マルウェアの傾向から見るインターネットセキュリティの動向

悪意を持って作られた機能を持つソフトウェア、いわゆるマルウェアが今日のインターネット世界において、極めて大きな脅威となっている。本稿では、JPCERT/CC シニアアナリストである椎木孝斉氏、さらにはJPCERT/CC理事である真鍋敬士氏が、脅威の変化とマルウェアの変化傾向に注目し、現在のインターネットにおける脅威とその対策について解説する。

椎木　孝斉
(Takayoshi Shiigi)
有限責任中間法人JPCERTコーディネーションセンター
シニアアナリスト

CISSP、CISA、ISMS審査員補。2003年より東芝および東芝ソリューションにて情報セキュリティサービスに従事。2005年有限責任中間法人JPCERTコーディネーションセンター(JPCERT/CC)情報流通対策グループマネージャを経て、現在はJPCERT/CCシニアアナリスト。

真鍋　敬士
(Takashi Manabe)
有限責任中間法人 JPCERTコーディネーションセンター
理事

ノーザンライツコンピュータ、テンアートニ　シニアマネージャを経て、2000年からJPCERT/CC運営委員。現在は、JPCERT/CC理事（2002年～）のほか、サイマル取締役（2004年～）、首都大学東京 産業技術大学院大学 情報アーキテクチャ専攻 非常勤兼任講師（2006年～）も務める。

脅威の変化はマルウェアに現れる

2001年、それは悪意を持って作られたソフトウェアがインターネットにおいて大きな脅威になることが実証された年であった。

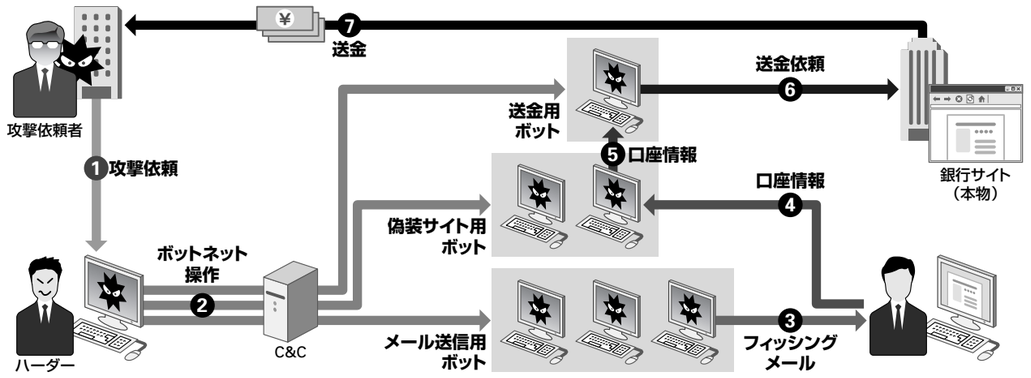
同年夏に爆発的に広まったCodeRedは随所でネットワークインフラを麻痺させた。続いて登場したNimdaに対してはCodeRedで得た教訓が活かされたものの、セキュリティ対策の裾野を一般ユーザーまで広げることの困難さを実感することになった。

この2001年頃にはインターネットは既に普及期に入っていたが、インターネット上に存在する資産として最も価値のあるものはインターネットそのものであった。つまり、インターネットにおいてはネットワークやコンピュータ等のインフラへの攻撃が最も大きな脅威であった。

その後、オンラインショッピングや著作物、個人情報や機密情報等、インターネットを介して交換される資産の価値が高まるにつれて、脅威も自己顕示を動機とするものから現実社会における犯罪に近いものへと変貌を遂げて来た。

攻撃に使われる道具の変化を追いかけることで脅威の変化が見えてくる。ここでいう道具とは悪性のソフトウェア、つまりマルウェアである。本稿ではマルウェアの傾向に注目するとともに、現在のインターネットにおける脅威とその対策について紹介する。

図1　ボットネットを利用したフィッシング詐欺



攻撃インフラとして実用化されるボットネット

近年、インターネットにおける脅威として注目されているのがボットネットである。ボットネットという名前はIRCの自動対話プログラムが“bot”と呼ばれていたことに由来する。botはもともとマルウェアとして世に現れたものではないが、当初から悪用されることが多かった。

今日のような攻撃ネットワークとしてのボットネットは2004年ころから注目されるようになった。ボットネットにおいて個々のボットはC&C（Command and Control）サーバと呼ばれるコンピュータの管理下にあり、ハーダー（HEADER）あるいはマスター（MASTER）と呼ばれる指令者によって運用されている。

