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

平成 28 年 11 月 14 日

Topic

Web サイトの改ざんに関する注意喚起について

Web サイトの改ざん事例を把握しています。Web サイトの管理者は、サーバの点検及び被害防止対策を早急に実施することを推奨します。

1 Web サイトの改ざんの状況について

Web サイトのトップページの改ざん及びファイルの蔵置により、アクセス回数や閲覧者など Web サイトの利用状況等についての調査活動が行われていることが判明しました。

攻撃者は、Web サーバに不正ファイル「index_old.php」を蔵置し、

① トップページに、蔵置した「index_old.php」を閲覧者に読み込ませる命令文

〈script type="text/javascript" src="./index_old.php"〉〈/script〉

を追加

② 「index_old.php」を読み込ませることで、閲覧者の IP アドレス、閲覧日時等を別ファイル名でログとして記録

していることが確認されています。

同調査活動は、不正に取得した Web サイトのアクセス情報等の調査のほか、水飲み場型攻撃やサイバー攻撃の踏み台としての利用の可否を確認していると見られ、現在まで国内の複数の Web サイトにおいて上記ファイルの蔵置が確認されています。

2 推奨する対策

(1) サーバの点検等

○ Web サイトのトップページに

〈script type="text/javascript" src="./index_old.php"〉〈/script〉

等の身に覚えの無い命令文が書き込まれていないかを確認する。

○ サーバ内の点検やファイルの差分等の確認により、サーバ内に「index_old.php」等の不審なファイルが蔵置されてないかを確認する。

○ 上記の状況が確認された場合は、サーバが攻撃者の制御下にあると認められることから、保全した後に、サーバに係る全 ID 及びパスワードを変更し、警察に相談する。

○ サーバの再構築を実施する。

(2) 被害防止対策

○ OS 及び IIS(Internet Information Service)、Apache 等のミドルウェアのバージョンアップ等によりぜい弱性を解消する。

○ ウイルス対策ソフトによる検索を定期的に実施する。

○ 20 番(FTP データ)、21 番(FTP コントロール)及び 23 番(telnet)ポートを無効化する。

○ 管理者による Web サイトへのアクセスを SSH(Secure Shell)プロトコルにより実施する。

○ 不正通信の早期発見のため、プロキシサーバログの点検を定期的に実施する。

○ Web サイトの差分確認を定期的に実施する。