5-2　ボットネットの把握と停止に向けての総合的検討：問題点と対策

5-2 A Holistic Perspective on Understanding and Breaking Botnets: Challenges and Countermeasures

張　宗華　　門林雄基
Zhang Zonghua and KADOBAYASHI Youki

要旨

マルウェアは今日のサイバー攻撃の中で最も多くの割合を占め、私たちのネットワーク資産に対して重大な脅威を与えている。さらに深刻なのは、ボットネットの構築によって多量のボット（マルウェアに感染したホスト）が特定の意図のもとに互いに協調した場合、被害が甚大になる点である。ボットネット対策としてこれまで様々な予防、検知、対処の方法が開発されてきたが、ボットネットの構築・維持をする攻撃者たちは防御システムの回避方法を常に考えている。本稿では特定の検知方法のテクニカルデザインに注意を向けるのではなく、ボットネットが有する可能性のある特徴やセキュリティの回避方法を総合的に概観する。その目的は、高度な攻撃者の挙動について基本的理解を得ることにある。それが効果的なボットネット対策を設計・開発する上で予備的かつ不可欠な工程であると考えられる。続いて、既存の対策に対する批判的評価の基礎として、トップダウン解析の枠組みを作成する。それによって、ボットが存在するコンピュータネットワークにおいて強固なディフェンスラインを実現する総合的方法が見えてくるだけでなく、ある程度高度なボットを様々なシステムレベルで検知するための、実用的方法が幾つか浮かび上がってくる。

Malware has gained the most prevalence in today's cyberattacks that threaten our network assets. More seriously, their attack consequence can be significantly enlarged when a huge amount of bots (hosts compromised by malware) coordinate each other with particular intents by constructing botnets. While various prevention, detection, and response techniques have been developed for defending against botnets, attackers constructing and maintaining botnets will always manage to evade defense systems. Instead of limiting our attention to the technical design of specific detection techniques, this paper rather gives a comprehensive review on the features and security-evasion techniques that can be possessed by the botnets, with the objective to obtain a fundamental understanding on sophisticated attacker behavior, which is believed to be the preliminary yet essential step towards the design and development of effective anti-botnet techniques. We then develop a top-down analytical framework as a basis for critical evaluation on the existing countermeasures. This framework not only allows us to envision a holistic methodology for achieving in-depth defense boundary of computer networks in the presence of bots, but also suggests a number of practical ways for detecting bots at different system levels with certain degree of sophistication.

[キーワード]
ネットワーク・セキュリティ，侵入検知，ボットネット，マルウェア
Network security, Intrusion detection, Botnet, Malware

1 はじめに

様々なサイバー攻撃の中で最も悪質で最も対処しにくいのは、複数の攻撃者が協力し、時間をかけて段階的に実行されるものである。これをMSCA（多段階協調攻撃）という[51]。このタイプの攻撃を実施するためには、攻撃者が偵察、侵入、攻撃し、脆弱性を突く必要がある。一方、攻撃参加者は共通の目的のためにリソースやツールの共有、タスクの割当て、情報のやりとり及び同期によって計画・協調することが必要である。ボットネットは、こうしたMSCAの一種である。現在のサイバー攻撃において主流になりつつあり、私たちのネットワーク資産に対して重大な脅威を与えている[18]。例えば、2003年に報告されたボットはわずか740件だったのに対し、2007年にはすでに100万件のレベルに達している。

