

SQLインジェクション

フィッシング

インターネット

闇経済レポート



ボットネット

情報漏えい

DDoS攻撃

スパムメール

マルウェア

新聞に載るような事件が少なくなっていることもあり、多くのユーザーはセキュリティ問題への関心がやや薄れているように見受けられます。しかし、これは「攻撃の見えない化」が進んだだけで、実際は凶悪な犯罪に知らないうちに巻き込まれている可能性も高いのです。本稿ではシマンテックが調べた最新の情報を基に、昨今の攻撃の傾向やそれを行なう犯罪者たちの実態、詐取される対象、アンダーグラウンドのマネーの動向などを解説します。

文●株式会社シマンテック シニア セキュリティレスポンス マネージャ 浜田譲治 編集●大谷イビサ

大きく変わりつつある インターネットの攻撃



今から数年前、英文メールを当たり前のように受け取るようになった経験はないでしょうか？ または、パソコンのパフォーマンスが低下したり、いきなりパソコンが不安定になったり、場合によっては自動的に再起動がかかったり

しなかったでしょうか？ このような嫌がらせの攻撃に振り回された経験は、筆者も数え切れないほどありました。

では近状はどうなのでしょう？ 最近では以前のように英文メールも大量に受信しないですし、パソコンの不具合も発生することが少なくなっています。最近ではウイルス添付メールを受け取るケースが減っているかもしれません。

攻撃により、パソコンがクラッシュすることが減ってないでしょうか？ こうしたことから、自分はコンピュータウイルスとは無縁と思っている方も増えているかもしれません。しかし、過去の攻撃手法と違って、近年のインターネット攻撃は巧妙化しており、感染や侵入の形跡を残さないのが特徴です。

こうした攻撃を仕掛けているサイバ



一犯罪者が現在どのように活動しているのでしょうか。サイバー攻撃の結果、盗まれるクレジットカード番号、銀行口座やオンライン銀行のIDとパスワード、メールアカウント／パスワードを含む個人情報や攻撃ツールなどが闇市場で売買されています。どのようなものがどう取引されているか、また、その市場規模といった実態を紹介していきます。

マルウェア登場の背景

では、ここで少しコンピュータウイルス（以下マルウェアと記述）を中心にインターネット攻撃の歴史に触れてみます。もともとマルウェアは1980年代に誕生し、悪戯心を持つ人たちが作成していました。コンピュータネットワークが普及する前の時代でしたので、フロッピーディスクから感染するものがほとんどでした。それからパソコンが普及するとともに徐々に進化し続け、2000年台にはメール感染やネットワーク感染するようなマルウェアが登場しました。これらは多くのインターネットの利用者は出会ったことがあるのではないのでしょうか。

当時のマルウェアの作成者の意図は、自分の能力が世の中でどのくらいの騒ぎを起こせるか試したかったわけです。その点、完全な愉快犯といえるでしょう。なかには作成者同士が、スキルを競い合いケンカまでしていることもありました。お互いのマルウェアを削除したり、侮辱のコメントをマルウェアのコードの中に挿入したりするわけです。

もちろん、感染したユーザーにとってはただ単に嫌がらせにすぎないもので、感染した場合はメーラのアドレス帳に登録されているユーザーに拡散し、

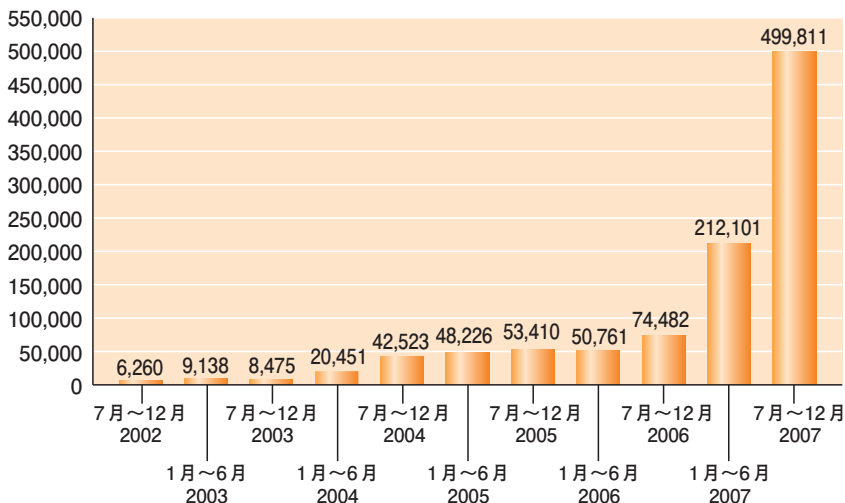


図1 新たに発見されたマルウェアの件数

周囲に迷惑をかけたり、恥ずかしい思いをした方もいらっしゃるでしょう。システム管理者にとっては大変な時代であり、マルウェアは無差別に拡散しているため、企業ネットワーク内に1台でも感染があるとそれが一気に広がったため、駆除の作業で追われた日々を過ごすはめになっていました。実際、基幹サーバに感染し、業務の停止に至るケースもありました。

しかしながら、今のマルウェア、インターネット攻撃は違う形でインターネット利用者に影響を与えるようになっており、状況は一変しています。もはや愉快犯ではなくなり、現在は金銭目当ての目的と変化したのです。金銭目的のため、攻撃も巧妙化、悪質化してきています。

たとえば、自身を巧妙に隠すマルウェアです。以前のようにマルウェアが表に堂々と現われると即座に発見されてしまいますので、それでは次の活動につなげなくなります。次の活動というのはパソコン利用者の個人情報を盗むことです。また万が一、形跡が見られても、駆除が困難になっています。さ