技術的に注目すべき特徴は、ボットネットが分散システムとして構成された攻撃インフラであるという点である。インターネット上に散在するボット化したコンピュータを活用することで、攻撃の量的能力や可用性を高めるだけでなくアクセス制限をすり抜ける可能性を高めることができる。攻撃インフラのボトルネックになり得るC&Cサーバについても多重化、多段化により冗長性を維持しようとする試みが見られる。

また、ボットネットには指令者に攻撃を発注する第三のプレイヤーが存在するといわれている。攻撃の動機を持った者が台数や時間を単位に販売されているボットネットをサービスとして購入するという構図である。これはつまり、ネットワークやコンピュータに関する知識がない人間でもボットネットを利用して攻撃を行うことができるということを意味する。これもボットネットが注目される大きな特徴である。

図1はフィッシング詐欺の流れを例示したものである。フィッシング詐欺を企てるためには偽装サイト用のサーバと、偽装サイトへ誘導するためのフィッシングメールを送信するサーバが必要になる。

偽装サイト用のサーバは侵入して確保することができるかも知れないが、手間のわりにリスクが高い。ボットネットを利用すれば、ひとつの偽装サーバが止められてもすぐに代替を立ち上げることができるし、アシがつきにくい。フィッシングメールについてもボットネットを使うことでメールの送信能力が増すだけでなく、OP25B（Outbound Port 25 Blocking）のような制限を回避してより効果的に送信することができるようになる。このように、ボットネットを利用することで従来からある攻撃をより確実に実施できるようになるのである。

巧妙化する侵入手口

今日のマルウェアの多くはネットワークを介して積極的にコンピュータに侵入する手段を持っている。主な手段としてはソフトウェアの脆弱性を悪用して侵入する方法と、ソーシャルエンジニアリング的手法を用いてメールやWebを介して侵入する方法がある。ソーシャルエンジニアリング的手法というのは、人の関心や錯覚を利用する方法であり、いわば「人間の脆弱性」を突く方法である。

最近のマルウェアは侵入の成功率を高

図2　ダウンローダによる多段化

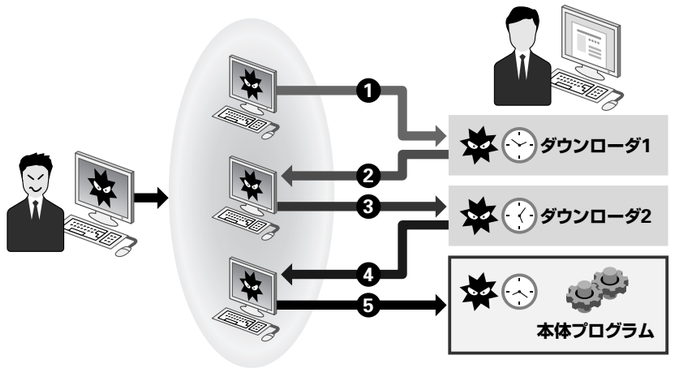
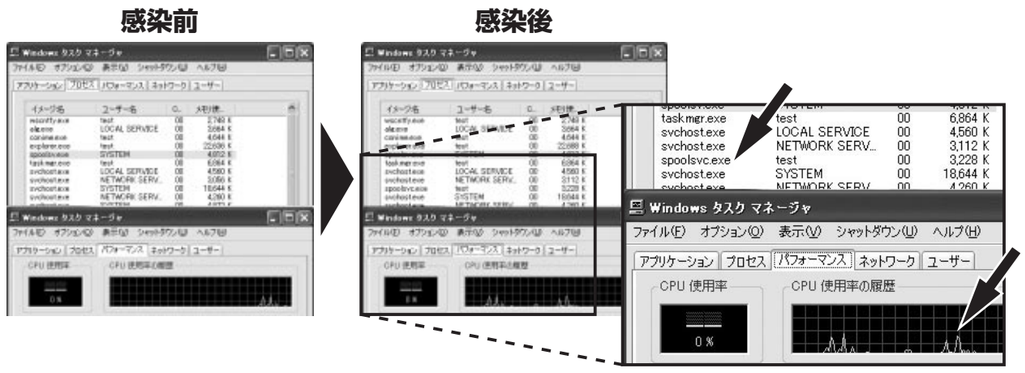


図3　ボットは潜んで動く



めるべく、複数の脆弱性を悪用する機能を持つものも少なくない。OSのバージョンやソフトウェアの稼働状態に応じて悪用する脆弱性を使い分けるような巧妙なマルウェアもある。

また、オフィス製品のようなユーザー層の広いソフトウェアの脆弱性を悪用するものやWeb経由での侵入を試みるものが目立つのも最近の傾向である。間口が広く敷居の低い入口に向かうのは自然な流れである。

