添付資料

【今月の呼びかけ】

「 ウェブサイトを閲覧しただけでウイルスに感染させられる“ドライブ・バイ・ダウンロード”攻撃に注意しましょう! 」

2009 年から 2010 年にかけて猛威を振るったガンブラー※1 ではウェブサイトを閲覧しただけで、利用者のパソコンにウイルスを感染させられてしまう“ドライブ・バイ・ダウンロード（Drive-by Download）”攻撃の手法が使われていましたが、この手法を用いて国内の多数のウェブサイトに影響を及ぼした新たな攻撃が、2010 年 9 月と 10 月に相次いで発生しました。今後も様々な形で“ドライブ・バイ・ダウンロード”攻撃が行われると思われるため、引き続き注意が必要です。

ここでは、改めて“ドライブ・バイ・ダウンロード”攻撃について整理するとともに、ウェブサイト管理者、パソコン利用者の対策について解説します。

※1 「"ガンブラー" の手口を知り、対策を行いましょう」（IPA、2010 年 2 月の呼びかけ）
http://www.ipa.go.jp/security/txt/2010/02outline.html

（1）“ドライブ・バイ・ダウンロード”攻撃とは

“ドライブ・バイ・ダウンロード”攻撃とは、ウェブサイトを閲覧した際に、パソコン利用者の意図に関わらず、ウイルスなどの不正プログラムをパソコンにダウンロードさせる攻撃のことをいいます。“ドライブ・バイ・ダウンロード”攻撃では、主に利用者のパソコンの OS やアプリケーションなどの脆弱性が悪用されます。

攻撃の主な流れについて図 1-1 を例に説明します。

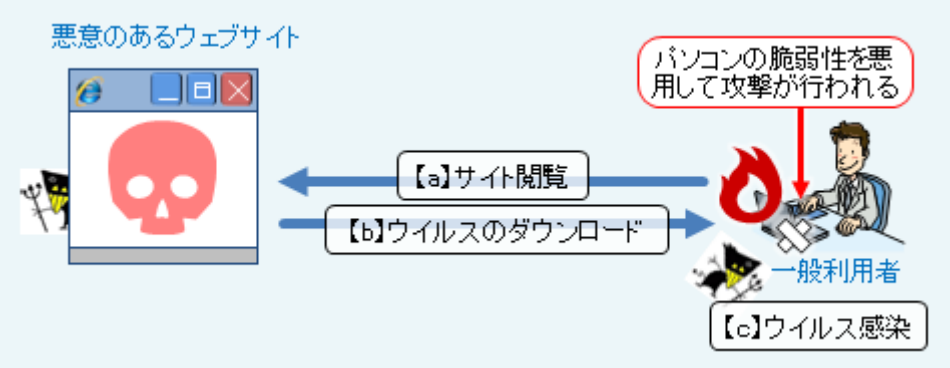

図 1-1：”ドライブ・バイ・ダウンロード”攻撃のイメージ

- パソコン利用者が悪意あるウェブサイトを閲覧する（図中【a】）。
- 利用者のパソコンの脆弱性を突かれて、ウイルスをダウンロードさせられる（図中【b】）。
- 利用者のパソコンにウイルスを感染させられる（図中【c】）。

（2）最近の“ドライブ・バイ・ダウンロード”攻撃の事例について

“ドライブ・バイ・ダウンロード”攻撃を使った事例としては、2009 年から 2010 年にかけて猛威を振るった、ガンブラーが有名ですが、2010 年 9 月には広告配信サービス会社のサイトを改ざんするという新たな手法を使って国内の多数のウェブサイトに影響を及ぼした攻撃が発生しました。ガンブラーの場合も広告配信サイト改ざんの事例の場合も、正規のウェブサイトを改ざんすることによって、上記（1）で説明した“ドライブ・バイ・ダウンロード”攻撃を応用した、閲覧者を悪意あるウェブサイトに誘導するための仕掛けを施すという手法が使われていました。

