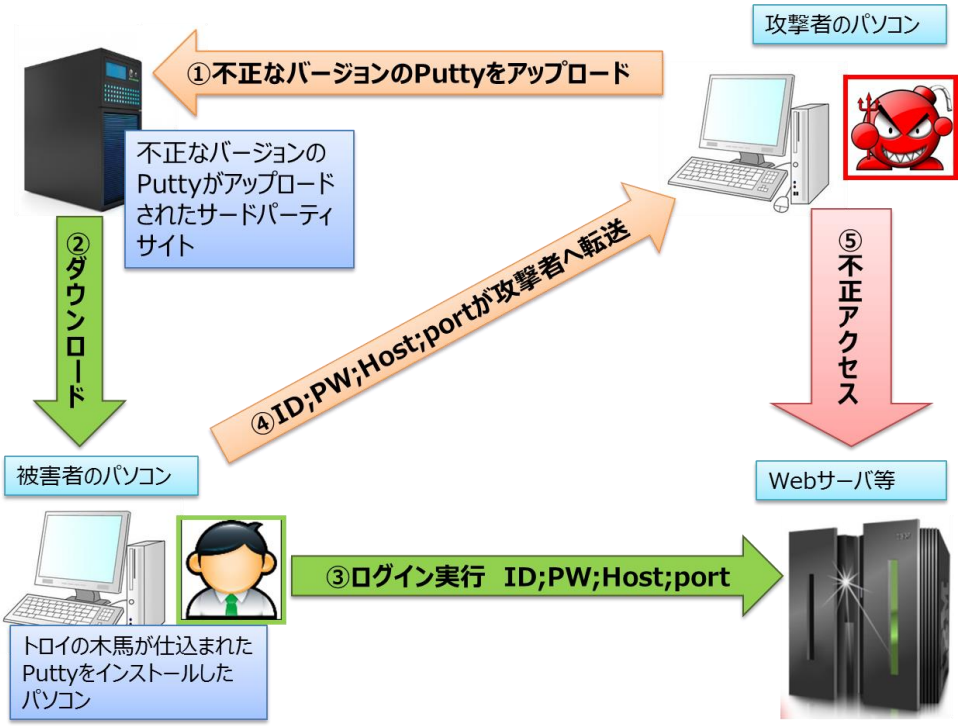
2015 年 6 月 5 日
株式会社セキュアソフト

注意喚起：トロイの木馬が仕込まれた PuTTY

1. 概要

PuTTY は Windows 向けの SSH クライアントソフトウェアで、システム管理者、Web 開発者などのエンジンニアなど多くの方が利用しています。PuTTY はオープンソースソフトウェアのため、世界中で様々な変更を加えたバージョンが配布されています。今回、トロイの木馬が仕込まれた PuTTY が確認されました。今回確認された不正なバージョンの PuTTY を利用した場合、サーバに接続する際のログイン情報などが攻撃者に取得される恐れがあります。

2. 攻撃の流れ



① 攻撃者はトロイの木馬を仕込んだ不正な PuTTY をサードパーティサイトにアップロードします。
② 利用者は PuTTY の公式サイトや信頼されるサイトではないサードパーティサイトから不正なバージョンと気付かずに PuTTY をダウンロードします。
③ 利用者は不正なバージョンの PuTTY をインストールし、トロイの木馬に感染します。
④ 利用者が PC から各種サービスを利用する際に使用する ID やパスワードなどの情報がトロイの木馬により攻撃者に転送されます。
⑤ 攻撃者は取得した情報を利用して対象サービス（サーバ）にアクセスし不正行為を行います。

3. 対策方法

① PuTTY をダウンロードする際には公式サイトや信頼されるサイトからダウンロードします。
② PuTTY をダウンロードする際にファイルサイズをチェックします。2015 年 6 月 4 日現在リリース 0.64 のファイルサイズは 524,288Bytes です。トロイの木馬が仕込まれたバージョンはファイルサイズが 593,920 bytes であったことが確認されています。
③ パソコンにインストールされた PuTTY を確認して、リリースバージョンが「Unidentified build」に表示された場合不正なバージョンの可能性があるため削除します。

以上