Topic

平成 25 年5月 24 日

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 24 年中と比較して2倍以上のペースでウェブサイト改ざん事案発生を認知

1 ウェブサイト改ざん事案の多発について

警察庁においては、平成 25 年1月以降、重要インフラ事業者等のウェブサイトに係る改ざん事案が増加していることを認知しています。これは平成 24 年中と比較すると、昨年の2倍を上回るペースとなっています。

各事案については、改ざんの手口等を断定するに至っていないものの、改ざんの状況や疑われる手口において類似性がある次の2つの形態の改ざん事案を多数認知しています。

(1) CMS の脆弱性を悪用したものと疑われるファイル蔵置事案

本年の1月から2月にかけては、コンテンツマネジメントシステム[注1](CMS)の脆弱性を利用していることが疑われるファイル蔵置事案を多数確認しています。このケースの場合は、既存ファイルは変更されることなく、テキストファイルや画像ファイルが新たに蔵置されている状況が多く見られました。それらのファイルには攻撃者自身のハンドルネーム等が記載されたものがあるため、ファイル蔵置に成功した旨を誇示しているものと考えられます。

(2) 窃取した FTP アカウントによるアクセスであると疑われるファイル改ざん事案

4月以降には、既存のトップページに外部サイトへの誘導を行う iframe [注2]タグを挿入する改ざん事案を多数認知しています。この形態の場合には、一見しただけでは表示内容には変化がなく、改ざんの事実に気付きにくい状況です。また、iframe により誘導された先には、マルウェアが蔵置されている可能性があり、閲覧者のコンピュータに感染する可能性も考えられます。

これらの改ざん事案のうち、幾つかの事例においては FTP [注3]経由により改ざんされたことが判明しています。また FTP ログ等を入手できている事例においては、ログイン試行を複数回実施している形跡が見受けられず、1回のアクセスだけでログインに成功しているケースを確認していることから、FTP アカウントが窃取されている可能性が考えられます。

2 ウェブサイト改ざんを防ぐための推奨対策について

これら改ざん事案の多発を踏まえ、以下の対策が推奨されます。

(1) CMS を利用しているウェブサイトの適切な管理

各組織であるいは、外部委託によりコンテンツ管理している全てのウェブサイトについて、次の対策が推奨されます。

- CMS の利用有無の確認
- CMS を利用している場合には、その CMS のバージョンを確認
- 古いバージョンの CMS を利用していることが判明した場合には、改ざんを許す重大な脆弱性が存在する可能性があるため、最新バージョンへのアップグレードの実施

(2) FTP アカウントの適切な管理

FTP アカウントの窃取を防ぐため、次の対策が推奨されます。

- 存在するFTPアカウントの洗い出しと、各アカウントの利用者及び利用状況の把握
- 不要アカウントの削除
- サイト構築やサーバ管理等に係る外部委託事業者を含めたアカウント管理状況の把握
- コンテンツ更新作業用のコンピュータへのマルウェア感染の防止
- FTPアカウントと同一のユーザ名及びパスワードの使い回しの禁止
- 現状において不要な場合には、FTPサービス自体の停止

また加えて、FTPアカウントを窃取された場合の被害防止措置として、次の対策が推奨されます。

- FTPログ等の定期的な監査の実施
- ファイヤーウォール等における不要なFTPアクセスの制限

注1 Webコンテンツを体系的に管理するためのソフトウェア。Webページを作成するための専門的な知識を必要とせず、コンテンツを管理することができる。

注2 1つのWebページに別のWebページを表示する際などに用いられるもの。通常のWebページでも使用されるが、サイズを小さくしたり、隠したりすることにより、閲覧者に気付かれることなく、埋め込んだWebページへ誘導するなど悪用されることも多い。

注3 File Transfer Protocol。ネットワーク上でファイルの転送を行うための仕組みのこと。Webサイトと Webサイト管理者のパソコンとでWebコンテンツのやり取りの際に使用されることも多い。