ガンブラーの場合と広告配信サイト改ざんの事例の場合の違いは、攻撃者が改ざんする箇所にありました。具体的な違いは以下のとおりです。

(i)ガンブラーの場合

ガンブラーの場合は、攻撃者が正規のウェブサイト自体を直接改ざんすることで、当該ウェブサイトの閲覧者が、意図せずに悪意あるウェブサイトに誘導され、ウイルスをダウンロードさせられていました（図 1-2 参照）。

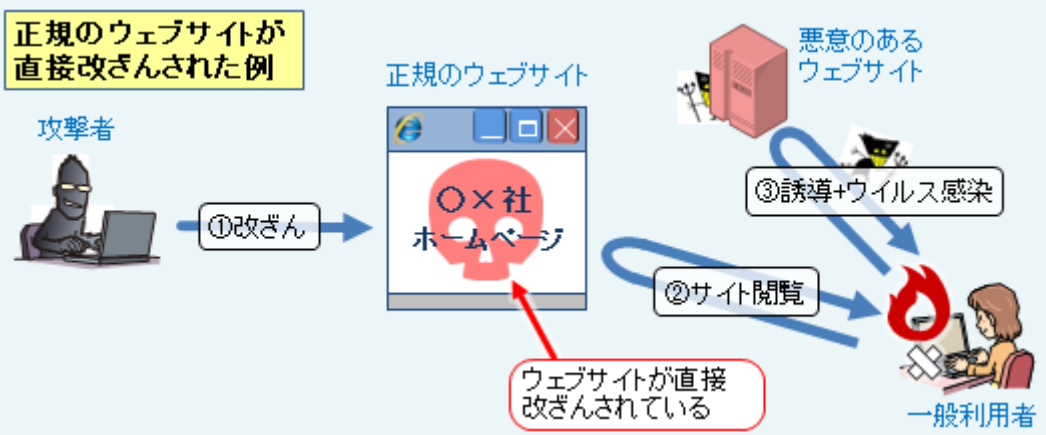

図 1-2：正規のウェブサイトが直接改ざんされた例のイメージ

(ii)広告配信サイト改ざんの事例の場合

広告配信サイト改ざんの事例の場合は、ガンブラーのようにウェブサイト自体が改ざんされたわけではなく、ウェブサイトを構成する部品（バナー広告など）が改ざんされていました。攻撃者がウェブサイトを構成する部品を提供している企業のサーバに侵入し、部品を改ざんすることにより、その企業から部品の提供を受けている企業のウェブサイトの閲覧者が、意図せず悪意あるウェブサイトに誘導され、ウイルスをダウンロードさせられるというものでした（図 1-3 参照）。この事例の場合、正規のウェブサイト側で作成した部分には改ざん箇所が見つからないため、問題箇所の特定が非常に困難です。

