個人を狙ったウイルスの最新動向

NTTコミュニケーションズ
株式会社
ソリューションサービス部
第二ソリューション部門
スマートセーフティソリューション担当
主査
おおむら　すぐる
大村　優

NTTコミュニケーションズ
株式会社
ソリューションサービス部
第二ソリューション部門
社会基盤ソリューション担当
主査
た なか　あきふみ
田中　昭文

NTTコミュニケーションズ
株式会社
ソリューションサービス部
第二ソリューション部門
スマートセーフティソリューション担当
か とう　じゅん や
加藤　淳也

はじめに

今日、インターネットは我々の生活を支える重要なインフラのひとつとなっているが、その一方で、不正アクセスや悪意のあるソフトウェア（ウイルスなど）によるインターネットを利用した様々な犯罪行為が増加している。かつてのウイルスはパソコンの画面に花火を表示したりハードディスク上のファイルを消去したりといった愉快犯的な活動であったが、その後、迷惑メールの送信やDDoS攻撃などに使われるボット等のウイルスは犯罪組織の情報詐取などに利用されるケースが増えてきている。

このボットは、パソコン利用者に気づかれないよう密かに感染活動をする、またウイルス対策ソフトに検知・駆除されない多くの亜種が短期間で発生するという特徴があり、パソコンの利用者が対策を行うことが非常に難しくなってきた。そのため、ボット対策をパソコン利用者自らの対策だけに委ねるのではなく、国が主導してISPやセキュリティベンダ、セキュリティ関連機関等と連携したボット対策を推進してきた。「サイバークリーンセンター」は、こうした背景のもと、国内ボット感染者を限りなくゼロにする取組として、2006年度より総務省・経済産業省連携プロジェクトとして開始され、ISPと連携した注意喚起活動を中心としたボット対策活動を進めたものである。この活動により、国内ユーザにおけるボット感染率は減少し、一定の成果を上げた。

しかし最近では感染活動が更に複雑化しており、検知がより困難なウイルスが発生している。手口としては、電子掲示板を通じて、個人のパソコンに遠隔操作ウイルスを感染させ、そのパソコンを乗っ取り、パソコンのユーザになりすましてインターネットを通じて襲撃・殺害予告の書き込みを行う事象がある。また、個人のパソコンを何らかのウイルスに感染させ、そのパソコンを利用したユーザがインターネットバンキング等のオンラインでのサービスへログインした後、更に追加で暗証番号や秘密の質問、顧客情報等を入力させるポップアップを表示させることで、不正に情報窃取する事例も発生している。このように、インターネット利用ユーザをターゲットにした悪質な犯罪が増加しており、被害に遭わないよう注意が必要な状況となっている。

そこで本稿では、その一例として、「遠隔操作ウイルス感染事例」「インターネットバンキングを狙った情報搾取事例」などの事例を紹介し、その対応策を解説する。

1．遠隔操作ウイルス感染事例

2012年、個人を狙ったウイルスで大きな注目を浴びたのが、いわゆる「遠隔操作ウイルス」事件である。同ウイルスを用いて他人のパソコンを勝手に遠隔操作する「なりすまし」により、公共機関のWebサイトや掲示板に襲撃や殺人などの犯罪予告が書き込まれ、ウイルス感染PCの所有者4名が誤認逮捕されるなど、報道やメディア等でも大きく取り上げられ社会問題にも発展した。

