セキュリティ関連ニュース

銀行口座を狙うウイルス「SpyEye（スパイアイ）」に注意呼びかけ（IPA）

情報処理推進機構セキュリティセンター（IPA/ISEC）は5日、8月のコンピュータウイルス、不正アクセスの届出状況のまとめを発表した。また、今年6月から7月にかけて発生したネットバンキングの不正利用事件について、ウイルス「SpyEye（スパイアイ）」が原因となっている可能性があるとして、SpyEye対策について解説し、注意を呼びかけている。

■8月のウイルス/不正アクセス届出状況

8月のウイルス検出数は約2.5万個で、7月（2.3万個）から9.6%増加した。届出件数は931件で、7月（1064件）から12.5%減少している。検出数1位は W32/Netsky（1.4万個）、2位はW32/Mydoom（9000個）、3位はW32/Autorun（600個）。不正プログラムの検知状況は、7月には動きがなかったが、8月には別のウイルスを感染させようとするDOWNLOADERなどが増加傾向をみせた。

不正アクセスの届出件数は10件（うち被害あり8件）、不正アクセスに関連した相談件数は37件（うち被害あり13件）だった。被害届出があった8件の内訳は、侵入7件、DoS攻撃1件。侵入被害は、メールアカウントを外部から勝手に使われて迷惑メール送信に悪用されたもの1件、Webページが改ざんされたもの1件、データベースからクレジットカード情報が盗まれたもの1件、外部サイト攻撃の踏み台に悪用されたもの3件、他は詳細不明。侵入の原因は、ファイアウォールの設定不備1件、IDやパスワード管理不備と思われるもの1件、Webアプリケーションの脆弱性を突かれたもの1件で、他は原因不明。

ウイルスや不正アクセス関連の相談総件数は1651件（7月1490件）。うち「ワンクリック請求」関連が535件（7月461件）、「偽セキュリティソフト」関連が7件（7月8件）、Winny 関連が7件（7月7件）。7月に2件あった「情報詐取を目的として特定の組織に送られる不審なメール」関連は0件だった。

■銀行口座を狙うウイルス「SpyEye」の動作と対策

IPAは先月3日にも、ネットバンキングの不正アクセス被害に注意を喚起しているが、今回は原因と目されるウイルス「SpyEye」の一種（v1.3.45）を入手し、解析を実施。現時点で判明している解析結果を基に、SpyEye対策を解説している。SpyEyeはインターネットバンキングで使われるIDとパスワードの窃取を目的としたウイルスで、IPAはSpyEye感染後の動作として次の2点を確認している。

・利用者が閲覧中のWebサイトで入力したIDとパスワードを窃取する
・窃取した情報をネット経由でウイルス作成者が管理するサーバーに送信する

SpyEyeはボットネット機能をもっており、ウイルス作成者がネットを通じて感染させたSpyEyeを新しいウイルスに置き換えることができる。ウイルス対策ソフトで検知できない新種ウイルスに置き換え続

セキュリティニュースTOPICS

- 無視してはいけない「ブラウザの警告」～ウイルス感染防止編

ニュースバックナンバー

So-netのセキュリティ関連サービス

- **《So-netの総合セキュリティ対策サービス》**
- ・マカフィー・セキュリティスイート

525円(税込)／月

- (各機能ごとのご契約)
- ・マカフィー・ウイルススキャン
- ・マカフィー・パーソナルファイアウォールプラス
- ・マカフィー・アンチスパム

各263円(税込)／月

- **《お子様を有害情報から守る》**
- ・有害サイトブロック

セキュリティ関連サービス一覧>>

セキュリティ通信 TOP

けることで、長期間感染させ、必要な情報を窃取することが容易になる。

SpyEyeの主な感染手口としては、「Webサイトからダウンロードさせる」「メールで送りつける」の2つが考えられる。前者は閲覧しただけで不正プログラムをダウンロードさせる「ドライブバイダウンロード」攻撃で、利用者のパソコンのOSやアプリケーションの脆弱性が悪用される。後者は添付ファイル付きメールを送り、添付ファイルを開かせて感染させる手口で、最近は関係者を装って送りつける「標的型攻撃」メールも多い。

上記をふまえ、IPAはSpyEye対策として、次の4項目をあげている。

(1) OSやアプリケーションソフトの脆弱性を解消する
(2) ウイルス対策ソフトでウイルスの侵入を防止する
(3) 簡単にメールの添付ファイルを開かない
(4) IDやパスワードを使い回さない

不幸にも感染してしまった場合は、最新状態のウイルス対策ソフトでウイルスチェックを行う。それでも発見されない場合、駆除したにもかかわらず正常に動作していないと思われる場合などは、パソコンの初期化を行う必要が出てくる。感染のみならずネットバンキングの不正利用被害にあってしまった場合は、利用銀行へ問合わせることが第一だ。この際、ウイルスに感染していない自分の安全なパソコンから、ネットバンキングで使用しているパスワードを変更する必要がある。

(2011/09/06 セキュリティ通信)

【関連URL:IPA】
・コンピュータウイルス・不正アクセスの届出状況[8月分]について
http://www.ipa.go.jp/security/txt/2011/09outline.html

【関連URL:セキュリティ通信】
・ネットバンキングで不正アクセスが増加し実害も発生、IPAが注意呼びかけ(2011/08/04)

その他のニュース

- 10/05 深刻な脆弱性を修正した「Google Chrome」公開～Flash Playerも最新版に
- 10/04 標的型攻撃～メール受信者が騙されるテクニックを分析し、対策提案(IPA)
- 10/03 海外タイヤ通販サイトに不正アクセス、カード情報聞き出す不審メール出回る
- 09/30 違法な医薬品のネット販売、国際刑事警察が世界81か国で一斉取り締まり
- 09/29 著作権法違反:ネットオークションで海賊版販売/アニメ無断公開
- 09/29 追補:「Firefox 7.0/3.6.23」で修正された脆弱性とアドオンが消える不具合
- 09/28 モジラ、複数の脆弱性を修正した「Firefox 7.0/3.6.23」を公開
- 09/27 SSL/TLSに情報漏えいの脆弱性～マイクロソフトがアドバイザリ公開
- 09/26 三菱重工業など防衛関連企業狙うサイバー攻撃～トレンドマイクロが手口分析
- 09/26 ボットが仕掛けた韓国へのサイバー攻撃～国内のパソコン関与が判明