

Q 「ボットネット」とは何ですか？

A

ボットネットとは

ボットネットの「ボット」とは、第三者のコンピュータに侵入し、所有者の知らない間に悪意ある命令を実行する、いわゆる「有害プログラム (malware : マルウェア)」の一種です。既存の有害プログラムとしてはコンピュータウイルスやワーム、トロイの木馬といったものがよく知られています。ボットも他の有害プログラムと同様の活動を行いますが、ボットの最大の特徴は「外部からコントロールされる」ことにあります。これによりボットに感染したコンピュータは所有者の知らない間に外部からさまざまな命令を受け、実行してしまいます。

ボットネットとはこういったボットに感染したコンピュータが束なってできた「外部からコントロール可能な」ネットワークのことをいいます。一般ユーザのコンピュータ1台1台の能力は大きくなくても束ねることで大規模な(主に有害な)活動を行います。過去には数十万台規模のボットネットの観測事例も報告されています。

ボットの語源はroBOT (ロボット) であるといわれています。またボットは別名をzombie (ゾンビ) ともいいます。これらは感染したコンピュータが外部からの命令により、統率の取れた軍隊のように一斉に活動することから付いたものでしょう。

ボットネットの仕組み

では、ボットネットはどのように構成されるのでしょうか。図1はボットネットの仕組みを示しています。

まず、ボットの感染には既存のウイルスやワーム、トロイの木馬といった有害プログラムと同じ侵入経路が用いられます。具体的には、インターネット上からコンピュータの脆弱性を突いて侵入する、Webサイトや添付メールの閲覧から感染する、便利なソフトウェアに偽装してユーザにダウンロードさせる、といった感染経路をたどります。一度ボットに感染してしまうと、そのコンピュータは起動することに自動的にコントロールサーバと呼ばれるボットネットの管理サーバに接続し、外部からコントロール可能な状態になります。

攻撃者は自分のばらまいた有害プログラムの感染コンピュータをいちいち探し回る必要はなく、コントロールサー

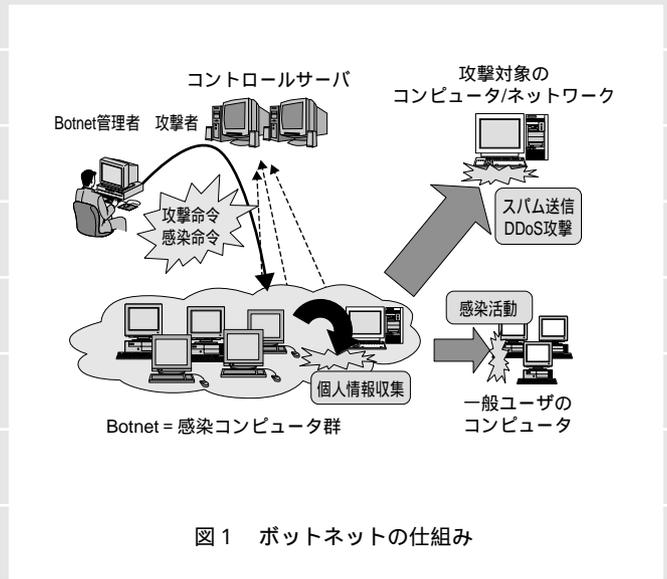


図1 ボットネットの仕組み

バから命令するだけですべての感染コンピュータを自由に操られてしまいます。現在ではこのコントロールサーバとの通信にIRC (Internet Relay Chat) と呼ばれるプロトコルが利用されることが多く、これらは特にIRCボットと呼ばれます。

複数の感染コンピュータを操れるボットネットは、次のようなさまざまな有害な活動に使われます。

(1) DoS攻撃, スпамメール送信

攻撃者がボットネットに命令するだけで、大規模なDDoS (Distributed Denial of Services : 分散サービス不能) 攻撃が可能です。攻撃された側からみるとインターネット中に分散する感染コンピュータから一斉に攻撃を受け、しかも1台1台は感染していることにすら気付いていない一般ユーザなので、対処が非常に難しいのが現状です。

またボットネットを用いてスパムメール(営利目的のダイレクトメール)の大量配信が行えます。送信元の特定を困難にし、同内容のメールを一度に効率的に送信できるため、ボットネットの感染コンピュータを踏み台にして大量のメールが送信されます。

(2) システム情報や個人情報の収集, 送信

ボットは感染コンピュータ上のメールアドレスやカード情報といった個人情報を収集し、コントロールサーバから命令された宛先に送信することも可能です。ボットの種類によってはほかにもキーログ機能やカメラやマイクを操作して映像や音声を転送する機能などを備えているものもあります。

