ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

緊急特集!!

●ワンタイムパスワードを無効化するマルウェア…警視庁が異例の対策乗り出し　（その①）

http://www.nikkei.com/article/DGXLASDG09HA2_Q5A410C1MM0000/
http://www.keishicho.metro.tokyo.jp/haiteku/haiteku/haiteku504.htm
http://mainichi.jp/select/news/20150410k0000e040191000c.html

このニュースをザックリ言うと･･･

- 4月10日（日本時間）、警視庁サイバー犯罪対策課・総務省・Telecom-ISAC Japan等がインターネットバンキングの不正送金を行うマルウェア「VAWTRAK(ボートラック)」について注意喚起を行い、マルウェアの「無力化作戦」を実施したと発表しました。

- 警視庁によれば、今年2～3月の一ヶ月間に行った調査では、VAWTRAKへの感染が確認されたPCは全世界で約82,000台、うち半数以上の約44,000台が日本国内のPCだったとのことです。

- 警視庁等では、感染したPCと直接通信してVAWTRAKを無力化するシステムを開発し、4月より稼働を始めたとしており、捜査機関がこういったシステムによる対策を行うのは世界でも異例とされています。

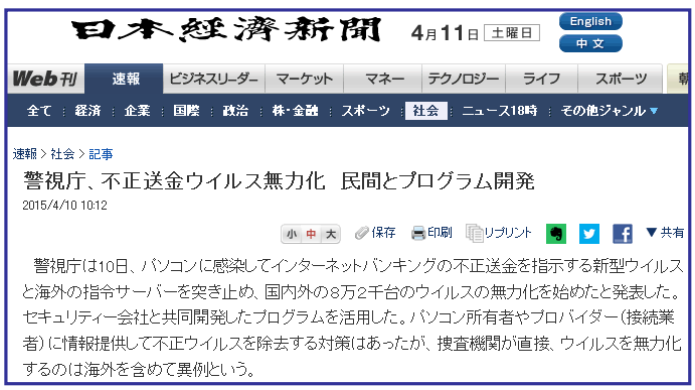
AUS便りからの所感等

- VAWTREKは国内では2014年5月に初めて確認されたマルウェアで、インターネットバンキングへのアクセス時に偽のフォームを表示し、送金時等に毎回生成される「ワンタイムパスワード」をも詐取することにより、不正送金を行うという行動をとるとされています。

- 今回警視庁等が開発したシステムは、VAWTRAKに対し指令を送信するサーバに成り代わり、アクセスしてきたVAWTRAKに対しその活動を停止するような偽のデータを受信させるというもので、これまでのPCユーザへの注意喚起のみの対策から、一歩進んだ直接的な対策を行っていることが特徴です。

- また、ISPの協力のもと、VAWTRAKに感染したPCのユーザに対し、アンチウイルスソフトの導入やOS・各種ソフトウェアのアップデートを行うよう注意喚起を行うとしており、本来必要となる根本的な対策がより確実に行われることが期待されます。

- UTMは、万が一PCがマルウェアに感染し、外部へ不正なアクセスを行うときにそれを食い止める機能を持つものもありますが、やはりそれ以上に、普段からマルウェアに感染する可能性を抑止するために採用されるべきでしょう。


日本経済新聞　4月11日 土曜日　English　中文

Web刊　速報　ビジネスリーダー　マーケット　マネー　テクノロジー　ライフ　スポーツ

全て　経済　企業　国際　政治　株・金融　スポーツ　社会　ニュース18時　その他ジャンル

速報 > 社会 > 記事

警視庁、不正送金ウイルス無力化　民間とプログラム開発

2015/4/10 10:12

小 中 大　保存　印刷　リプリント　共有

警視庁は10日、パソコンに感染してインターネットバンキングの不正送金を指示する新型ウイルスと海外の指令サーバーを突き止め、国内外の8万2千台のウイルスの無力化を始めたと発表した。セキュリティー会社と共同開発したプログラムを活用した。パソコン所有者やプロバイダー（接続業者）に情報提供して不正ウイルスを除去する対策はあったが、捜査機関が直接、ウイルスを無力化するのは海外を含めて異例という。