ボットネットは多数のボットで構成される。ボットとは、ユーザ又は他のプログラムに対して自動的に動作するプログラムである。このほか、マルウェアに感染し、マルウェアによって制御されるホストを広く指す場合もある。マルウェアがシステムに侵入する形にはトロイの木馬、スパイウェア、キーロガー、ルートキットなど様々な形があるが、その最終的な目的はシステムに対する特権的アクセスを獲得し、オーナーが気づかない間に、またはオーナーの同意がないままに悪意ある活動をすることである。特にボットネットは次の2点において他の侵入形態と異なっている。一つ目は、明確な意図（例えば経済的利益）があること[17]。二つ目は、ボットマスタ（ボットを制御する攻撃者）が指令・制御（C&C）チャネルを使って配下のボットとインタラクトできることである[40]。ボットネットの典型的なライフサイクルには、脆弱性のあるホストの調査、ホストへの侵入、C&Cの確立とボットマスタとのインタラクト、次のターゲットへの感染、という四つの段階がある。しかし、感染及びボットマスタとボット間の対話型動作が成功するためには、特定のアーキテクチャ及びプロトコルが必要になる[14]。例えば、ボットネットがよく使用するプロトコルにIRC（Internet Relay Chat）がある[6]。これは大規模なチャットルームを念頭に作られたものである。ボットネットが構築されると、ボットマスタはインターネット中に拡散するボットを使ってスパム、DDoS、盗聴など多様な攻撃を仕掛けることができる。

多段階の協調的な性質が分かれば、ボットネットの時間的・空間的性質が明らかになることには疑う余地がない。具体的には、ボットの感染には幾つかの過程が必要になるが、個々の過程が発生するためにはその直前の過程が実現しなければならない。よって、侵入シーケンスが最後まで完了するまでにはある程度の時間を要する。また、ボットマスタは通常、多数のボットをコントロールするため、ある瞬間にボット群が同じ挙動を同時に取る可能性がある。一方において、空間・時間特性が分かればネットワーク防衛者はボットネットを監視することができる[13][20]上、ホスト型侵入検知システム（HIDS）とネットワーク型侵入検知システム（NIDS）を統合してボットネットの防衛に当たることが可能である。他方、ボットマスタの立場からすると、自分の侵入地を難読化して発見の回避をねらうことが想定できる。例えば、高度なボットネットが暗号化技術を採用して指令・制御（C&C）チャネルを保護し、ハニーポットトラップを回避することが考えられる[53]。また、より高度なボットマスタであれば、ピアツーピア通信を用いることによって、C&Cサーバの単一故障に対してボットネットの頑健性を高めることができる[48]。一つのボットはマクロな特性のほか、トラフィックパケット、システムログファイル、ファイルシステム、メモリといった、攻撃の結果としてのミクロな観測項目について動作トレースを残す可能性がある。ボットに関する完璧なプロファイルには、上記の特性がすべて含まれることが期待される[49]。これを実現する方法の一つは、ボットネットを捕捉及びトラッキングするハニーネットを、仮想マシン（VM）を用いて構築し、ミクロなマルウェアの挙動解析を行うことである[2]。

本稿はボットネットの基本的特性を出発点として、ボットの特徴に関する総合的な概要を最初に提示する。特に次世代ボット及びセキュリティ回避技術について述べるが、これは攻撃者の高度な挙動について理解を深め、効果的な対策の設計開発に役立つものと期待される。次に、既存のボットネット検知技術に関する批判的評価及び比較研

究の基礎として、インターネットからホストに至るトップダウン解析の枠組みを作成する。この枠組みでは、ボット対処に関する様々なモデル、方法及びツールを開発・統合することによって、強固な防御メカニズムを実現するための総合的方法を構想することができる。またその枠組みは、ある程度の脅威と高度性を備えたボットを様々なシステムレベルにおいて監視、検知、トラッキングする実用的方法を示唆している。

本稿の以下の構成は次のとおりである。**2**では、一般的なボットネット解析について述べる。特にそのアーキテクチャと基本的特性に焦点を当てる。**3**は、次世代ボットネットの特徴とセキュリティ回避技術を取り上げる。続く**4**では、ボットネットの検知に関する既存技術について調査し、ボットネットの解析と検知を実施する総合的方法を提案する。最後に**5**において本稿のまとめを行う。

