PRESS RELEASE

2015 年 12 月 17 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、セキュリティ対策ソフトを推奨する偽画面を表示する 不正送金ウイルス「Rovnix」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：新保　勲、以下「セキュアブレイン」）は、国内の金融機関のインターネットバンキングにおいて、暗証番号やパスワード等を詐取する不正送金ウイルス「Rovnix（ロヴニクス）」を捕獲し解析を行いました。 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。

Rovnix は以前より確認されていたウイルスですが、今回捕獲した Rovnix は国内の金融機関をターゲットとするようカスタマイズされています。Rovnix は、攻撃用モジュールをダウンロードすることで種々の攻撃活動を行う機能を有しており、今回の攻撃活動は、ブラウザへのインジェクション機能を持つモジュールを攻撃者サーバからダウンロードすることで MITB 攻撃を実行するものです。

本 Rovnix に感染した PC で攻撃対象の金融機関のインターネットバンキングのログインページにアクセスした場合に、攻撃者のサーバから不正なスクリプトを読み込み、ログインページを改ざんします。改ざんされたログインページでは、金融機関の提供する不正送金に関する注意喚起が表示されないなどの現象が発生します。さらに、改ざんされたログインページで情報を入力しログインボタンを押下すると、攻撃者のサーバに情報を送ります。

またログインボタンの押下後、金融機関がセキュリティ対策ソフトの使用を推奨しているように見せかける偽画面を表示します。これにより、偽画面で正規のログイン画面を表示させないようにしており、セキュリティ対策ソフトの使用を推奨する偽画面の表示以降、ログイン状態を維持させ、その他必要な情報の詐取を行います。

セキュリティ対策ソフトの使用を推奨しているように見せかける偽画面以外に、以下を表示させることを確認しています。

- ●システムメンテナンスを装い、情報の入力を促すメッセージ
- ●暗証番号等の入力を促すコンテンツ
- ●ワンタイムパスワード等の入力を促すコンテンツ
- ●偽のセキュリティ対策ソフトの配布ページと思われるコンテンツ
- ●偽のセキュリティ対策ソフトのインストール中を装うと思われるコンテンツ

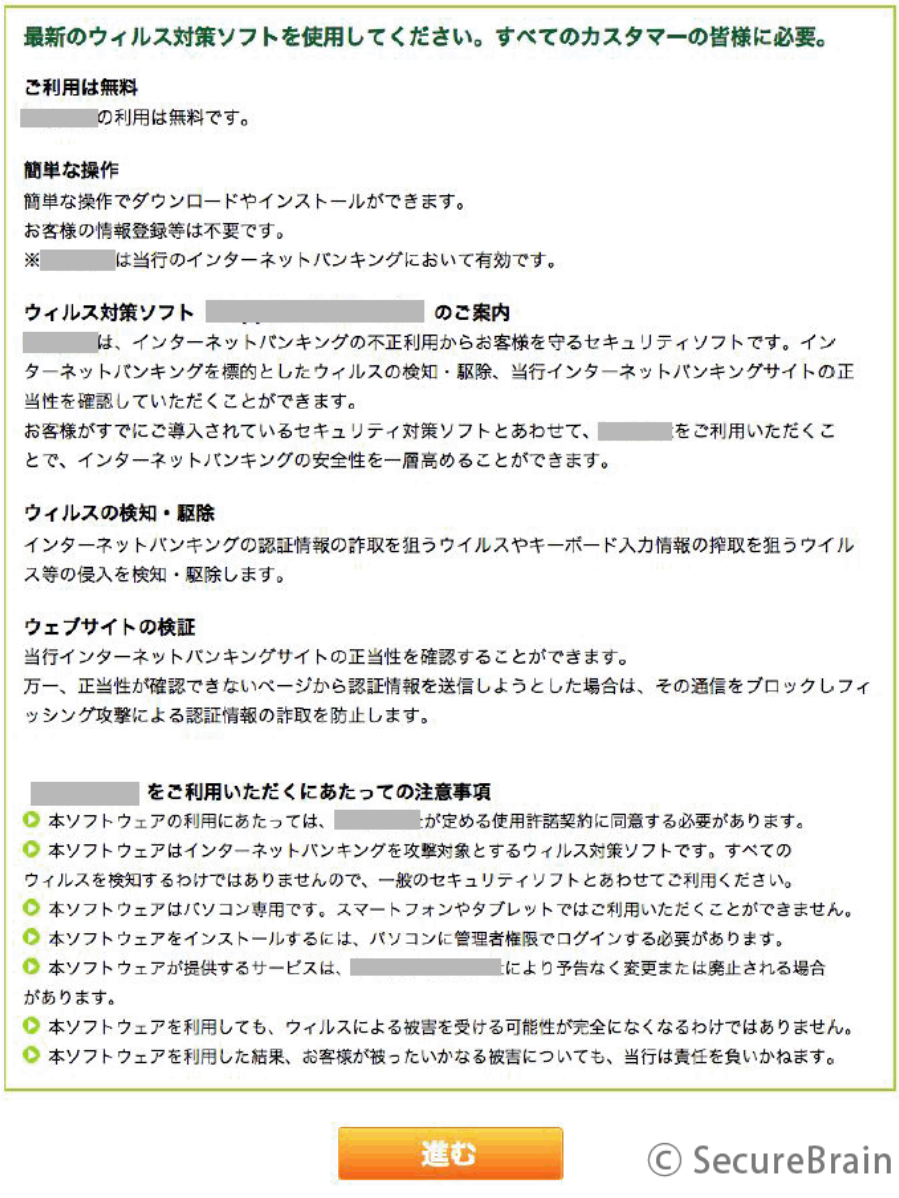
※詐取される情報は、攻撃対象となる金融機関毎に異なります。

本 Rovnix は、カーネルに感染する可能性が高く、感染した場合は OS の再インストールが必要になる可能性があります。

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。OS やアプリなどを最新の状態にアップデートしてください。そして、使用している金融機関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、不審なメールの添付ファイルや URL は決して開かないようにしてください。使用している金融機関等からの通知メールの形式を理解してスパムメールではないか注意を払ってください。使用している金融機関等の提供する注意喚起等の情報に常に注意を払ってください。

なお、セキュアブレインは、自社が開発・販売する不正送金対策ソリューション「PhishWall プレミアム」が本ウイルスの攻撃を検知することを確認しています。

【金融機関がセキュリティ対策ソフトの使用を推奨しているように見せかける偽画面】



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

東京都千代田区紀尾井町 3-12 紀尾井町ビル 7F