

ボットネット (botnet)に注意

1 概要

様々な活動が行われているインターネット上で、今後、特に警戒が必要と思われるものに botnet が挙げられる。botnet とは、攻撃者が作り出すネットワークのことで、攻撃者の命令を送信する指令サーバ、bot¹に感染した一般のコンピュータ群から構成される。

bot には DoS 攻撃やスパムメール送信をはじめとする、様々な機能が組み込まれており、攻撃者は botnet に属する bot を制御することができる。例えば、攻撃者が DoS 攻撃の命令を送信すると、bot に感染した各コンピュータは一斉に指定されたサイトに対して DoS 攻撃を実行する。英国では、商用の賭博サイトに対し「DoS 攻撃を行う」として金銭を要求する、いわゆるサイバー恐喝が行われた。今後、botnet を利用したサイバー犯罪による被害が懸念される場所である。

サイバーフォースセンターでは、botnet の現状を把握するため、観測システムを構築して運用している。現在のところ、約 20 の botnet を観測の対象としており、1 日当たり約 3 万台以上の bot を有する複数の botnet を確認している。以下では、観測結果の一部を紹介するので、今後の botnet 対策の参考としていただきたい。

2 botnet の特徴

botnet は「攻撃者」「指令サーバ」「bot に感染したコンピュータ」から構成される(図1)。各 bot は指令サーバと通信を行い、攻撃者からの命令を待ち受ける。命令の通信は IRC プロトコルが使われることが多く、この場合、指令サーバが IRC サーバ、bot に感染したコンピュータは IRC クライアントとして動作する。一部の bot は HTTP プロトコルを利用することもある。

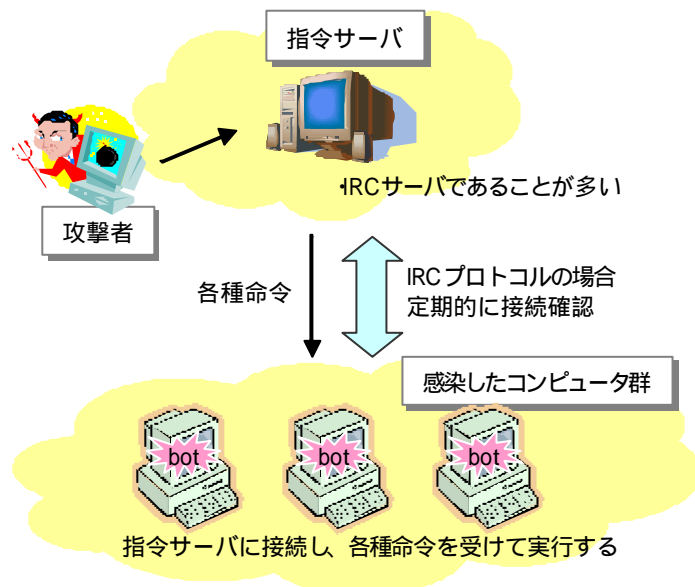


図1 botnet の全体像

¹ 一般に bot という用語は有害・無害を問わず用いられる。ここでは botnet を構成する有害プログラムを意味する。

bot には様々な機能が実装されている。代表的なものには、「他のコンピュータへの感染活動」「DoS 攻撃」「bot 本体の更新」「スパムメール送信(中継)」「特定の広告を参照」がある。さらに「キーロガー」などといった、いわゆるスパイウェアとして機能するものもある。これらの機能は攻撃者から命令を受けて各 bot が実行する。

bot が用いる感染手段には、「OS やアプリケーションの脆弱性を攻撃」「他のウイルスが開くバックドアポートを悪用」「パスワードの辞書攻撃」といったものがある。脆弱性を攻撃する場合、攻撃者は感染対象とするコンピュータを限定 (IP アドレスの第 1・第 2 オクテットを指定) し、局所的な攻撃を実行することが多い。また、感染した直後に自分自身の IP アドレスを基準に攻撃先を決定することもあり、この場合、プライベートアドレスを利用しているのであれば、そのセグメント内が攻撃対象になりうる。

膨大な bot の亜種が存在する理由には、雛形となるソースコードがインターネット上で流通している点が挙げられる。攻撃者は、新たな脆弱性情報が公表されると、その脆弱性を利用した攻撃プログラムを追加して新種の bot を作成する。新しい bot は、主に HTTP プロトコルを利用して転送された後、更新される (図 2)。bot は自分自身の実行プロセスを隠すなど、巧妙に作成されており、利用者は bot に感染していることに気が付きにくい。また、新種の bot が次々と発生するため、ウイルス対策ソフトでも検出できないこともある。