2　ボットネットの概要

ボットネットの構築及び維持手順を図1に示す。線上の数字はボットネットの動作順序を表す。具体的には次のとおりである。

1. ボットネットがターゲットネットワーク（あるアドレスの範囲内）を調査し、自己複製するワームやウイルスなどの手段によって被害者の脆弱性を突く。
2. 被害者は（知らない間に）シェルスクリプトを実行し、感染源からボットのバイナリファイルをダウンロードする。ボットはシステムのブートプロセスにそのボット自体を組み込むことによって、自動的にインストールされて動作する。
3. ボットはC&Cサーバと接続をするために、DNSサーバにホストのIPアドレスを確認しに行く（これは無視できるほか、ネットワーク構造や通信プロトコルに依存する）。
4. ボットはC&Cサーバとの接続を確立し（特定の通信チャネルを使用）、ボットネットに参加する。
5. ボットは、バイナリアップデートの取得や更なる攻撃の実施のためにボットマスタから指令を受け取る一方、脆弱性を持つ他のホストに感染する。

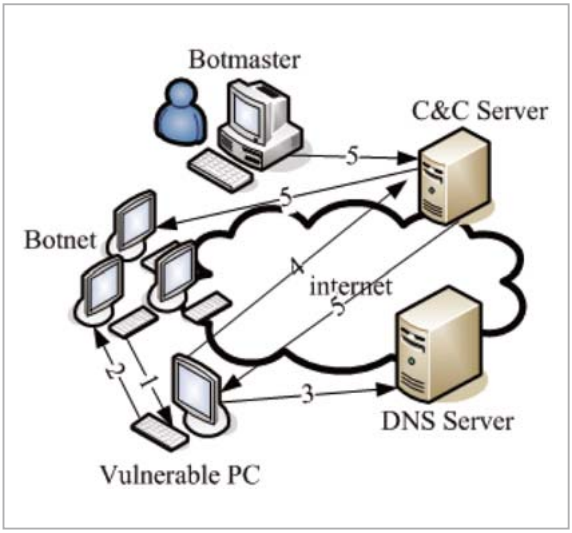

図1　ボットネットの構築と維持

基本的な手順は似ている（最初の四つの工程は自動だが、最後の工程はコマンド制御である）が、各段階の実施において同じ方法を使うとは限らない。特にフィルタリング方式、C&Cサーバのアーキテクチャとプロトコル（IRC、P2P、HTTPなど）、チャネル難読化の方法、ボットとボットマスタ間の集合メカニズムと認証スキームなどは、異なるものを用いることがある。そのため、ボットネットの基本的理解を得るには、マクロな属性とミクロな属性の両方を調べる必要がある。

2.1　指令制御サーバの構成

ボットネットの構築と維持及びボットとボットマスタ間の通信には、特定の構成とプロトコルが必要になる。ボットがボットマスタからバイナリアップデートを取得する方法及びボットマスタが指令によってボットを制御する方法は、それによって決まる。図1に示すように、新たに感染した被害者は通信を開始し、ボットネット参加のためにC&Cサーバとの接触を試みる。ボットネットの構成は一般にC&Cサーバのモデルによって中央管理型と分散型の2種類に大別される。また、分散型構造の実施形態にはP2P型とランダム型とがある。その原理を図2に示す。

中央管理型では通常、ボットネットが複数のC&Cサーバを所有し、ボットとボットマスタ間の通信はすべて1台のC&Cサーバに向けられる。その様子を示したのが図2(a)である。この

中央管理型 C&C モデルは実装が容易であるため、通常は既存ボットネットによってよく使用される。ボットマスタは常に合目的かつ利益指向であるため、1 台のコンピュータを感染させて C&C サーバにするだけで何千というボットを制御し、それによって中央管理型 C&C モデルのボットネットが容易に構築できる。このタイプのモデルが持つもう一つの長所は、ボットマスタが比較的小さい遅延でボットを制御・調整することが容易な点である。ボットネットの維持も他のモデルに比べて容易である。しかし、中央管理型 C&C モデルが持つ欠点は、C&C サーバがボットネットの単一障害点になるため、C&C サーバが発見されて機能を失うとボットネット全体が機能を停止することである。AgoBot、SDBot、BRbot、SpyBot など多くのボットが中央管理型 C&C モデルを採用している。

