PRESS RELEASE

2014 年 5 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、ワンタイムパスワードを盗むタイプのウイルスの挙動を解析

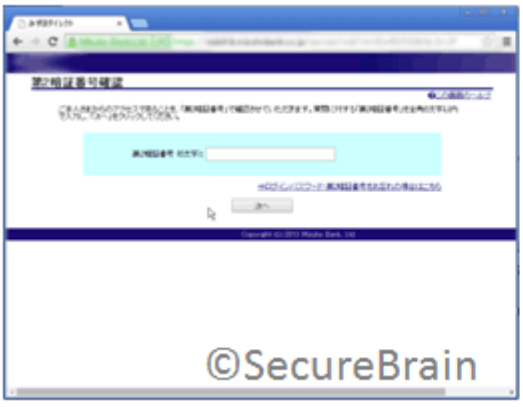
国内メガバンクを含む 5 行がターゲットに

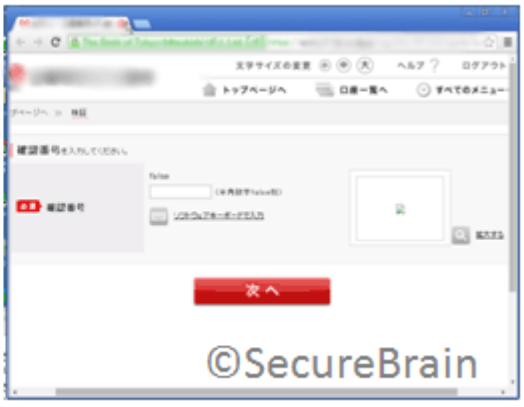
株式会社セキュアブレイン（本社：東京都千代田区、代表取締役社長　兼　CEO：成田　明彦、以下「セキュアブレイン」）は、ワンタイムパスワードを盗むタイプの MITB（マン・イン・ザ・ブラウザ）攻撃型ウイルスを捕獲し、その挙動を解析した結果、国内メガバンクを含む 5 行への攻撃を確認しました。セキュアブレインは、注意喚起を促すと共に、その手口を公開します。

セキュアブレインが、国内で被害が発生したワンタイムパスワードを盗む MITB 攻撃型ウイルスと同タイプのウイルスを解析した結果、同ウイルスに感染した PC では、対象になった複数のオンラインバンキングサイトにアクセスした場合にコンテンツの改ざん及び情報を盗む挙動を確認しました。

対象となっているオンラインバンキングサイトにアクセスした際に、正規オンラインバンキングサイトから受信した HTML が、MITB 攻撃によって書き換えられます。書き換えの結果、外部のサーバから JavaScript を別途取得し実行します。この JavaScript が実際の画面の改ざんや情報の送信を行います。それぞれの金融機関ごとに別の JavaScript が取得、実行されますが、それらの JavaScript は全て同一のサーバから取得されていました。

■MITB 攻撃でワンタイムパスワードや暗証番号をウイルスが要求する偽画面例

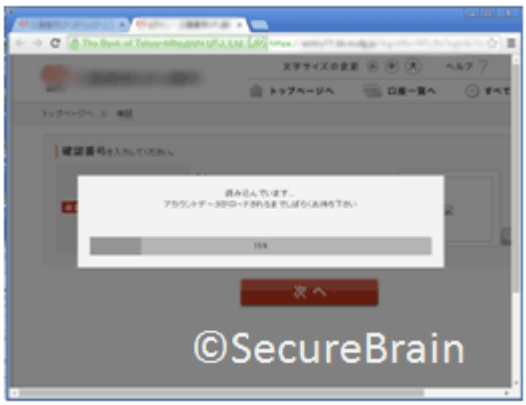




改ざんを行う JavaScript は、偽の入力画面を表示するだけでなく、正規の画面に入力されたログイン ID を外部に送信するなど、画面を変更しないで情報を盗むケースも確認されています。

また、複数の金融機関の改ざんで、「アカウントデータがロードされるまでしばらくお待ち下さい」という同じ文言、デザインの偽画面を表示する機能が存在しており、それぞれの金融機関ごとに改ざんを行う JavaScript は異なるものの、プログラムの部品の共通化が行われていることも判明しました。

■ワンタイムパスワードや暗証番号を入力後、ウイルスが表示する偽画面例



防御策としては、オンラインバンキングで使用する 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つ必要があります。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、使用している銀行の正しい操作画面を把握し、異変に気が付くよう警戒心を持ってください。

セキュアブレインでは、今回解析したウイルスを「PhishWall プレミアム」で防御できることをすでに確認しています。「PhishWall プレミアム」を導入済みの金融機関のユーザは、「PhishWall クライアント」をインストールすることによって、同ウイルスの脅威から保護されます。

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、全てのインターネットユーザに安心を届ける、セキュリティのスペシャリストチームとして、「より快適で安心できるネットワーク社会を実現するために、一歩進んだ技術で貢献する」というビジョンのもと、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