

平成27年2月20日

インターネットバンキングご契約者様各位

インターネットバンキングにおける警察庁からのウイルス情報について

標記について、警察庁から提供を受けましたウイルスに関する情報を精査した結果、当該情報の中に個人 I B および法人 I B にログインする際に不正な画面を表示させ、I D、パスワード等を搾取する機能を持つウイルスがあることを確認いたしました。

つきましては、ウイルス情報および対策について下記のとおり取り纏めましたのでご案内申し上げます。

記

1. ウイルスの情報

(1) ウイルス名

VM Zeus[ブイエム ゼウス]

※セキュリティ会社により名称が異なる場合があります。

※VM Zeus は、多くの存在が確認されている Zeus ウイルスの亜種のひとつです。

(2) Zeus ウイルスとは

Zeus(Zbot[ゼッドボット]とも呼ばれる)は、I B 利用者のパソコンに侵入し、I B にログインする際に不正な画面を表示し、この画面に入力した I D、パスワード等の情報を盗み取ります。感染経路としては、不正な Web サイトからのダウンロード(第三者に改ざんされたサイトでは、閲覧しただけで感染する。)やスパムメール、Facebook に張られたリンク等が考えられます。

(3) 今回確認された不正画面

I B のログイン画面にて I D、パスワードを入力し、ログインボタンを押下すると「あなたのコンピュータを認識できませんでした」の偽画面を表示しパスワードを詐取し、詐取したパスワードを用いて不正送金を行います。

なお、ログイン画面は、I B システムが送信した画面をウイルスが改ざんしたうえで表示され、I D、パスワードを入力すると I B システム側に送られることはなく、搾取されます。

(個人 I B の偽画面)

あなたのコンピュータをシステムが認識できませんでした。

ログイン

インターネット・サービスプロバイダーが行った最近の変更、
またはあなたが行ったソフトウェアの更新による可能性があります。
引き続きバンキングサービスを利用するには、表からコードを入力してください。

ア	イ	ウ	エ	オ	カ	キ	ク
(2)			(4)			(3)	(1)

(1)(り)	(2)(ア)	(3)(キ)	(4)(工)
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

■ 英字は大文字と小文字を区別しますので、ご注意ください。
■ ブラウザの「戻る」「進む」ボタンは使用しないでください。
■ ご利用の os およびブラウザや文字の大きさによっては、画面のレイアウトが若干崩れる場合がありますが、お取引に影響はありません。

(法人 I B の偽画面)

あなたのコンピュータをシステムが認識できませんでした。

インターネット・サービスプロバイダーが行った最近の変更、
または、ソフトウェアの更新による可能性があります。
引き続きバンキングサービスを利用するには、表からコードを入力してください。

都度振込送信確認用パスワード1	都度振込送信確認用パスワードの左から1桁目を入力してください。	<input type="text"/>
都度振込送信確認用パスワード2	都度振込送信確認用パスワードの左から6桁目を入力してください。	<input type="text"/>
都度振込送信確認用パスワード3	都度振込送信確認用パスワードの左から7桁目を入力してください。	<input type="text"/>
都度振込送信確認用パスワード4	都度振込送信確認用パスワードの左から9桁目を入力してください。	<input type="text"/>

2. ラポート (Rapport) での検知

上記画面が表示された I B 利用者にラポートをインストールしたところ、VM Zeus を検知のうえ駆除されることが、確認されています。(ウイルス検知サービスでは、検知できておりませんでした)

なお、ラポートにつきまして、すべての Zeus ウイルスの亜種*が検知可能かは、ウイルスの検体を確認しない限り確実なことは言えません。

*亜種・・・既存のウイルスの一部を変更して作られたウイルス。一部を変更することでウイルス対策ソフトに見つからないようにする。

3. 対策

VM Zeus の対策は以下のとおりです。

- ・電子証明書 (法人 I B) およびワンタイムパスワード (個人 I B) の利用
- ・ラポート等の I B 専用セキュリティソフトの利用

以 上