IPアドレスやドメイン情報を利用することで指向性を持って攻撃を行うマルウェアは従来からある。最近では個人情報や機密情報を利用して人間の脆弱性を突くという、非常に高い指向性を持つマルウェアもある。友人から普段通りの書きぶりで、友人しか知らないような内容のメールが送られて来たら、セキュリティに対する意識が高い人でも添付ファイルを開けてしまうかも知れない。敷居の高い入口を狙うときに、そのような指向性の高い攻撃が行われる。

マルウェアも分業する

従来のマルウェアは基本的には単体で機能するものが主流であった。ボットネットにおいてもボットそのものは多機能なひとつのマルウェアから構成されていた。しかし、最近のマルウェアには多機能化とは別の傾向が見られる。

最もわかりやすい例は図2に示すようなダウンローダと呼ばれる種類のマルウェアである。これは別のマルウェアをダウンロードすることを目的としたマルウェアである。ダウンローダを介することでダウンロード元のサーバでダウンロードさせる本体プログラムを制御することができる。それにより、マルウェアの解析や攻撃者の追跡が困難になることも事実である。

最近はOS等の機能によりソフトウェアの脆弱性の悪用を抑制できるケースもあり、人間の脆弱性についてもユーザーインターフェイスの改良等により回避しようとする試みが進んでいる。サイズや機能がシンプルなダウンローダの利用はそのような状況に順応した結果であるとも考えられる（図2）。

単機能化とは異なる傾向もある。マルウェアにはパッカーと呼ばれるツールを使って本体プログラムがエンコードされたものが多い。パッカーはプログラムファイルを小さくしたり、複製・解読から保護することを目的として圧縮や暗号化を行うツールである。しかし、それがマルウェアで利用されることにより、アンチウイルスソフトウェア等による検知を妨害するという役割を担うようになる。

最近ではパッカーもマルウェア化している。たとえば、アンパック時に感染処理を行うものが散見されるようになった。ある程度定型化してきた機能をパッカーが吸収することでマルウェア開発者は本来の機能に集中することができるようになる。パッカー自身がパッカー業界の中での生き残りを図ろうとしていると見ることもできる。

このように、環境への順応や機能によって分業するというのが最近のマルウェアに見られる傾向である。ボットネットの特徴のひとつも利用者と運用者という攻撃側の分業であった。このような傾向は、その仕組みや取り巻く環境が成熟し、安定性を求めるようになってきたことの現れであると解釈することができる。

セキュリティに特効薬はない

セキュリティ対策の重心は事後対応ではなく事前対応にあるべきである。事前対応は漢方医学のようなもので、特定の問題に対する特効薬ではない。しかし、ある程度の普遍性を持っており、最近のマルウェアに対しても有効であることがわかる。

例えば、最近のマルウェアは侵入経路としてWebやメールのようなユーザーに近いところを狙う傾向がある。Webサイトへのアクセスやメールの添付ファイルの取り扱い等、セキュリティのための習慣を身に着けるという基本的な対策がますます重要になっているということである。

セキュリティアップデートで既知の脆弱性を塞ぐことの重要性も変わらない。アップデートだけではいわゆるゼロディ攻撃には対抗できないが、多くのマルウェアが利用しようとする既知の脆弱性を塞ぐことはできる。

ボットに限らず最近のマルウェアはソースプログラムの状態で入手可能なものが少なくない。そのために、ボットネットが注目され始めた当初はパターンマッチングによるマルウェア検出の限界が指摘されていた。

確かに今日においてもアンチウイルスソフトウェアの対応がマルウェアの変化に追い付いているとは言い難い。しかしながら、最近のアンチウイルスソフトウェアは単純なパターンマッチングだけではなく挙動からマルウェアを検出する機能も備えており、そのチューニングの成果が出始めて来ている。

ソフトウェアの脆弱性に対しては、これまでは製品が市場に出た後の対策を中心に体制が整理されて来た。今後は脆弱性を低減できる開発手法等、市場に出る前の段階からの対策がより重視されるであろう。

一方、人間の脆弱性については教育・啓発活動を広げていくことが中心になる。また、OSや主要なアプリケーションソフトウェアが自動アップデートの機能を持つようになりつつある今日においては、自動アップデートの機能を持たないソフトウェアが野ざらしにされてしまわないように気をつける必要がある。例えば、ブラウザの自動アップデートに満足してプラグインのアップデートを怠っているということはないだろうか。