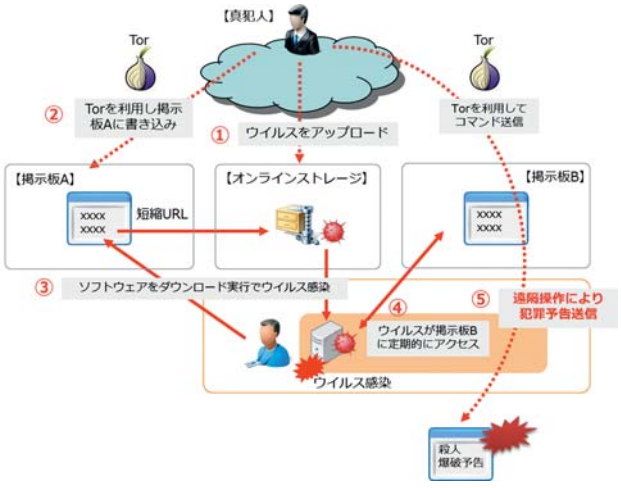

図1．遠隔操作ウイルス概要

今回の事件で、攻撃者（真犯人）がウイルスを感染させるために用いた手法は、あらかじめウイルスを仕込んだソフトウェアを、オンラインストレージサービス上に配置し、インターネット上の掲示板にそのソフトウェアをダウンロードするためのリンク（誘導URL、実際に用いられたものは短縮URL）を書込むというものである。誤認逮捕された4名のうち、遠隔操作ウイルスに感染の疑いのある3名は、たまたま掲示板に書き込まれたリンクをクリックし、ソフトウェアをダウンロード、実行することで感染に至っている。

感染経緯や感染経路は上記のとおりであるが、このウイルスは、感染したPCを別の無料レンタル掲示板経由でコントロールし、真犯人からの命令に従い、遠隔から今回の事件で行われた犯罪予告の送信等を行わせることが可能になっている。このように、ウイルスに関してはインターネット経由で遠隔操作ができるという特徴を持っていることから、「遠隔操作ウイルス」あるいは「なりすましウイルス」と呼ばれることが多いが、決して特別なウイルスというわけではない。ウイルスの世界では、バックドア型やトロイの木馬型に分類され、出回っている多くのウイルスには、同様の機能が組み込まれているものが非常に多い。ボットや、昨今の標的型攻撃で利用されるウイルスなど、感染したPCを遠隔操作することができるウイルスは決して珍しいものではないのである。

また、今回の事件で用いられたウイルスは、真犯人が自作したものとされるが、同様のウイルスを専門のプログラミング知識がなくても容易に作成できるツールキットや、もともとPCを遠隔管理する目的で利用するRAT（Remote Administration Tool）を悪用してウイルスを作成する手法など、ウイルス作成の敷居は確実に下がっており、これらのことが今日のウイルス増殖に拍車をかけていると言える。

一方、今回の事件では、掲示板への書き込みやウイルスに感染したPCに対する命令の送信等について、発信元を隠ぺいする匿名化技術が使われていることが特徴である。具体的には、Tor（The Onion Router、https://www.torproject.org/）と呼ばれる接続経路の匿名化を行うフリーのソフトウェアの利用が濃厚であると言われている。

Torは、無作為に選ばれた複数の中継ノードを経由して宛て先との通信を行うが、中継ノード上にログを残す機能がないことや、出口以外の通信路が暗号化されること、さらに一定時間ごとに通信経路も変更されるなどの特徴を持っている。このため、送信元や通信経路を追跡することが非常に困難になり、真犯人特定を難しくしている要因にもなっている。現在のTorにおけるノード数の状況については、TorProject

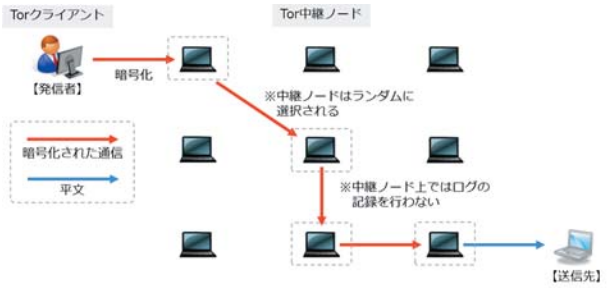

図２．Torの特徴

のホームページ上で公表されており、全世界で3,000台以上、日本でも数十台以上が稼働している状況にある。

このように、今回の遠隔操作ウイルス事件では、IPアドレスによる送信元特定に頼った捜査手法の在り方、ウイルスによる犯行であることを立証することの難しさ、そもそもウイルス感染を防ぐこと、及び気付くことの難しさなど、今まで明るみにならなかった脅威が現実となったことで、改めてサイバー犯罪に対する課題が浮き彫りになったと言える。