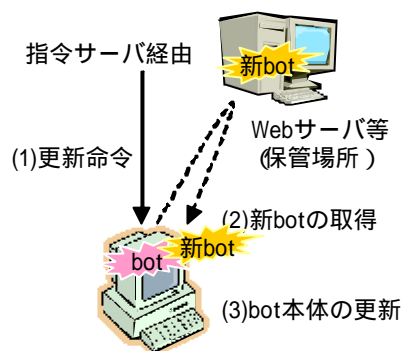


図 2 bot の更新

指令サーバについては、現時点では明確に判明していないが、第三者のサーバを無断で利用するほか、攻撃者が Dynamic DNS サービスを利用して独自に用意したサーバであると考えられる。bot からはドメイン名で接続するため、指令サーバの IP アドレスは固定である必要はない。

以上が botnet の特徴となるが、今後も新たな bot が作成されるのは間違いない。具体的な botnet 対策については後述するが、bot に感染しないためにも、情報セキュリティ対策を十分に行うことが大切である。

3 botnet 観測状況

注意 以下の観測結果は、サイバーフォースセンターの観測システムで把握した botnet の一部について、その実態を示したものである。

(1) 観測例

ア botnet-A

観測期間	自 平成 16 年 11 月 25 日 至 平成 16 年 12 月 5 日
指令サーバ名	xxxxx.xxxxxxxx.net (一部伏せ字)
通信手段	IRC プロトコル 使用ポート：TCP6667 番
ウイルス名	W32.Spybot.Worm, WORM_RBOT.GEN

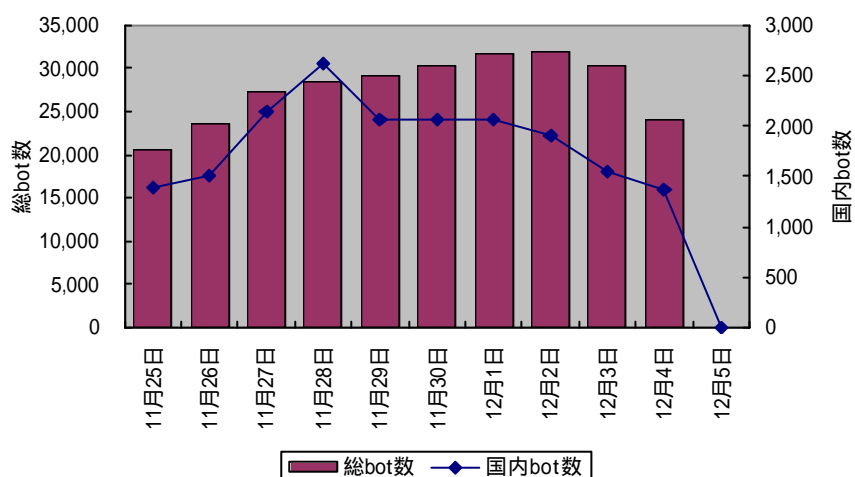


図3 1日毎の bot 数の推移

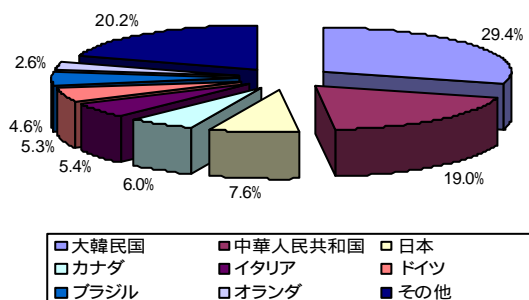


図4 国・地域別比率

bot に感染したコンピュータは、稼働状態になると、指令サーバに接続を試みる。このため、botnet を構成するコンピュータの台数は時間とともに変化する。図3・4 は botnet-A に接続したコンピュータの IP アドレスを集計したものである。観測期間中、bot に感染

したと推定される IP アドレスは約 235,000 件存在し、そのうち国内が発信元と推定される件数は約 18,000 件であった。このように、国内でも bot に感染したコンピュータが存在していると考えられる。

12 月 5 日以降、bot 数がゼロになっている理由は、bot 本体が更新命令を受信して自分自身を新たな bot に置き換え、一時的に他の指令サーバへ移動したためである。この時点で botnet-A は消滅したかに見えたが、後日、別の bot が当該サーバを利用することになった。

イ botnet-B

観測期間	自 平成 16 年 12 月 22 日 至 平成 17 年 1 月 16 日
指令サーバ名	xxxx.xxxxxxxx.net (一部伏せ字)
通信手段	IRC プロトコル 使用ポート：TCP8080 番
ウイルス名	WORM_SPYBOT.HD