これより頑健性が高いのが P2P 型 C&C モデルである。このタイプでは C&C サーバがボットネット内に分散している。この構成ではボットとボットマスタ間の通信が数台ではなく一群の C&C サーバによって行われるため、中央管理型モデルに存在する障害点を回避する可能性がある。その様子を示したのが図 2(b) である。一部の C&C サーバは発見されるが、ボットマスタは残ったサーバによってそのままボットネットを制御できる。とはいえ、構築過程と維持において更に労力が必要なことは明らかである。この構成のスケーラビリティは P2P の本質的な特性によって制限されるため、少数のクライアントにしか対応できない。また、ボットマスタは C&C サーバ及びボットと C&C サーバ間の通信を維持する必要があるため、その分だけボット間の協調が実現しにくくなり、ボットの応答遅延は大きくなる。この構成を用いる代表的なボットに Phabot、Storm、Slapper、Nugache、Sinit がある。これより複雑な C&C モデルは本質的にランダムである[8]。その構成を図 2(c) に示す。このモデルではボットはボットマスタとの接続を積極的に開始せず、ボットマスタの呼び出しを待ってからその指令に従って動作する。したがって、ボットマスタが配下のボットに指示を与えて攻撃を開始する前にそのボットの確保に時間を取られる。ランダムモデルは論理的には実施可能だが、実際のボットネットではまだ普及していない。P2P 型 C&C モデルと同様、ランダムモデルは実施が容易で発見やトラッキングに強い反面、スケーラビリティが小さく、応答遅延が大きいという欠点がある。

異なるボットネット構成の有用性を評価するため、Dagon ら[14] は有効性、効率、頑健性という三つの指標を提唱した。これらの指標はボットのネットワーク (主にボットの調整) に対する考察を助けるが、上記三つの C&C モデルの評価には不適当かつ不十分である。そこで上記 C&C モデルの特性比較に関し、私たちは新たに五つの指標を提唱する。具体的には、構築と維持 (C&M) の容易さ、有効性、頑健性、応答遅延、そしてスケーラビリティである。簡単な比較を表 1 にまとめる。

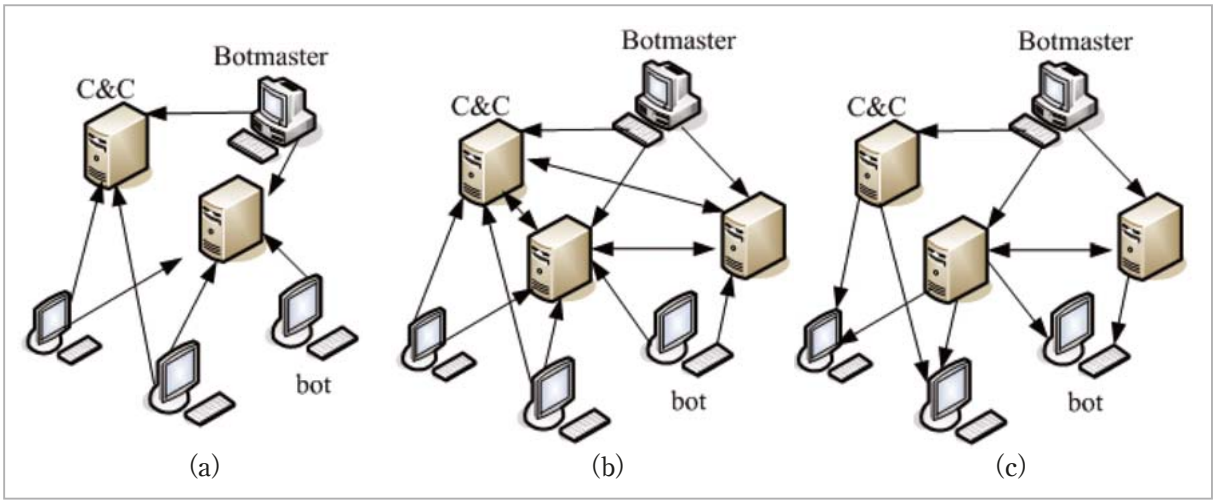

図2 C&C サーバの構成

(a) 中央管理型 C&C サーバ (b) P2P 型 C&C サーバ (c) ランダム型 C&C サーバ

表1　代表的な三つの C&C モデルの比較

Structure	C&M	Effectiveness	Robustness	Latency	Scalability
Centralized	High	High	Low	Low	High
P2P-based	Low	Medium	High	Medium	Medium
Random	Medium	Medium	Medium	High	Low

