

2014 年 7 月 16 日

報道関係各位

株式会社セキュアブレイン

セキュアブレインが国内 20 のカード会社を狙うウイルスに対して注意喚起

株式会社セキュアブレイン(本社:東京都千代田区、代表取締役社長 兼 CEO:成田 明彦、以下「セキュアブレイン」)は、金融機関を狙う不正送金ウイルスが国内 20 のカード会社を攻撃対象とする更新がされたことを確認しました。セキュアブレインは、注意喚起を促すと共に、その手口を公開します。

今回、攻撃対象の変化が観測されたのは通称 VAWTRAK、または Papras と言われるウイルスで、感染した PC で攻撃対象のインターネットバンキングサイトにアクセスした際に、MITB(マン・イン・ザ・ブラウザ)攻撃によりコンテンツを改ざんし、情報を盗むタイプのウイルスです。このウイルスは以前から銀行だけでなく、数社のカード会社も攻撃対象としていました。しかし、改ざんを実行する JavaScript を配信するサーバが停止したことに伴い、改ざんや情報の窃取は行われていませんでした。

今回のウイルスの設定情報の更新により、国内 20 のカード会社を攻撃対象としていることを確認しました。攻撃対象のページにアクセスすると、MITB 攻撃により<script>タグを含む短いコード片が挿入されます。この<script>タグが外部のサーバから偽画面の表示などを行う JavaScript を読み込み、改ざんや情報の窃取を実行します。今回の更新では、新たに海外にある5つの改ざん実行 JavaScript の配信サーバを使ってカード会社に対して改ざんを行うように更新されています。銀行だけでなくカード会社も攻撃対象になっていることを認識する必要があります。

今回、以下のカード会社が攻撃対象として確認されました。(50 音順)

イオンカード、出光カード、NTTグループカード、エポスカード、OMCカード、オリコカード、JCBカード、JP BANKカード、セゾンカード、TS CUBIC カード、DCMX、日産カード、ポケットカード、Honda C カード、三井住友 VISA カード、三菱 UFJ ニコス、UCS カード、ライフカード、楽天カード、りそなカード

インターネットバンキングユーザを狙った MITB 攻撃と同様に、このウイルスも偽の入力画面を表示させます。カード会社のサイトのログインフォームで、ID とパスワードを入力するとそれが攻撃者のサーバに送信された上で、カード番号、有効期限、セキュリティコードなどを入力させる画面が表示されます。多くのカード会社では、通常 1 つの画面でセキュリティコードまでの入力を求めることはないで、そのような画面が表示された場合は、入力を停止してください。また、この画面が出る前に入力した ID とパスワードは既に攻撃者のサーバに送信されていますので、すぐに変更をしてください。

■MITB 攻撃でカード情報を盗む偽画面例

あなたのIDを登録されるため下のフォームを記入して下さい

© SecureBrain

(1) 氏名(漢字)	必須	(姓) (名) (全角)
(2) 氏名(カナ)	必須	(セイ) (メイ) (全角カナ)
(3) 生年月日(半角数字)	必須	西暦 年 月 日 ※入力数字が1桁の場合は先頭に0を加えてください。 例:「1990」年「08」月「01」日
(4) 会員番号(半角数字)	必須	- - - ※クレジットカードの会員番号を4桁ずつ入力してください。 例:「3500」-「1234」-「5678」-「9012」
(5) 有効期限(半角数字)	必須	月 / 20 年 ※カードの表示「04/18」⇒「04」月/20「18」年
(6) セキュリティコード(3桁の半角数字)	必須	 カード裏面の署名欄に印字されている番号の下3桁になります。 

防御策としては、PC を常にウイルスに感染していないクリーンな状態に保ってください。ウイルス対策ソフトを必ず使用し、さらにウイルス定義ファイルを最新の状態にしてください。そして、使用しているカード会社の正しい画面を把握し、異変に気が付くよう警戒心を持ってください。また、使用しているカード会社が特定のセキュリティソフトの使用を呼びかけている場合は、そのソフトウェアをインストールし、使用して下さい。

セキュアブレインは、本ウイルスの MITB 攻撃を検知しユーザに警告する機能を搭載した「PhishWall プレミアム」と「PhishWall クライアントレス」を金融機関に提供しています。

以上

セキュアブレインについて:

株式会社セキュアブレインは、インターネット上の脅威が多様化する中、Web サービスを提供する事業者や企業に IT セキュリティを届ける、サイバーセキュリティ専門会社です。「ネット犯罪からすべての人を守る」というミッションのもと、信頼性の高いセキュリティ情報と高品質なセキュリティ製品・サービスを提供する、日本発のセキュリティの専門企業です。詳細は、<http://www.securebrain.co.jp> をご覧ください。

◆ 本件に関する報道関係者さまからのお問い合わせ先 ◆

株式会社セキュアブレイン 広報担当: 丸山 芳生(まるやま よしお)

e-mail: info@securebrain.co.jp 電話: 03-3234-3001、FAX: 03-3234-3002

東京都千代田区麹町 2-6-7 麹町 RK ビル 4F