警視庁 Metropolitan Police Department

警視庁のウェブサイトからさがす　検索開始

トップ / 情報セキュリティー広場 / ネットバンキングウイルス無力化作戦の実施について

ネットバンキングウイルス無力化作戦の実施について

概要

インターネットバンキングの不正送金被害は、昨年（平成26年）一年間で1,876件、被害額は約29億円と過去最悪を記録しており、その手口もますます悪質・巧妙化しています。

今回、警視庁サイバー犯罪対策課では、主に日本を標的としているとみられるウイルスの感染端末に関する情報を入手し、世界で約8万2,000台、うち国内で約4万4,000台の端末を特定しました。

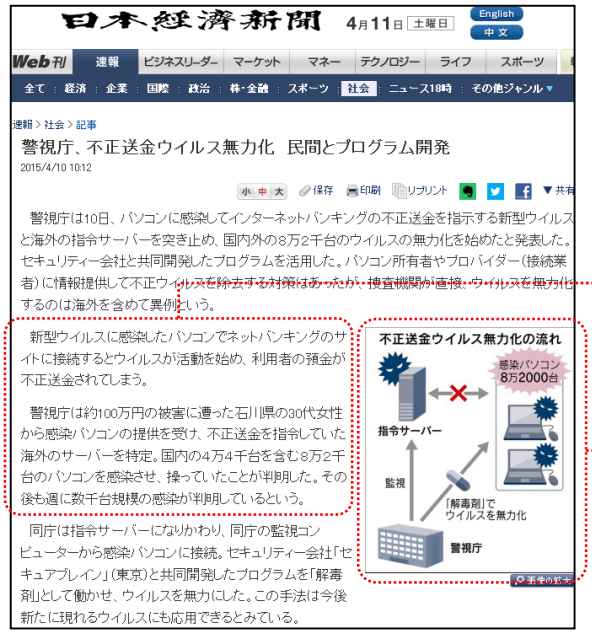
日本独自でこのような大規模なボットネット（ウイルスのネットワーク）をテイクダウン（撲滅）する取組は初めてです。当課ではこれを「ネットバンキングウイルス無力化作戦」と名付け、セキュリティ事業者の協力を得て、ウイルス感染端末の不正送金被害を防ぐための対応策を講じています。

— 次ページに続く —

緊急特集!!

●ワンタイムパスワードを無効化するマルウェア… 警視庁が異例の対策乗り出し （その②）

http://www.nikkei.com/article/DGXLASDG09HA2_Q5A410C1MM0000/
http://mainichi.jp/select/news/20150410k0000e040191000c.html



日本経済新聞 4月11日 土曜日 English 中文

Web刊 速報 ビジネスリーダー マーケット マネー テクノロジー ライフ スポーツ

全て 経済 企業 国際 政治 株・金融 スポーツ 社会 ニュース18時 その他ジャンル

速報 > 社会 > 記事

警視庁、不正送金ウイルス無力化 民間とプログラム開発

2015/4/10 10:12

小 中 大 保存 印刷 リプリント 共有

警視庁は10日、パソコンに感染してインターネットバンキングの不正送金を指示する新型ウイルスと海外の指令サーバーを突き止め、国内外の8万2千台のウイルスの無力化を始めたと発表した。セキュリティー会社と共同開発したプログラムを活用した。パソコン所有者やプロバイダー（接続業者）に情報提供して不正ウイルスを除去する対策はあったが、捜査機関が直接、ウイルスを無力化するのは海外を含めて異例という。

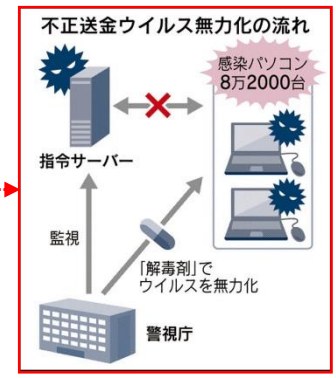
新型ウイルスに感染したパソコンでネットバンキングのサイトに接続するとウイルスが活動を始め、利用者の預金が不正送金されてしまう。

