Distributed via
@police
http://www.npa.go.jp/cyberpolice/

平成 26 年1月 24 日

Topic

偽ソフトウェアのインストールを誘うウェブサイト改ざん事案の認知等について

ウェブサイト上に、偽の Adobe Flash Player のインストール画面を表示させ、不正なプログラムを実行させようとする改ざん事案が発生しています。

1 偽ソフトウェアのインストールを誘う新たな形態の改ざん事案について

警察庁においては平成 25 年5月以降、ウェブサイト改ざん事案の多発と、改ざんされたウェブサイトを閲覧することによるマルウェア感染の危険性について、これまでも注意喚起[1]を実施してきましたが、平成 26 年1月以降、従来の改ざんに加え、新たな形態の改ざん事案が増加し始めていることを認知しました。

この新たな形態の改ざんでは、改ざんされたウェブサイトにアクセスすると、通常表示されるウェブページの前面に、偽の Adobe Flash Player（以下、「Flash Player」と記載する。）のインストール又はアップデート画面を表示させ、閲覧者に対して不正なプログラムの実行を行わせようとします。これは、サイトの閲覧に Flash Player のインストール又はアップデートが必要であり、同画面からインストール又はアップデートが実施できると誤信させるものと考えられます。当庁が認知した2種類の偽のインストール及びアップデート画面を図1及び図2に、それぞれ示します。

図1 改ざんされたサイトの前面に表示される偽の Flash Player のアップデート画面

[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
「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
「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」（平成 25 年6月 26 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20130626.pdf
「ウェブサイト改ざん事案の再多発に係る注意喚起について」（平成 25 年9月 30 日）
http://www.npa.go.jp/cyberpolice/detect/pdf/20130930.pdf

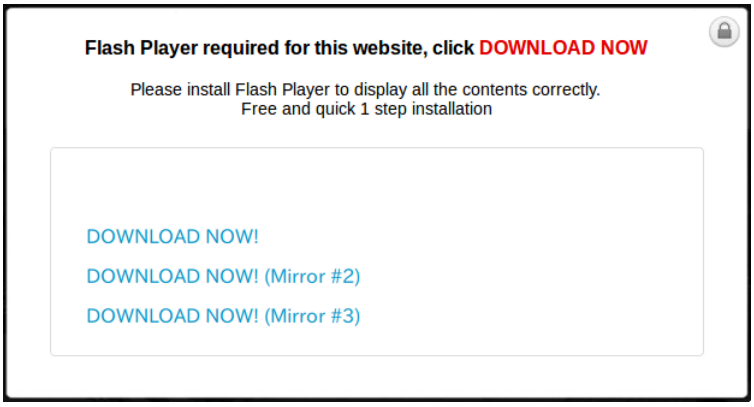

図2　改ざんされたサイトの前面に表示される偽の Flash Player のインストール画面

これらの画面の「DOWNLOAD」や「DOWNLOAD NOW!」等と記載されたリンクをクリックすると、ファイル名が「flashplayerinstaller.exe」[1]である実行ファイルがダウンロードされることを確認しています。ダウンロードされたファイルを実行すると、マルウェアに感染する可能性があります。また、このファイル名は他の類似した名前が使用される可能性もあることから、注意する必要があります。

2　従来の改ざん事案の再多発について

ウェブサイトに外見上変化のない改ざんが行われ、脆弱性のある状態で閲覧することにより、マルウェアに感染する可能性がある形態の改ざん事案についても、再び増加に転じています。一度は収束していた同形態の事案についても、平成 26 年1月には、25 年 11 月及び 12 月と比較して、4倍を上回るペースで事案発生を認知しています。同形態の改ざん事案についても、引き続き注意を払う必要があります。

3　新たな形態の改ざん事案に対する対策

(1) インターネット利用者の対策

全てのインターネット利用者は、改ざんされたウェブサイト等を経由して、偽のソフトウェアを実行してしまうことを防止するため、次の対策を実施してください。

- ウェブサイトの一部として表示されたアップデートやインストールを促す画面については、サイト管理者が意図としている正規なものではなく、改ざん等により不正に挿入されている可能性を考慮する。
- ソフトウェアのアップデートやインストールは、開発及び配布を実施している事業者の正規サイトに直接アクセスして実施する。

[1] 正規の Flash Player の最新バージョンのインストーラには、この様なファイル名は使用されない。

(2) サイト管理者の対策

改ざんされたウェブサイトには図3のようなscriptタグが挿入されていることを確認していることから、サイト管理者は、これまでの注意喚起で示した対策と同様の対策を講ずることが推奨されます。

図3　改ざんされたウェブサイトに挿入されていたscriptタグの例
（ドメイン名の一部については置き換えを実施しています。）

次に、ウェブサイト改ざんを防ぐための推奨対策について再掲します。

- コンテンツマネジメントシステム（CMS）[1]やサーバ管理ソフトウェア[2]の利用有無と、利用している場合には最新のバージョンであるかを確認する。
- FTP[3]、SSH[4]、CMS及びサーバ管理ソフトウェア等のアカウントを適切に管理する。
- サーバにおいて稼働している不要なサービス及び機能は可能な限り停止する。
- コンテンツ管理やサーバ管理のためのアクセスは必要最小限の範囲で許可し、不要なアクセスについては制限する。
- コンテンツ管理及びサーバ管理作業用のコンピュータへのマルウェア感染を防止する。可能であれば、作業を行うコンピュータについては専用のものとする。
- 各種ログについて定期的な監査を実施する。
- 正常な状態のコンテンツファイルのバックアップ、ハッシュ値リスト等を作成しておき、サーバ上のファイルと定期に比較を行うことにより、意図していないファイルの変更や作成がないかを確認する。

[1] ウェブコンテンツを体系的に管理するためのソフトウェア。
[2] サーバの管理作業をウェブ画面等で用意に実施することを可能とするソフトウェア。コントロールパネルとも呼ばれる。
[3] 「File Transfer Protocol」の略。ネットワークを経由してファイル転送を行うためのプロトコルであり、サイト管理者がウェブコンテンツの更新等に使用することも多い。
[4] 「Secure Shell」の略。ネットワーク上で暗号化した通信を行うためのプロトコルであり、サイト管理者がウェブコンテンツの更新や、サーバの管理等に使用することも多い。