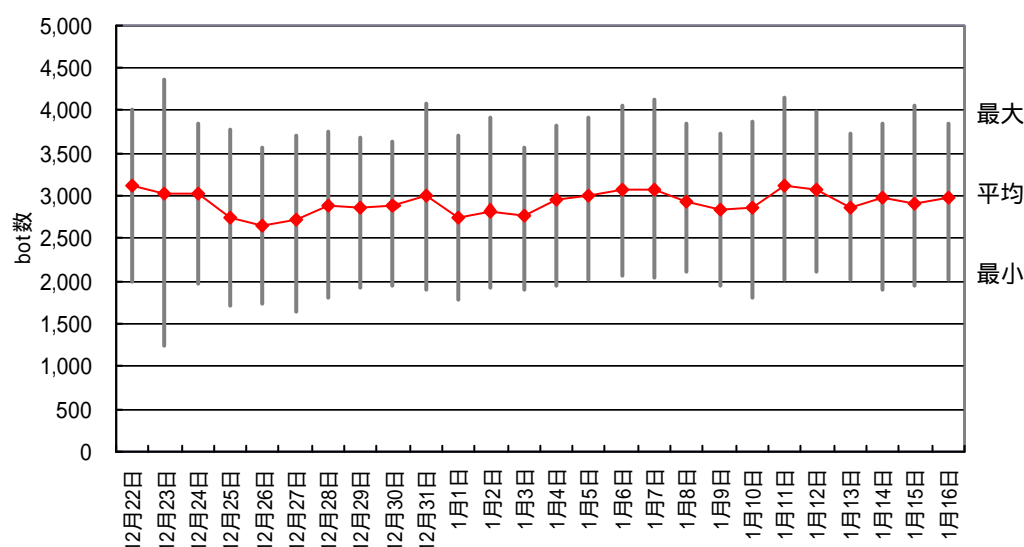


図5 1時間毎に観測した平均 bot 数の推移 (1日毎)

図5で示した bot 数は1時間毎の平均であるため、図3の botnet-A とそのまま比較することはできない²。しかし、別の観測結果から、botnet-B は約2倍の bot を保有していると推定された。この中には国内の IP アドレスも含まれている。

botnet-B では、命令の通信は IRC プロトコルが使われるが、使用する通信ポートは TCP8080 番であった。また、botnet-B の指令サーバは、他の botnet (TCP7776 番を利用) と兼用となっていた。

² botnet-A は接続するすべてのコンピュータを観測できるが、botnet-B はある瞬間における接続数のみ観測できる。これは指令サーバの違いによるものである。図5は、1時間毎に bot 数を観測したもので、1日の中で最大・平均・最小の推移を示した。

その他、観測を行った botnet の中には、複数の指令サーバで構成されるものも存在した。このように botnet によって構成や規模は異なる。どのような botnet として動作するかは、感染した bot の種類によって異なり、作成する攻撃者次第となる。

(2) 観測期間中、botnet で実行された主な命令

上記で紹介した botnet のほか、サイバーフォースセンターで観測中の botnet において攻撃者が実行した主な命令を次に示す。

【感染活動】

- ・ MS03-026(DCOM)の脆弱性を悪用して感染を拡大
- ・ アドレス範囲を指定した上記感染活動
- ・ MS04-011(LSASS)の脆弱性を悪用して感染を拡大
- ・ Windows ネットワーク共有の脆弱なパスワードを標的にして感染の拡大
- ・ MS SQL Server の脆弱なパスワードを標的にして感染の拡大

【DoS 攻撃】

- ・ 指定したホストに対する SYN Flood 攻撃
- ・ 指定したホストに対する UDP Flood 攻撃
- ・ 指定したホストに対する Ping Flood 攻撃

【ネットワークサービスの起動】

- ・ HTTP サービスの起動
- ・ TCP 通信をリダイレクトする SOCKS を起動

【スパイウェア、bot の更新】

- ・ 盗聴(スニッフィング)
- ・ 特定のアプリケーションの CD キーを取得
- ・ ダウンロード命令によるトロイの木馬等のダウンロードと実行
 - ・ Internet Explorer のスタートページを指定されたページに変更するトロイの木馬
 - ・ 特定の Web サイト上にあるバナー広告をクリックするように設計されたトロイの木馬
- ・ bot 本体を更新

【状態表示】

- ・ システム情報(ハードウェア、OS、IP、botnet 接続時間等)の表示
- ・ ネットワーク情報(回線種別、IP 等)の表示

観測期間中、最も数多く用いられた感染手段は、MS03-026(DCOM)の脆弱性を悪用するもので、次いで MS04-011(LSASS)の脆弱性を悪用するものであった。既に、これらの脆弱性を解消する修正プログラムは配布されているが、今もなお、適用していないコンピュータが数多く存在していると言える。