２．インターネットバンキングを狙った情報搾取事例

2012年、個人を狙ったウイルスのもう一つ特徴的な事例が、インターネットバンキングを狙った情報搾取に関する事件である。インターネットバンキング利用者を標的にした事件であるが、具体的な手口は、利用者がインターネットバンキングサイトに正規な手順でログインした後、偽装したポップアップ画面を表示し、第二暗証番号や秘密の質問、顧客情報等を不正に搾取するというものである。

この一連の事象により、金融機関への報告では400件以上の不正ポップアップ表示と、一部の金融機関においては、顧客口座から別口座に対して実際に不正送金・出金が行われていたことが確認されている。この事件でも、不正ポップアップ表示にウイルス感染したPCが利用されており、各金融機関から注意喚起が行われる事態となっている。

金融機関を狙った攻撃は、従来のフィッシングやキーロガーが代表的なものとして挙げられるが、今回の事件の特徴は、利用者が正当な手順によりインターネットバンキングサイトにログインした状態で不正なポップアップが表示されるという点である。通常のフィッシング詐欺とは異なり、接続したURLはあくまで正規サイトであり、URLから不正であることを判断することが不可能となる。具体的な手口としては、ウイルスがブラウザの正常なセッションを監視し、本物のWeb

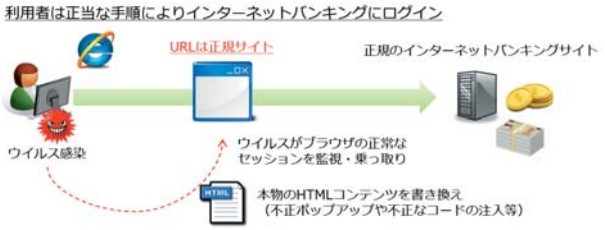

図３．HTMLインジェクション

ページ（HTML）を置き換えるという、HTMLインジェクションあるいはWebインジェクションと呼ばれる攻撃手法が利用されている。

今回の攻撃で特に脅威となる部分は、各金融機関で採用されている乱数表を用いた暗証カード等による、いわゆる二要素認証を突破できてしまう点である。このようなウイルスの事例は、欧米では数年前から報告されており、金融機関を狙ったウイルスとしては、Zeus/SpyEyeと呼ばれるものが特に有名である。Zeus/SpyEyeは、ウイルスを作成するツールキットの一種であり、指令サーバを介したボットネットを構成、攻撃者からの指令を待ち受けて動作する。Zeusについては、2011年5月にソースコードが流出しており、このコードを利用して同様のウイルスを作成することが可能になっている。このような背景もあり、今回の国内の事例でも、各金融機関で一斉に事象が発生していることや、各銀行の認証方式を十分に調査し、各銀行に応じた巧妙な画面をあらかじめ作成している点などから、同様のウイルスの使用が疑われており、実際にアンチウイルスベンダの報告によると、Zeusの一種として検知されるとの報告がある。今回の日本国内のケースでも、既にウイルス感染しているPCに対して、指令サーバ経由で攻撃者側から一斉にアップデートが行われ、情報搾取に利用されたのではないかと推察される。言い換えれば、日本国内でも同種のウイルス感染者が多数存在していることを意味しており、実際に不正なポップアップが表示される場合は、何らかのウイルスに感染している可能性が非常に高いと言える。

このように、金融機関を狙ったウイルスについては、攻撃自体が高度化しているが、利用者自身のウイルス感染の経緯や感染経路が明らかになっておらず、感染者は引き続き攻撃に利用される可能性が高いので、早急なウイルス駆除が求められる。

3．エンドユーザにおける対策

今回の遠隔操作ウイルスやネットバンキングを狙ったウイルス感染の対策を**表1**にまとめる。

表１．ウィルス感染の対策

ソフトウェアによる対策	
	①OSとアプリケーションのアップデート
	②ウイルス対策ソフトの導入とパターンファイルの最新化、リアルタイムスキャンと定期的なフルスキャンの併用
ユーザ個人の判断による対策	
	①信頼の置けるサイトから信頼できるアプリケーションのみインストール
	②不審なサイトに不用意にアクセスしない
	③身に覚えがないメールに添付されたファイルやメール本文中のURLを不用意にクリックしない
	④ネットバンキングで必要以上に個人情報を入力させる入力画面がないか確認

