2015 年 8 月 7 日

株式会社セキュアソフト

Sniper IPS による対策：金融系ホームページを改ざんして攻撃を行う不正コード

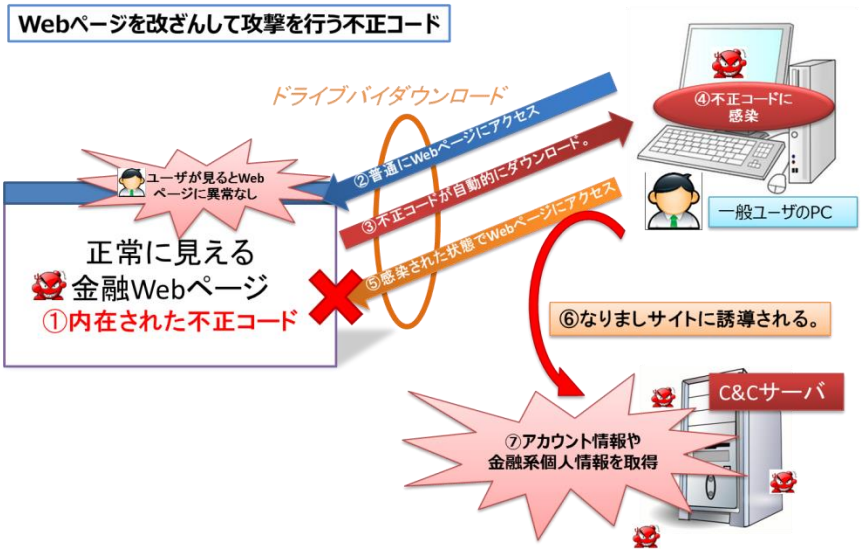
1. 概念

最近、金融系のホームページを改ざんして不正コード（マルウェア）をひそかに組み込まれ、該当のホームページを利用するユーザのアカウント情報などの個人情報が取得される被害が発生しております。ホームページを運用するシステム管理者やサービスを利用するユーザは注意が必要です。しかし、今回、判明した攻撃方法は一般ユーザがその危険性を気づく事が困難です。Sniper IPS ではこの不正コードに対応するシグネチャをリリースしました。本レポートでは攻撃方法と対策方法に関してご案内いたします。

2. 攻撃方法

ホームページを改ざんして攻撃を行う不正コード Win32/Trojan.Banker.141312 は以下の方法となります。

① 攻撃者は正常な Web ページに不正コードをアップロードし Web ページを改ざんする。Web ページの見た目（デザイン）は変わらない。
② 一般ユーザはサイトの危険性を気付かずにアクセスする。
③ ドライブバイダウンロードと呼ばれる手法によって自動的に不正コードが PC にダウンロードされる。
④ 一般ユーザの PC は不正コードに感染。（PC の特定ディレクトリに不正コードファイルが生成される。）
⑤ 不正コードが実行された後に一般ユーザがポータルサイトや金融サイトへ接続する。
⑥ 一般ユーザの通信がなりすましサイトに誘導される。
⑦ 攻撃者はなりすましサイトから一般ユーザが入力したアカウント情報、金融系個人情報を奪取する。



【図 1】攻撃の流れ

3. 脆弱システム

以下のシステムに脆弱性があります。注意が必要です。

・Windows 95/98/ME
・Windows NT
・Windows 2000
・Windows 2003
・Windows XP
・Windows Vista
・Windows 7

4. 対策方法

不正コードに監視した PC は以下の対処が必要です。

① 最新のワクチンプログラムを利用して不正コードを駆除します。
② 手動で PC の特定ディレクトリに感染されている不正コードを駆除します。

Sniper IPS では以下のシグネチャで対処可能です。

【表 1】 リリースシグネチャの情報

攻撃コード	攻撃名
3167	Win32/Trojan.Banker.141312

＊本シグネチャは遮断設定を推奨するシグネチャとなります。

以上