また、各指標について以下に説明する。

- C&M は、ネットワーク規模、伝播スケール、ボット更新速度などに関するボットネットの構築と維持の容易さを示す。
- 有効性は、電子メールのスパミングや DDoS など、ある特定の意図に対するボットネットの全体的な有用性の推定に用いる。
- 頑健性は、ボットネットの脆弱性及びC&Cサーバの耐障害性に関する評価を示す。
- 遅延は、指令メッセージの送受信やその調整などに関するボット挙動の効率を示す。
- スケーラビリティは、ボットネットが容易に拡張又は縮小可能かどうかを表す。

2.2　通信プロトコル

C&C サーバはボットネットのバックボーンを構成する。ボットは C&C サーバ経由でボットマスタに接触し、特定のネットワークプロトコルを用いてボットマスタと通信しなければならない。C&C サーバのアドレスは通常、ボットバイナリに含まれているため、ボットはそのバイナリコードを解析・実行するときに当該 C&C サーバに直接接続できる。しかし、IP アドレスが固定的にコーディングされていると、いずれかのボットがブートストラップ中に捕捉及び傍受された場合に追跡されるリスクがある。より安全で信頼できる通信メカニズムを確立する方法として、ダイナミック DNS サービスがある。この仕組みを使用すれば、新たなサーバのダイナミック DNS エントリーに登録された（旧 C&C サーバの）IP アドレスを更新するだけで、ボットマスタは C&C サーバを自由に変更できる。このように、ボットは DNS サーバに照会を行うことによって C&C サーバに自動的に到達する。ボットマスタの立場からすると、一つの DNS サーバに新たな脆弱点が発生する可能性がある（ボットから同時に多量の照会メッセージが発生する可能性がある）のに対し、分散型の DNS サービスではそうした異常事態が低減され、C&C サーバの残存率が大幅に向上する。

必然的に生じるもう一つの基本的課題は、ボットがボットマスタと通信する方法である。実際にはボットが新しいプロトコルを生成するだけの差し迫った必要性はない。ボットはコンピュータに侵入するためにシステム及びソフトウェアの脆弱性を攻撃しなければならないため、感染したソフトウェアと同じプロトコルを使用する可能性がある。今日のボットネットの多くは IRC（Internet Relay Chat）プロトコルを使用している。このプロトコルは、複数の通信モード（例：ユニキャスト、ブロードキャスト、マルチキャスト）や多数のメンバによるデータ共有が可能である。IRC ベースのボットネットの場合、新しいボットはボットネットへの参加にあたって初めに IRC サーバにアクセスする。そのためには、ボットが IRC サーバ及び C&C チャネルに対して認証を行うことが必要である（ユーザ名とパスワード）。認証が正常に実施されるとボットはボットネットに組み込まれ、さらに処理をする権限を持つようになる（例えば、ボットマスタの指令を含んだチャネルトピックを解析して実行するなど）。しかし、IRC はボットとボットマスタ間の通信手段を提供するものの、自他を区別するためのコマンドセットはボットネットごとに異なる可能性がある。IRC ベースのボットネットに関する詳細な説明は文献[6]に記載されている。また、IRC ベースのボットネットにおける各バージョン間の総合的な比較が文献[3]において報告されている。

多くのボットネットが使用するもう一つのプロトコルは HTTP である。HTTP は今日のインターネットにおける主流プロトコルの一つであるため、ボットマスタはボットとの通信を膨大な通