4 botnet 対策

基本的には、botnet 対策は従来のウイルス対策と同じである。コンピュータの利用者は「オペレーティングシステムやアプリケーションの修正プログラムを適用」「ウイルス対策ソフトの導入及び定義ファイルの更新」といった基本的な情報セキュリティ対策を、常に心がける必要がある。さらに「パーソナルファイアウォールの導入」によって安全性を高めることが期待できる。

ウイルス対策ソフト以外の bot 感染の確認方法には、Windows OS の標準コマンドである netstat コマンドを利用して不審な通信が確立されていないか確認するほか、bot のプログラムファイルには ReadOnly, System, Hidden 属性が設定されていることが多いため、attrib コマンドを利用して該当するファイルを確認すると良い。ただし、いずれの方法を用

いても巧妙に作成された bot を発見できるとは限らないので注意されたい。

仮に bot に感染した場合であっても、指令サーバと通信できなければ攻撃者に制御されることはない。このため、ファイアウォールの設定で不要なポート（特に IRC）の通信を遮断することは有効である。ただし、bot が他番号のポートを利用するものや、HTTP プロトコルを利用するものであったならば、完全に阻止することは困難となる。また、指令サーバなどの botnet に関連する IP アドレスをフィルタリングすることは効果的ではあるが、新たな bot が次々と発生するため、そのすべての指令サーバを網羅することは難しい。

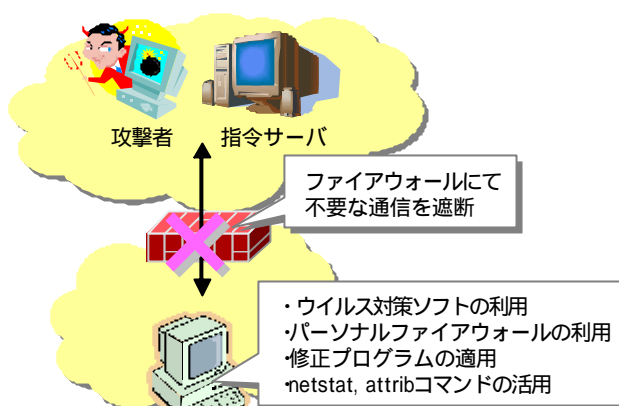


図6 botnet 対策

5 おわりに

サイバーフォースセンターで行った観測結果で示したとおり、既に数多くのコンピュータが bot に感染している。bot の脅威が大きい理由には、

- (1) 新たな機能追加が容易である
- (2) 改変による亜種や新種を作りやすい
- (3) 攻撃者は非常に簡単な操作で多数のコンピュータを制御できる

が挙げられる。

サイバーフォースセンターでは、botnet 対策を推進する国際的な協力体制（司法機関を含む）の元、緊密な情報交換を行っている。引き続き、サイバーフォースセンターでは botnet の動向を把握するとともに、国内外における関係各機関との連携を強化する予定である。

@police 参考資料

[分析レポート]

- ・複数の脆弱性を悪用する Gaobot ワーム <2004/07/13>
http://www.cyberpolice.go.jp/detect/pdf/report_gaobot.pdf

[世界のセキュリティ事情]

- ・トロイの木馬攻撃に移行しているフィッシング攻撃者 <2005/01/06>
http://www.cyberpolice.go.jp/international/north_america/20050113_211237.html
- ・1週間に150のゾンビプログラムを作成する有害プログラム作成者 <2005/01/05>
http://www.cyberpolice.go.jp/international/vulnerability/20050106_235720.html
- ・オンラインゲームの得点を増やすことに使われた Botnet <2004/12/21>
http://www.cyberpolice.go.jp/international/europe_russian/20041224_000340.html
- ・防御されていないパソコンは、ほんの4分でハッカーのボットに成り下がる <2004/11/30>
http://www.cyberpolice.go.jp/international/vulnerability/20041202_220051.html
- ・大規模に「ボット」を配備するハッカー <2004/09/20>
http://www.cyberpolice.go.jp/international/north_america/20040923_013951.html
- ・ワームにネットワークスニファを仕込むウイルス作者 <2004/09/14>
http://www.cyberpolice.go.jp/international/north_america/20040916_020348.html
- ・サイバー空間に侵入する組織犯罪 <2004/08/30>
http://www.cyberpolice.go.jp/international/europe_russian/20040904_232519.html
- ・ウィンドウズの欠陥を攻撃する攻撃ボット <2003/08/04>
http://www.cyberpolice.go.jp/international/vulnerability/20030806_001240.html
- ・Windowsのブロードバンドユーザが攻撃者のターゲットに <2003/03/12>
http://www.cyberpolice.go.jp/international/vulnerability/20030318_163736.html