(3) さらなる感染活動

感染活動を命令されると、各ボットはネットワーク上の他のコンピュータの脆弱性をスキャンし侵入を試みます。ボットネットの1台1台がこの活動を行うので、ネットワーク全体ではボット感染コンピュータが瞬く間に拡大してしまいます。

(4) 自己アップデート

攻撃者がさらなる有害プログラムの更新を行うこともあります。例えばボットに新しい機能を追加する、感染コンピュータの所有者により見つかりにくくする等といったプログラムの更新や追加、設定の変更も容易に行えます。実際にはWebサイトからのダウンロードやP2P機能を用いたコピーでプログラムの追加が行われます。

このほかにもフィッシング詐欺に用いられたり、Open Proxy（代理接続サーバ）として使われたりといった事例も報告されています。また近年では攻撃者がボットネットを利用する権利を売買するなど、いわゆる商用利用の実態も徐々に明らかになってきました。大規模なスパムメールの送信、DDoS攻撃の利用、またはコントロールサーバから命令できる権利そのものといったボットネットの利用権が月額レンタル制などで取引されています（図2）。

ボットネットの現状と脅威

ここまでで述べたようにボットネットは感染後も外部からコントロール可能なことで、既存のウイルスやワームと比べても非常に脅威といえます。

実際に、最近のアンチウイルスベンダが定期的に更新する新種ウイルスリストのうち実に8割はボットです。この背景にはボットはオープンソースとして配布されているものも多く、自由に改変が可能で亜種が非常に回りがやすいという実情があります。例えばSpybotという名称のボットからは

All I have to offer at the time are all exclusive.
I hope to offer shared services within the next two weeks.

-- Exclusive a -- (SOLD OUT)

10-15k always online, \$400 / weekly - \$1300 / monthly.
and RBL/Connect checked once every 13 minutes.

-- Exclusive b -- (SOLD OUT)

20-30k always online, \$700 / weekly - \$2400 / monthly.

-- Exclusive c -- (AVAILABLE)

2-3k always online, \$150 / weekly - \$450 / monthly.

図2 掲示板でのボットネット売買の事例

判明しているだけでも2000種類以上の亜種が派生しています。感染規模を誇示するような愉快犯的なワームとは異なり、ボットネットには商用利用や個人情報収集といった実利目的の面が強く、膨大な亜種が作成され実態の把握が大変困難になっています。セキュリティに関する非営利組織JPCERT/CC (<http://www.jpccert.or.jp/>) と通信事業者の業界団体Telecom-ISAC JAPAN (<https://www.telecom-isac.jp/>) が本年7月末に合同で発表したボットネットの調査によれば、1日当たり約70種もの新種が発見されています。またこの報告では、日本国内で少なくとも50台に1台のコンピュータがすでにボットに感染している実態や、Windowsコンピュータに何もセキュリティ対策を行わない状態でインターネットに接続すると平均4分で何らかのボットに感染するといった事例も紹介されています。

ボットにならないために

ボットネットの実態はまだ全容がつかめていないのが現状ですが、まず各個人がボットの脅威を認識し、その拡大と利用を防ぐための基本的なセキュリティ対策を行うことが重要です。

ボットも感染活動は基本的に既存の有害プログラムと同様の手法を用いています。まず、Windows Updateを必ず行い、OSのセキュリティ機能を最新の状態に保つことが重要です。またウイルス対策ソフトを導入し、ウイルス定義ファイルを最新のものに更新しておくことも必要です。他にもメールに添付されたファイルは安易に実行しない、コンピュータ上にパスワードやカード情報を書き込んだファイルを保存しておかない、などといった人為的な努力も必要になります。

ボットネットの活動の全容や感染実態などの現状の究明と対策も始まりました。先に挙げた業界団体のほかにも欧米中心に活動しているHoneyNet Project (<http://www.honeynet.org/>) などがボットネットの実態の把握に努めています。国内では警察庁の@policeが本年1月にボットネットに関する警告を発し、その後も継続的にボットネットの追跡を行っています。また総務省が本年7月に行ったセキュリティ対策報告書ではボットネット対策について提言しています。今後は制度面も含め、業界全体で具体的な対策が徐々に行われていくことになるでしょう。

このコーナーで取り上げて欲しい質問をE-mailで編集部までお寄せください。
(社)電気通信協会内 NTT技術誌事務局 E-mail jrr@tta.or.jp