これら以外にもIDSのようなセキュリティ製品を導入するという対策もあるだろう。いずれにしても、何か一つの対策に頼るのではなく、複数の対策を総合的に活用して事前対応を行うことではじめて、多くのリスクを排除できるようになる。

事後対応に頼るスタンスでいる限りマルウェアが優位である。ボットのような実用型のマルウェアは自らの存在に気付かれないように潜む傾向にある。OS標準のプログラム名を模倣したり、ルートキットと呼ばれる隠蔽ツールを使ったりする。

図3はマルウェア感染時の動きをタスクマネージャで観察した結果である。このマルウェアはボットで、感染後に名前を変える。図3ではspoolsvc.exeという名前になっている。svchost.exeやspoolsv.exeはOS標準のプログラムである。

同図のパフォーマンスグラフで最初の山はインターネットエクスプローラを起動したときの負荷を表している。次の山が感染時の負荷であるが、際だって重いというわけではないし、感染後は大人しくしていることがわかる。コンピュータが遅くなったりおかしな動きをしたりする、といった従来のマルウェアに見られる症状を期待していたら、末永くお付き合いさせられることになる。

ボット対策プロジェクト

2007年2月に総務省・経済産業省の連携事業である「ボット対策プロジェクト」が本格運用を開始した。このプロジェク

図4　CCCクリーナーを使った駆除

トでは、ボットプログラムを収集・解析して対策手段としての駆除ツールを提供するとともに、ISPの協力を得て感染コンピュータのユーザーに通知を行っている。

C&Cサーバを停止させるというアプローチは目新しくはないが、ユーザーにリーチするというのは世界的に見てもユニークな試みである。JPCERT/CCもボットプログラムの解析からボットプログラム駆除ツール「CCCクリーナー」へ反映するところまでを行う「ボットプログラム解析グループ」としてプロジェクトに参加している。

ユーザーはサイバークリーンセンターからこのプロジェクトの成果を活用することができる。CCCクリーナーも同センターのホームページ（https://www.ccc.go.jp/）から誰でもダウンロードすることができる。感染コンピュータのユーザーにはISPから注意喚起メールが届けられるので、そのメールに記載された対策サイトのURLにアクセスしてCCCクリーナーを入手していただきたい。

また、ホームページにはプロジェクトの活動実績やボットネットの説明、リンク集等の有用な情報が掲載されているので是非ご参照いただきたい。

図4は図3で例示したボットをCCCクリーナーで駆除した様子である。CCCクリーナーが1件のファイルについて検出と駆除を報告しており、タスクマネージャの画面ではspoolsvc.exeが消えていることが確認できる。

なお、このプロジェクトでは駆除ツールを提供しているが、それは決して事後対応の可能性を広げようとするものではない。ボットに感染しているコンピュータが旧来型のマルウェアに感染していないとは限らない。むしろ、新旧のマルウェアが同居しているケースの方が多いくらいかも知れない。

そのような状況では技術的に駆除することができない場合がある。駆除ツールはボット対策の「答え」にはなり得ないのである。不幸にして駆除ツールを使わざるをえなくなったとしても、それをきっかけとして事後対応に頼らないセキュリティ対策に取り組んでいただけることを願っている。

一人一人の対策でインターネットを安全に

今日、インターネット上で悪意を持って使われるソフトウェアが現実社会と関連した脅威になる時代となった。

感染と破壊を繰り返す従来型のマルウェアが相変わらず多く出回っている一方で、高い指向性を持って攻撃を行うマルウェアが着実に実用の場を広げている。そのような状況では感染数や攻撃数だけで脅威の度合を見定めようとしても、セキュリティ対策どころか真の脅威を見付けることすらできないだろう。マルウェアの変化に対して我々も進化しなければならない。

一方で、セキュリティ対策の基本は昔から変わっていない。個々の目的に応じた適切な対策を組み合わせて、積極的かつ柔軟なアプローチを継続していくことである。しかし、そのような考え方や手段を誰もができるわけではない。対策を率先して実施したり、製品やサービスとして一般ユーザーに提供する役割を担うのが本書の読者を始めとする専門的な知識を持った人たちである。そして、一般ユーザーも含めて、一人一人がセキュリティに対する意識を一段ずつ高めて行くことによって脅威に対抗できるようになるのである。

振り込め詐欺や誘拐事件において電話は重要なアイテムであるが、だからといって電話が危険で使用すべきではないという考え方は主流にはならないだろう。マルウェアが現実社会における犯罪との接点を持ち始めたとはいえ、インターネットやコンピュータあるいはソフトウェアが全て有害というわけではない。各自が各々の立場で強い心を持って正しく活用することによって、インターネットが安全になるだけでなく、今よりももっと便利な道具になるはずである。