常トラフィックの中に隠すことができる。それによって、トラフィックパターンの検査を手段としている多くの検知システムをごまかすことができる。言い換えれば、HTTP を使用するシナリオは IRC プロトコルのものよりはるかに多様かつ複雑であるため、HTTP ベースのボットネットのほうが生き残る機会は多いかもしれない。例えば、IRC ベースのボットネットが普及していることから大半のファイアウォールポリシーは IRC に関係するトラフィックを除外する。そのため、ヘッダやペイロードの解析[47]で多少の異常パケットが見つかったとしても、HTTP トラフィックを遮断することはまずできない。

中央管理型ボットネットでは IRCと HTTP のプロトコルが最も一般的であるが、IM、P2P 、VoIP など、分散型ボットネットで使用できる他のアプリケーションプロトコルも存在する。例えば、P2P のファイル共有プロトコルの脆弱性を突くことによって、Phatbot はあらゆる P2P ネットワーク内にボットネットを構築できる。MSN メッセンジャや SKYPE の脆弱性も、ボットによるランダム型ボットネットの構築を助ける可能性がある。

2.3 観察型のボットネット挙動

ボットネットはインターネット全域に広がっているため、最初の段階ではインターネット設備からデータを収集し、グローバルな観点から動作指標を指定するべきである。ボットネットの伝播を測定する日変化モデルが文献[13]に記載されている。これを使えば異なるボットネット間で伝播速度が比較でき、対応の優先付けが可能となる。Rajab ら[42]は、ボットネットの有効規模は文献[13]で推定する 35 万ボットではなく、数千を超えることはほとんどないと論じている。さらに、ボットネットの規模推定が依然として困難なものであり、一つの指標からボットネットの規模を推定することはできないことが示されている。逆に、ボットネットの挙動に関する複数の独立かつ並行した視点を組み合わせることで、より信頼度の高い推定が得られると思われる[43]。ただし、ボットネットの挙動は目的によって異なる可能性があるため、異なる指標が必要である。文献[14]は、様々な活動に対するボットネットの有用性を測るため、有効性、効率、頑健性の三つの指標を提唱している。文献[1]は、ボットネットの検知に関して関係性、応答、同期という上記とは異なる 3 種類の一般的指標を提唱しているが、その対象は協調的に振る舞う IRC ベースのボットネットに限られている。

このほか、ネットワークベースの異常検知では、有効かつ効率的な検知システムを設計するにあたって観察型分析が常に予備的かつ不可欠な工程になっている[52]。ボットネットは本質的にマルウェア駆動型のネットワーク異常であると考えることができる。そのため、特定の構成やプロトコルによらない観察型のボット挙動が、ボットネットに対する理解を深めてくれる可能性がある。特に、攻撃結果の面からボット挙動トレースの特性評価を実施すれば、特定のマルウェアの変種及び戦略が多量にカバーできるかもしれない。ボットとそれ以外のマルウェアでは挙動に基本的な違いはないため、特定の観察対象（例：ネットワークパケット、システムログ、ファイルシステム、メモリなど）に関する情報フロー、特にボットとボットマスタ間の通信中に生成されるものをシステム全体で収集・抽出すれば、ボットネットに特有の特徴が明らかになるかもしれない。システム正常性を測定するための観察カテゴリー[7]に従えば、ボットネットによって得られるトレースは以下のように記述できる。

- マクロレベル：ネットワークの長期的な平均挙動に関するもの。主にインターネットにおけるボットネットの協調的グローバル挙動。
- 中間レベル：トラフィックパターンやネットワークパケットなど、イントラネットレベルのイベントを調べる。主に空間・時間特性を調査する。
- ミクロレベル：ソフトウェアプログラム、各プロセス、システムコールといった OS 内の不可分操作のカーネルレベルにおける正確なメカニズムに焦点を当てる。

しかし、異なるレベルでの観察結果を分離することに固執することは、ボットネット挙動の理解にとって無用かつ無意味である。そのため、監視に役立つシステムスケールの観点からのみ分類を行う。具体的にいえば、マクロレベルのボットネット挙動は、DNS サーバなどインターネット

