NTTデータ・セキュリティ株式会社

TrueCrypt に対する Evil Maid 攻撃に関する検証レポート

2009/11/9
NTT データ・セキュリティ株式会社
辻 伸弘
松田 和之

【概要】

ハードウェアの暗号化を行うソフトウェア「TrueCrypt」を攻撃するコンセプト実証コードが発表されました。
発表者によると、その攻撃は、ホテルの部屋などに、ハードディスクを暗号化した PC を宿泊客が置いている場合を想定し、その部屋に侵入したメイドが、宿泊客が置いた PC に対して、ディスク暗号化のパスフレーズを記録するように細工し、パスフレーズを盗み出すことを想定されることから、「Evil Maid 攻撃」と名付けられています。

コンピュータが盗難被害に遭った場合でも、ハードディスクの暗号化が行われていれば、ハードディスクの内容を閲覧することはできませんが、今回の Evil Maid 攻撃を受けると、暗号化を解除するためのパスフレーズが窃取されるため、ハードディスクの内容を閲覧される危険性があります。

今回、この TrueCrypt の Evil Maid 攻撃の脆弱性について検証を行いました。

【影響を受けるとされているシステム】

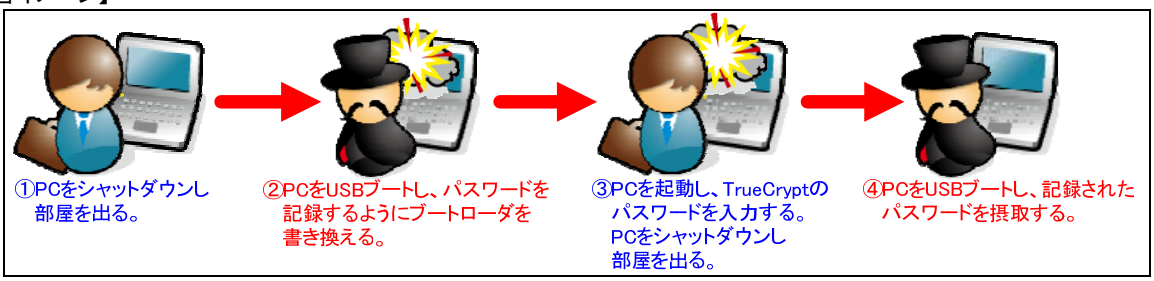
TrueCrypt を導入したシステム

【対策案】

このレポート作成現在（2009 年 11 月 9 日）、対策方法はリリースされておりません。

この攻撃手法はコンピュータを直接、操作できることが前提条件となります。そのため、運用による回避策として、第三者にコンピュータを操作されないよう、厳重に管理することが推奨されます。

【被害イメージ】



NTTデータ・セキュリティ株式会社

【想定される被害フロー】

① コンピュータ持ち主が、コンピュータをシャットダウンし、部屋（例えばホテルの一室）に置いたまま、外出します。なお、当該コンピュータは、TrueCrypt によってハードディスク全体を暗号化されています。

② コンピュータの持ち主が部屋にいない間に、悪意あるユーザは、部屋に置かれたままのコンピュータに、TrueCrypt のパスフレーズ入力を記録するプログラムが格納された USB メモリを挿入し、コンピュータを起動させます。これにより、パスフレーズ入力が記録されるように、ブートローダが書き換えられます。その後、悪意あるユーザはコンピュータをシャットダウンします。

③ コンピュータの持ち主が、TrueCrypt のパスフレーズを入力し、コンピュータを起動します。このタイミングで、暗号化されない領域に TrueCrypt のパスフレーズが記録されます。その後、コンピュータの持ち主は、コンピュータをシャットダウンし、外出します。

④ コンピュータの持ち主が部屋にいない間、悪意あるユーザが、記録されたパスフレーズを読み出すプログラムが格納された USB メモリを挿入し、起動させます。これにより、TrueCrypt のパスフレーズの窃取が可能となります。

