
TRAM SYSTEM
NEWS LETTER
Ver. 2014. 09

今月のコンテンツ

不正送金ウィルス

◎ ネットバンキング不正送金

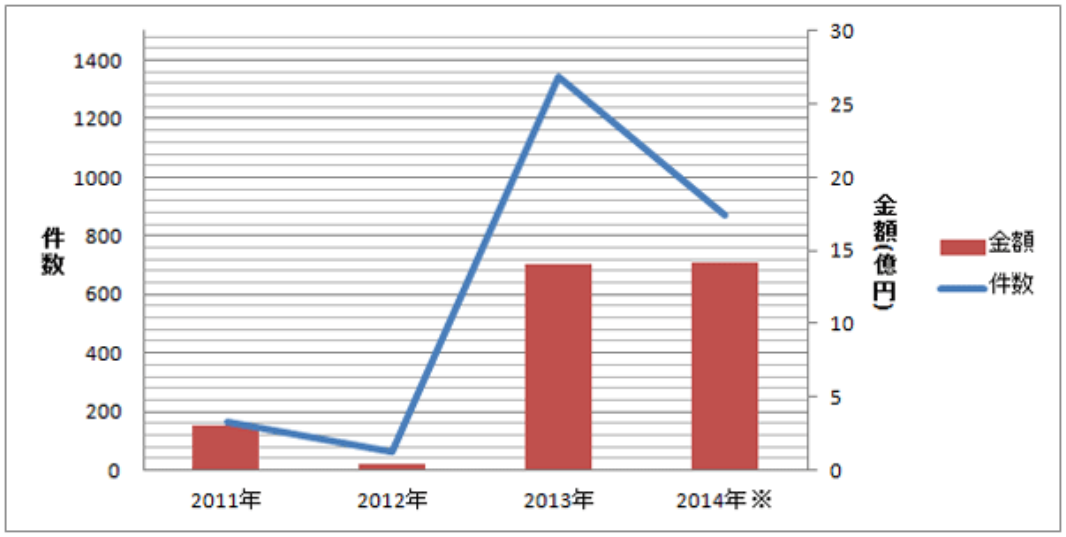
- 企業被害の実態
- 不正送金ウィルス　ZBOTファミリー
- クレジットカードの被害も拡大中
- 不正送金ウィルスの感染経路
- 法人ネットバンキング　被害補償について

インターネットバンキングのパスワードがコンピューターウィルスによって盗まれ、預金を奪われる被害が過去最悪のペースで増えています。
法人向けネットバンキングでの被害も目立ち、今年の5月時点で被害額が4億8000万円にも上ります。
そこで今回はウィルス対策特集として、不正送金の実態とその予防対策についてご紹介していきたいと思います。

◎ ネットバンキング不正送金

・企業被害の実態

警察庁は2014年7月18日、インターネットバンキングの不正送金被害を引き起こすウィルスに感染したパソコンが日本国内に少なくとも15万5000台あると発表しました。
　米連邦捜査局（FBI）によると、世界で100万台が感染している可能性があるとし、被害は既に100億円を超えてるそうです。依然、国内での不正送金被害は急増しており、2014年5月9日現在で14億1700万円と昨年の被害総額を超えて、史上最悪となりました。



警察庁によりますと企業被害は昨年全体の4%だったのに対し、今年は12%と大幅に増えています。被害額も大きく、今年だけで4億8000万円と全体の33%を占めています。

この不正送金被害を引き起こすウィルスは「ゲームオーバーゼウス」と呼ばれており、2007年ごろから発生した「ZBOT」と呼ばれるウィルスの進化版です。

◎ ネットバンキング不正送金

・不正送金ウィルス　ZBOTファミリー

「ZBOT」の「BOT」とは、感染の結果、不正リモートユーザーに外部から操作されるゾンビPCのことであり、そのようなゾンビPC同士のネットワークのことを「ボットネット」と呼びます。
「ZBOT」はそうしたボットネットの中でも特に悪質なものとして有名なのです。先にあげられた「ゲームオーバーゼウス」もZBOTの一種で、その数実に2,000個以上ともなり、これらを総合した名称が「ZBOTファミリー」と呼ばれています。

まったく、はた迷惑なファミリーがいたもんです・・。

2012年にパソコン遠隔操作事件で遠隔操作されたPCがまさにこのゾンビPCというわけですね。
真犯人が名乗り出なければ誤認逮捕と気づかぬままに事件が完結されていたと言われています。

次に「ゲームオーバーゼウス」が実際にどうやって不正送金していくのか見ていきましょう。
企業ではネットバンキングを安全に利用する為に電子証明書で認証していますが、このウィルスはその電子証明書自体を盗み取り、攻撃者へ送信してしまいます。
電子証明書が「エクスポート可」で「秘密キーの保護なし」だと感染した時点で情報が抜き取られます。保護が掛かってるなど窃取できなかった場合は電子証明書を削除しておき、企業では不審に思いながらも再発行したところを傍受し、電子証明書を窃取します。