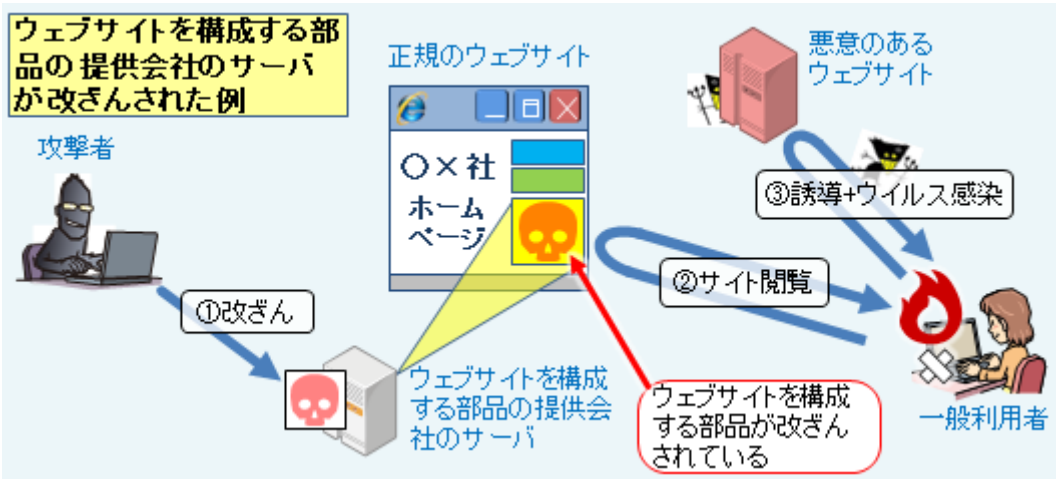

図 1-3：ウェブページを構成する部品の提供会社のサーバが改ざんされた例のイメージ

このように今回紹介した新たな事例では、問題箇所を発見しにくいため対策が非常に困難ですが、(3)項に示すような被害軽減策がありますので、利用することをお勧めします。

（3）ウェブサイト管理者向けの対策（被害軽減策）

今回紹介した事例に適用できるウェブサイト管理者向けの被害軽減策を、以下に説明します。

（i）セキュリティ専門会社が提供しているサービスの利用

今回紹介した事例における被害を軽減する方法としては、セキュリティ専門会社が提供するサービスを利用することが挙げられます。自身の管理するウェブサイトが、改ざんされていないか、また”ドライブ・バイ・ダウンロード”攻撃に使われていないかを監視するサービスが有効です。

（ii）複数のウイルス対策ソフトによるウェブサイトのチェック

複数種類（なるべく多い方がよい）のウイルス対策ソフトを用意し、それぞれのウイルス対策ソフトをインストールしたパソコンを使って、自組織のウェブサイトを定期的にチェックします。複数のウイルス対策ソフトでチェックを行うことで、問題箇所を発見できる可能性が高まります。

また、今回のように自身で作成したウェブサイト自体には改ざん箇所が見当たらないにも関わらず、ウェブサイトの閲覧者から、「あなたの会社のウェブサイトを閲覧したら、ウイルス対策ソフトがウイルスを検知した」などといった連絡があった場合は、IPA に相談してください。

（ご参考）
情報セキュリティ安心相談窓口（IPA）
http://www.ipa.go.jp/security/anshin/
ウェブサイト管理者へ：ウェブサイト改ざんに関する注意喚起
一般利用者へ：改ざんされたウェブサイトからのウイルス感染に関する注意喚起（IPA）
http://www.ipa.go.jp/security/topics/20091224.html

（4）パソコン利用者向けの対策

今回紹介した新たな事例は、ウェブサイト管理者にとっては非常に厄介なものですが、パソコン利用者の対策はこれまでと変わりません。このような攻撃に対する「被害に遭わないための対策」と、被害にあった場合の「復旧のための対策」を以下に示します。

（i）被害に遭わないための対策

このような攻撃の被害に遭わないためには、Windows などの OS や、アプリケーションの脆弱性を解消しておくことが重要です。一般的に利用の多いアプリケーションは狙われやすい傾向にあるため、脆弱性を解消して、常に最新の状態で使用してください。IPA では利用者のパソコンにインストールされているソフトウェア製品のバージョンが最新であるかを、簡単な操作で確認するツール「MyJVN バージョンチェッカ」を公開しています。

（ご参考）
MyJVN バージョンチェッカ（IPA）
http://jvndb.jvn.jp/apis/myjvn/#VCCHECK
「ホームページからの感染を防ぐために」（サイバークリーンセンター）
https://www.ccc.go.jp/detail/web/

また、最近では、ガンブラーや今回紹介した新たな事例のように、正規のウェブサイトが改ざんされ、危険な状態になっている場合があります。このようなサイトからのウイルス感染を防ぐためには、ウイルス対策ソフトの利用が必須です。ウイルス対策ソフトを導入し、ウイルス定義ファイルを最新に保ってください。

（ii）復旧のための対策

ウェブサイトを閲覧した後、明らかにパソコンの動作がおかしくなり、ウイルスに感染した可能性があると感じられるにも関わらず、ウイルス対策ソフトによるウイルスの発見や駆除ができない場合、IPA では、確実にウイルスを除去する手段として、パソコンの初期化（購入時の状態に戻す）をお勧めします。