中間者攻撃」が発生する恐れもあります。

- 脆弱性を悪用する攻撃の検知はさほど難しくはなく、Webアプリケーションファイアウォール（WAF）あるいはその機能を持ったUTMをWebサーバの前面に設置することにより、これを含めた各種脆弱性に対する攻撃を遮断することを推奨致します。