ソフトウェアによる対策としては、Windowsをはじめとする各種OSとアプリケーションのアップデートとウイルス対策ソフトによる対策である。特にアプリケーションに関してはAdobe Flash Player、Adobe Reader、Java Runtime Enviroment、Microsoft Officeの脆弱性を利用したウイルス感染が多いので、確実にアップデートを行う必要がある。IPAのMyJVNバージョンチェッカ(http://jvndb.jvn.jp/apis/myjvn/vccheck.html)を利用すれば、バージョンが最新であるか簡単に確認することができる。

ウイルス対策ソフトは、世の中で初めて作成されたウイルスを検出することは難しいが、ウイルスによる被害が発生すればウイルス対策ベンダが検体を入手しパターンファイルを作成するので、その後に続く拡大感染フェーズのウイルスを検出する上で有効である。

ただし、ウイルス対策ソフトによる対策にはある程度時間を要することを理解しておきたい。今回の犯罪予告のケースでは、遠隔操作ウイルスを利用した最初の犯行予告が、2012年7月29日であり、遅くともこの時点で犯罪に利用されたPCは遠隔操作ウイルスに感染していた。それに対して大手の主要なウイルス対策ベンダが、パターンファイルを作成しリリースしたのは2012年10月10日前後であり、少なくとも２か月と数日間、遠隔操作ウイルスを検出できなかった。これは事件当初、PC所有者による犯行予告と誤認され、真犯人

によるウイルスを介した犯行予告と認知されるまでに時間がかかったためと考えられる。

このように新しいウイルスによる被害が発生してから、そのウイルスを検出するパターンファイルの配信までタイムラグがある。パターンファイルを最新の状態に更新し、リアルタイムスキャンと併せて、1週間に1回など定期的にPCのフルスキャンを実施することも有効である。これは、タイムラグにより遅れて配信されたパターンファイルが、以前からPCに潜伏していたウイルスを検出する可能性があるためだ。

次にユーザ個人の判断による対策を述べる。ウェブサイトからアプリケーションを探してインストールする際は、信頼のおけるサイトから信頼できるアプリケーションと判断できた場合に限りダウンロードすることが対策となる。特に誰でもファイルをアップロードできるオンラインストレージサービス等のサイトから、作成者が分からないアプリケーションをダウンロードしてインストールすることは危険である。

また、アプリケーションをインストールする前にVirusTotal(https://www.virustotal.com)等の複数のウイルス対策エンジンを用いてファイルを検査してくれるウェブサービスを利用し、アプリケーションがウイルスでないか確認することも有効だ。これは、PC上のウイルス対策ソフトでは検出できなかったウイルスを、別のウイルス対策ソフトが検出してくれる可能性があるためである。

ウェブを閲覧する際は不審なサイトに不用意にアクセスせず、特にリダイレクト先が分かりづらい短縮URLは、悪用されるケースが多いので、不審なサイト上でクリックする際は特に注意が必要である。どうしてもアクセスする必要がある場合は、短縮URLを展開してリダイレクト先のURLを表示するウェブサービスや、aguse gateway(http://gw.aguse.jp)等のアクセスしたいウェブページを画像として表示してくれるウィブサービスを利用するとよい。

メールを利用する際は、身に覚えがないメールに添付されたファイルや、メール本文中のURLを不用意にクリックしてはいけない。

ネットバンキングを利用する際は、今までのログイン情報と比較して、必要以上にIDやパスワード、顧客番号、暗証番号、質問、合言葉などの個人情報を入力させる入力画面が表示されていないか確認し、表示された場合は、入力をせず金融機関等へ相談する必要がある。

まとめ

本稿では、「遠隔操作ウイルス感染事例」「インターネットバンキングを狙った情報搾取事例」などの事例を紹介し、その対応策を解説した。

ここでの課題としては、パソコンの利用者の多くが十分なセキュリティ対策を行っていないことで、インターネット犯罪に巻き込まれてしまうことである。最終的にセキュリティ対策を行うのはユーザ自身にほかならない。そのためにはユーザ一人一人がセキュリティ意識を高めていくとともに、テレビ、新聞、雑誌等のメディアで発信されている様々なセキュリティ情報や最新動向を継続的に確認していくことが重要である。