らに、パソコン利用者を騙す方法が巧妙になっているのです。マルウェアによっては感染が自動化され、正規のホームページを見るだけで感染する攻撃が一般化しつつあります。

また、マルウェア以外にもフィッシング攻撃も誕生しました。これは一般のパソコン利用者にとってはかなりの脅威でしょう。知らないうちに攻撃され、個人情報盗まれるわけです。

そして、重大な変化はマルウェアの数が膨大に増加していることです。以前は少数のマルウェアが一斉にインターネットに増殖し騒ぎを起こしていましたが、今はまったくその逆で、多数のマルウェアが密かに活動しパソコンの中に悪質な行為を行なっているわけです。マルウェアがウイルス対策ソフトから1つでも多くすり抜けるように量が増えてきたこともあります。

シマンテックの調査によると、2002年の上半期には6260の新しいマルウェアが発見されました。それが2007年の上半期にはなんと49万9811にまで増加しています(図1)。このように、さまざまに形を変えながらインターネットの

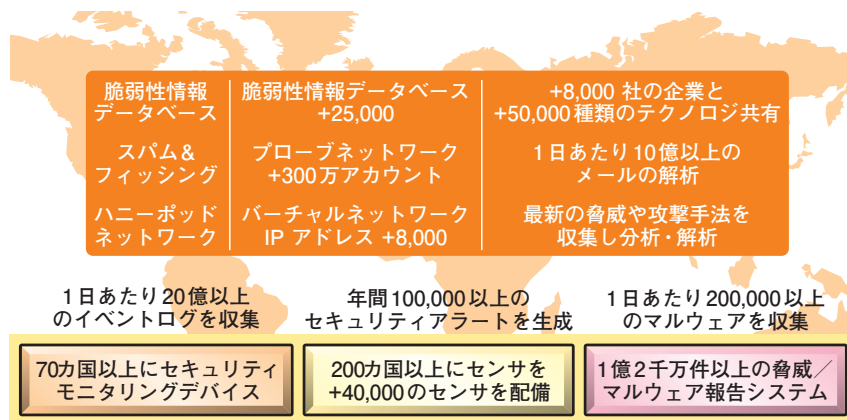


図2 シマンテックのGlobal Intelligence Network

攻撃は進化し、金銭を得ようとしているのです。

シマンテックの活動とレポートの概要



こうした実態を掴むため、シマンテックは情報収集ネットワークのGlobal Intelligence Networkを基に闇市場の調査を行ないました。Global Intelligence Networkは、70カ国以上の顧客ネットワークでの24時間365日体制の監視、200を超える国でのネットワーク活動を監視している4万基以上のセンサ、シマンテックのセキュリティ対策製品を使用している1億2000万台以上のクライアント/サーバ/ゲートウェイから収集した情報で構成されている情報収集基盤を指します(図2)。

また、Probe Networkというシステムも運営していますが、こちらは200万以上のおとりメールアカウントを設け、世界20カ国からメールを収集して世界中のスパムおよびフィッシング行為を計測しています。要はさまざまな監視装置を通じてマルウェア、スパム(迷惑)メール、フィッシング、ソフトウェアの脆弱性、ネットワーク攻撃などサイバー犯罪に関連する情報を総合的に収集し、

インターネット上の安全性をつねに把握しているわけです。シマンテックはこのGlobal Intelligence Networkを通じて定期的にセキュリティ調査レポートを発表しています。

2008年の11月には『シマンテック アンダーグラウンドエコノミーレポート』を発表しました。これはインターネットの闇市場においてサイバー犯罪を調査したレポートです。同レポートによると2007年7月1日から2008年6月30日までの1年間を観察した結果、闇市場で宣伝されていた商品の総価値は2億7600万ドル(約255億7000万円)を超えたと推定されています(以下、すべて米ドル)。これはあくまでも、闇市場の一面について分析を試みただけに過ぎないものであり、実際の規模はさらに大きいものでしょう。では、これからレポートの内容を細かく紹介していきます。

闇経済は自給自足的なシステムである



インターネットの闇市場は現在、自給自足的なシステムまで成長しています。以前のサイバー犯罪者は多くの方々が想像されるいわゆる「ハッカー」でありま

した。暗い部屋の中で1人のコンピュータオタクがコツコツとキーボードを打ちながら、攻撃を仕掛けるようなイメージがあるでしょう。ですが、実際のサイバー犯罪者たちはこのような人たちだけではありません。深い技術力がなくても、ある程度の資金さえあれば、昔のサイバー犯罪者と同様の攻撃ができてしまうからです。また、資金力によっては、今まで以上に大規模な犯罪を起こすことも可能なのです。現在の闇市場は、自給自足の市場まで成長しています。

闇市場の1つの資金の流れを見てみましょう(図3)。まずは罪を犯してまでお金に対して意欲がある人物の登場から始まります。仮にサイバー犯罪初心者であると仮定して、この人物はどのような手口を利用して金銭を得るかを考えます。この選択肢は自分のスキルや経験や資金力に応じて絞られるようになるでしょう。

彼はサイバー犯罪には経験が浅いので、マルウェア作成ソフトを購入することに決めました。そして、このソフトを利用し、オンラインショッピングをするユーザーからクレジットカードのアカウント情報を盗むマルウェアを作成します。項目を入力して、設定を指定して、ボタンをクリックする程度で作成できてしまうので、プログラミング経験がなくても使用できます。

さて、マルウェアは完成しましたが、これをどう利用してクレジットカード情報を収集したらよいのでしょうか?

次はマルウェアの配布の手段を選ばないといけなわけです。候補としては、いくつかあります。スパム業者を雇って、ボットネットを介して作成したスパムメールを配信する。またはホ