◎ ネットバンキング不正送金

・クレジットカードの被害も拡大中

2014年4月頃からクレジットカードでも同じ手口で情報が盗まれ、高額の買い物をされる被害が相次いでいることが発覚し、カード会社などが注意を呼びかけています。

あるカード会社では、こうした手口による被害が分かっているだけで20件に上り、何者かが不正に合せて200万円ほどの買い物をしたということです。

これもZBOTファミリーの一員で、新参者ながらかなりの被害をだしています。
手口としては感染しているPCでカードの利用明細の確認などを行うホームページにログインすると、別のニセログイン画面が表示され、利用者にカード番号や有効期限・セキュリティコードを入力させて盗み取ります。

セキュリティー会社によりますと、クレジットカード情報を盗むウィルスが検出されたパソコンは国内で、先月だけで少なくとも1万台を超えているそうです。

現在ウィルスが確認されているカード会社

- TSCUBICカード
- 三井住友VISAカード
- 三菱UFJニコスカード
- ライフカード
- 楽天カード

彼の力でもZBOTファミリーには敵わないようですね・・。

◎ ネットバンキング不正送金

・不正送金ウィルスの感染経路

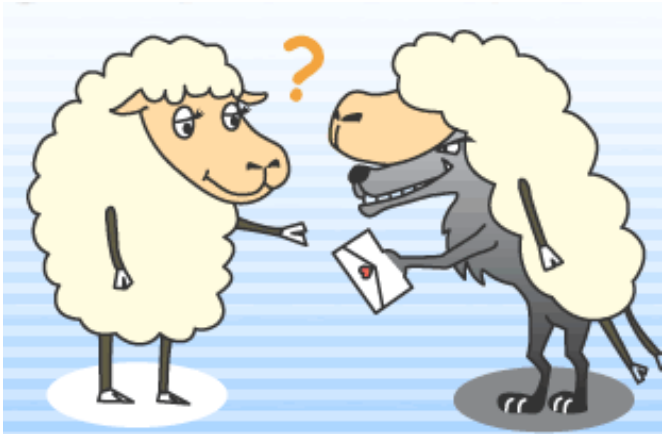
それでは次に、「ZBOT」感染経路を見ていきましょう。
主な感染経路は2系統です。

【1】 メール経由

スパムメールと呼ばれ、有名企業や銀行を騙ったメールがユーザーに送付されてきます。

①メールに添付されているファイルを開くと感染
②メールに書かれている誘導URLをクリックすると感染

最近では政府関係機関を装った事例も報告されており、マイケル・ジャクソンの死因騒動といった、世間の注目を集める話題に便乗したスパムメールもあるようです。



感染経路を見て「あ、それオレやん。」
と思った方はすぐにでもウィルススキャンして下さいね。

【2】 ブラウザ経由

①第3者にハッキングされている一般サイトやブログを訪問して感染
②ZBOTが仕掛けてあるフリーソフトをダウンロードして感染

ウィルス対策ソフトを入れてるとサイトに飛ぶ前に危険だから飛ばない方が良いですよとポップアップが出ますが、これを無視してサイトに飛ぶとウィルス対策ソフトを入れてても感染してしまいます。

◎ ネットバンキング不正送金

・法人ネットバンキング　被害補償について

全国銀行協会では今まで個人の被害については預金保護法に基づき補償を行ってきましたが、企業は原則として対象外になっていました。しかし、企業での被害が拡大する中、一定のセキュリティー対策をしていることを条件として、法人のネットバンキングも補償するとの指針をだしました。

複数ウィルス対策ソフトを入れてしまうと、互いにケンカしてPC自体の能力が大幅にダウンすることがあるので注意しましょう。

◆法人が実施すべきセキュリティー対策

1. 各銀行が導入しているセキュリティー対策の実施。
2. 基本ソフト（OS）やウェブブラウザー等、インストールされている各種ソフトウェアを常に最新状態に更新する。
3. メーカーのサポート期限が経過したソフトやOSを使用しない。
4. セキュリティー対策ソフトを導入し、常に最新状態に更新する。
5. ネットバンキングに係るパスワードを定期的に変更する。
6. 銀行が指定した正規の手順以外での電子証明書の利用は止める。

TREND MICRO　KASPERSKY lab
McAfee Proven Security　symantec.

ここまで駆け足で不正送金について見てきましたが、企業を狙う手口が巧妙化しており、さらに被害が拡大する可能性が非常に高いです。経営者に限らず、ネットバンキング担当者はもちろん、従業員全員が危険を知り、不用意なクリックをしないことが重要です。

TRAM SYSTEM

トラムシステム株式会社
〒465-0063
愛知県名古屋市名東区新宿2丁目55番地
TEL:052-701-2634
FAX:052-701-2637
Mail：info@tramsystem.jp