【検証ターゲットシステム】

TrueCrypt 6.3 をインストールした Windows XP

【検証概要】

TrueCrypt をインストールしたターゲットコンピュータに対して、TrueCrypt のパスフレーズを記録するようにブートローダを書き換えます。コンピュータの持ち主によって TrueCrypt のパスフレーズを入力された後、記録されたパスフレーズの窃取を試みます。

【検証結果】

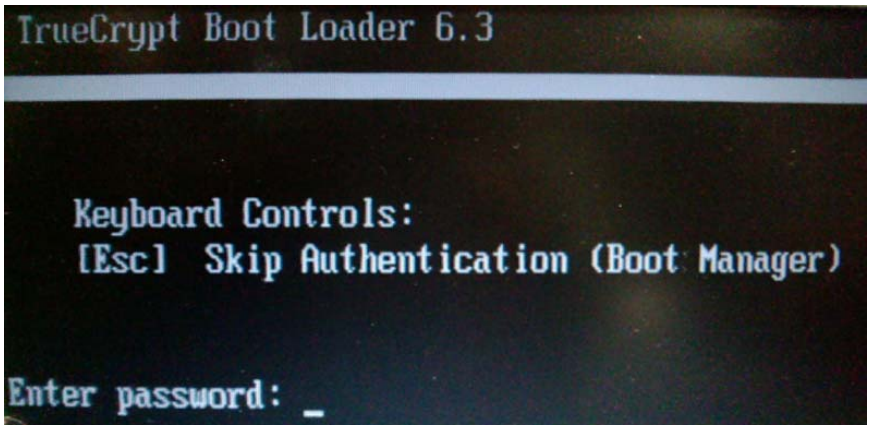
下図は、ターゲットコンピュータに USB を挿入し、起動した後、TrueCrypt のパスフレーズ入力を記録するようにブートローダを書き換えた画面です。（想定される被害フロー②）

USB ブート後、ブートローダを書き換えた画面

NTTデータ・セキュリティ株式会社

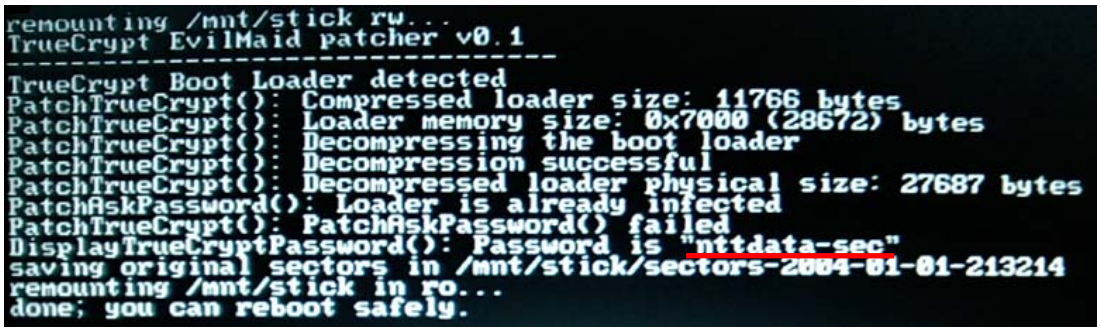
下図は、コンピュータの持ち主が、起動し、TrueCrypt のパスフレーズを入力する画面です。
（想定される被害フロー③）
ここで入力されたパスフレーズは、暗号化されない領域に記録されることとなります。

TrueCrypt のパスフレーズ入力画面



下図は、ターゲットコンピュータに USB を挿入し、起動した後、記録された TrueCrypt のパスフレーズを読み出した画面です。
（想定される被害フロー④）
赤線の部分が示すとおり、TrueCrypt のパスフレーズ窃取に成功しました。
これを用いることにより、ハードディスクの内容を閲覧することが可能となります。

TrueCrypt のパスフレーズを読み出した画面



＊各規格名、会社名、団体名は、各社の商標または登録商標です。

【お問合せ先】
NTT データ・セキュリティ株式会社
営業企画部
TEL：03-5425-1954
http://www.nttdata-sec.co.jp/