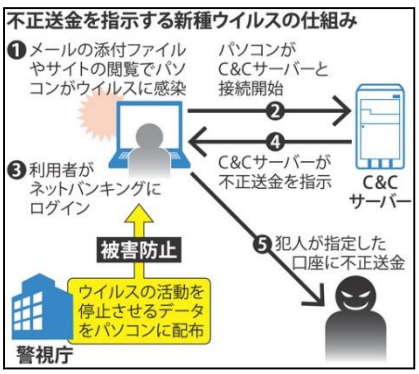
警視庁は約100万円の被害に遭った石川県の30代女性から感染パソコンの提供を受け、不正送金を指令していた海外のサーバーを特定。国内の4万4千台を含む8万2千台のパソコンを感染させ、操っていたことが判明した。その後も週に数千台規模の感染が判明しているという。

同庁は指令サーバーになりかわり、同庁の監視コンピューターから感染パソコンに接続。セキュリティー会社「セキュアブレイン」（東京）と共同開発したプログラムを「解毒剤」として働かせ、ウイルスを無力にした。この手法は今後新たに現れるウイルスにも応用できるとみている。

新型ウイルスに感染したパソコンでネットバンキングのサイトに接続するとウイルスが活動を始め、利用者の預金が不正送金されてしまう。

警視庁は約100万円の被害に遭った石川県の30代女性から感染パソコンの提供を受け、不正送金を指令していた海外のサーバーを特定。国内の4万4千台を含む8万2千台のパソコンを感染させ、操っていたことが判明した。その後も週に数千台規模の感染が判明しているという。





「C&C（Command and Control＝命令と制御）サーバー」

●家庭用ルータへの不正ログインとLAN上の情報収集を行うマルウェア

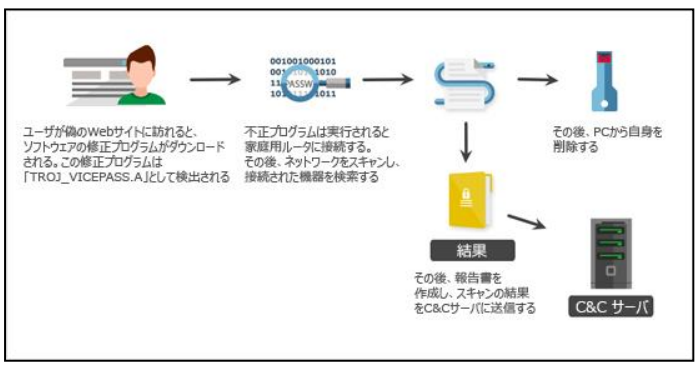
http://internet.watch.impress.co.jp/docs/news/20150330_695355.html

このニュースをザックリ言うと・・・

- 3月30日（日本時間）、トレンドマイクロ社より、家庭用ルータを検索して不正ログインを試行し、またLAN上の機器の情報を収集しようとするマルウェアの存在を確認したと同社ブログにて発表されました。
- 「TROJ_VICEPASS.A」と名付けられたマルウェアは、感染したPCから家庭用ルータの管理画面にアクセスし、ID・パスワードのリストを元に不正ログインを試行、そしてログインに成功した後にネットワークのスキャンを行って機器情報を外部に送信するという行動をとるとされています。
- 同社では、「一見標的にならなそうな機器も保護される必要性」があるとし、ルータの管理画面のパスワードを初期設定から変更するよう呼びかけています。

AUS便りからの所感等

- ルータをはじめとするネットワーク機器およびその管理画面については、必要のない限り外部からアクセスできないようにすることはもちろんですが、万が一マルウェアに感染して内部からアクセスされる可能性も決して見過ごしてはいけないものです。
- パスワードの変更に加え、内部ネットワークからのアクセスについても何らかの制限を行う機能があれば、可能な限り有効にすべきでしょう。
- 一方で、こういったマルウェアに感染しないためには、アンチウイルス・UTM等による防御も欠かせないものとなります。



「TROJ_VICEPASS.A」の感染フロー