Topic

平成 25 年6月 26 日

改ざんウェブサイト閲覧によるマルウェア感染に関する注意喚起について

改ざんされたウェブサイトを閲覧するだけで、気付かないうちにマルウェアに感染してしまう可能性があります。ウェブブラウザ及びプラグインを最新バージョンにアップデートすることを強く推奨します。

1 改ざんされたウェブサイトの閲覧によるマルウェア感染の可能性について

警察庁では、ウェブサイトが改ざんされ iframe タグや難読化された JavaScript が挿入されることにより、閲覧者が外部のサイトへ誘導される事案の多発について注意喚起を実施しているところです。[1,2]

改ざんされたウェブサイトからの誘導先について調査を進めたところ、ブラウザプラグイン[3]の脆弱性を悪用することによりマルウェアのダウンロード及び実行が行われる可能性を確認できた事例がありました。これらの事例においては、次のブラウザプラグインの脆弱性が悪用される可能性があります。

- Adobe Flash Player
- Adobe Reader 及び Adobe Acrobat
- Oracle Java

誘導先にアクセスすると、閲覧者のパソコンにインストールされたブラウザプラグインが持つ脆弱性を悪用するファイルの読み込みが行われます。読み込まれたファイルはブラウザプラグインに存在する脆弱性を悪用して、マルウェアのダウンロード及び実行を行う可能性があります。改ざんされたウェブサイトからの誘導の状況は、図1のとおりです。

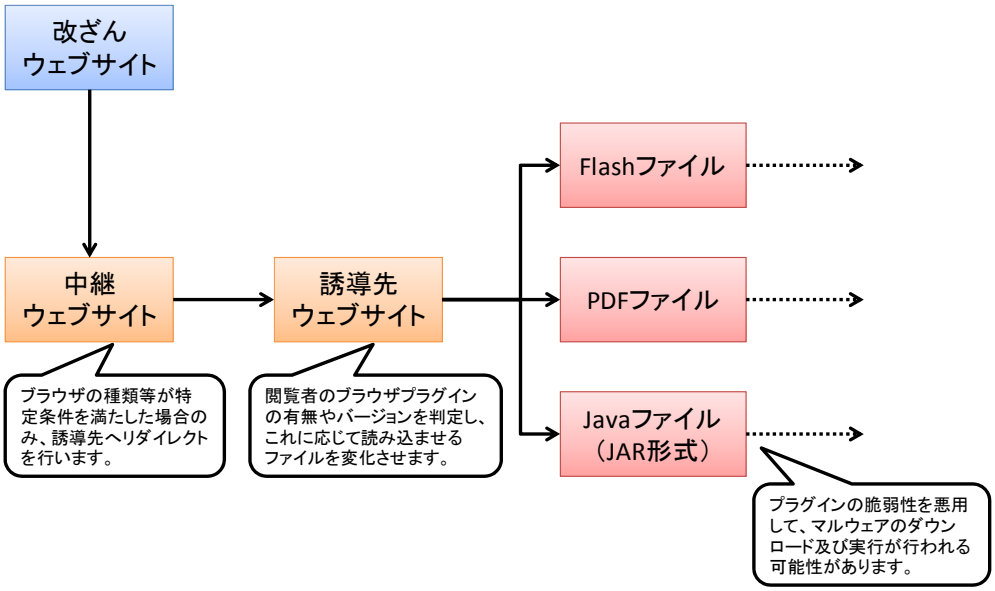

図1 改ざんウェブサイトからの誘導状況

2 マルウェアに感染しないための推奨対策について

改ざんされたウェブサイトの多くは、普段は問題ないコンテンツを提供している健全なサイトであり、かつての「怪しいサイトを見にいかなければ大丈夫」という常識は通用しません。このため、全てのインターネット利用者が、改ざんされたウェブサイトを意図せずに閲覧してしまう可能性を念頭においた対策を実施する必要があります。

改ざんされたウェブサイトを閲覧してしまった際のマルウェア感染を防止するために、次の対策を実施することを推奨します。

- ウェブブラウザを最新バージョンにアップデートする。
- ウェブブラウザにプラグインをインストールする各種ソフトウェアを最新バージョンにアップデートする。以下のソフトウェアについては、特に注意を払う。
  - Adobe Flash Player
  - Adobe Reader 及び Adobe Acrobat
  - Oracle Java
- ウェブブラウザ及び各種ソフトウェアの自動アップデートを有効にする。
- ウェブブラウザ及び各種ソフトウェアが最新バージョンとなっていることを定期的に確認する。

また、マルウェア感染防止のため一般的な対策として、次の対策についても実施することを推奨します。

- OS を最新バージョンにアップデートする。また、自動アップデートを有効にする。
- セキュリティ対策ソフトをインストールし、定義ファイルを最新バージョンに保ち続ける。

---

[1] ウェブサイト改ざん事案の多発に係る注意喚起について（平成 25 年5月 24 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20130524_1.pdf

[2] 外見上変化のないウェブサイト改ざん事案の多発について（平成 25 年6月７日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20130607.pdf

[3] 機能や処理できるファイル形式を拡張するためにウェブブラウザに追加する外部プログラムのこと。ブラウザによっては「アドオン」とも呼称される。