設備において観察できる[42]。多くのボットマスタは、配下のボットがC&Cサーバの IP アドレスの解決をするためにDNSサーバを使用することから、ある特定の DNS サーバのある一定期間内に、多量のクエリが発生することがある。この現象はボットマスタがC&Cサーバを変更したいときに出現する。このとき、すべてのボットは旧C&Cサーバとの接続を切り、(IP アドレスが異なる)新しいサーバに切り替える。すなわち、ダイナミック DNS のドメイン名を設定した DNS クエリを送出する。その様子はインターネットに分散する監視ツールの相関によって観察できる。中央管理型 C&Cサーバのボットネットでは、DNS クエリの集団挙動に加え、通常パターンとは大きく異なる異常なネットワークフローが引き起こされる場合がある。

中間レベルの観察は、通常、ボット、ボットマスタ、攻撃対象の間の通信によって得られる。それは特別な空間・時間特性を示す。一つ目として、ボットはバイナリ取得のためにC&Cサーバに接触する必要があるため、バイナリアップデートのリリースによって中央管理型の C&C サーバに多量のトラフィックが集まることがある(IP アドレスの照会が DNS サーバに集まるのと同様である)。二つ目に、ボットはボットマスタによって調整及び制御されるため、指令に対する応答は同時的であるとともに、遅延の様子も酷似している(人間の応答のようにばらつきがない)。したがって、ネットワークトラフィックの統計的性質は異常なパターンを示す(例：通常よりバースト性が高い)。三つ目として、ボットマスタの指令に対する応答において、ボットはターゲットに対して何らかの接続を開始する可能性がある。このとき、このボットのホストは正当なシステム動作によらない怪しげな出リンクを観察する。一般的にいえば、協調するボット群では通信トラフィック(ボットマスタへの上りリンク)と攻撃トラフィック(ターゲットへの下りリンク)が似通っているはずであり、両トラフィックのパターンもかなり似ている可能性がある。

ミクロレベルでのボット駆動による観察は、ワームやウイルスなど各種マルウェアの場合と本質的に同じである。マルウェアと正当なソフトウェアを分ける根本的特徴は、情報へのアクセス及び処理に関する動作がユーザの認識及び同意なく実行される点である。システム要素に及ぼす影響はボットによって異なるかもしれないが、ハードウェア状態からカーネルモジュールまで、システムの正常性に影響を与えるきっかけを作ることは共通している。例えば、ボットを実行すると、異常な監査イベントやシステムログファイルが生成される。アプリケーションポートを開き、また、ウイルス対策プログラムを無効にすることもある。悪質なコードの実行によって異常なプロセスやシステムコールのシーケンスが発生し、また、ウェブブラウザをねらったボットが API アプリケーションやシステムプロセス、あるいはブラウザヘルパオブジェクト(BHO)を呼び出すことがある。正当なプロセスではそのようなことは絶対に起こらない。ボットに顕著な特徴は、その目的から考えて、常に出側のネットワーク接続を試みることであり、それによってネットワークインタフェースにおいて異常なイベントが発生するのである。

3　ボットネットの強化

ボットネットはまだ発展途上であり、ボットネットの強化に向けて多くの技術が攻撃者たちによって開発される可能性がある。詳細な調査によって、既存ボットネットの多くには三つの脆弱性があることが分かっている。それは、C&Cサーバの構成、通信プロトコル、そして観察可能なボット駆動型トレースである。そのため、次世代ボットネットはこの3点の改善に取り組むことが考えられる。

3.1　C&Cモデルの頑健性向上

C&Cサーバが1台しかないボットネットは明らかに容易に発見・追跡できる。中央管理型C&Cモデルのボットネットの残存力はC&Cサーバの台数を増やすことによって高めることができるが、障害を根本からなくすことはできない。一部のボットネットはC&Cサーバの発見ないし追跡をできるだけ回避するため、**2.1** で述べたP2P型及びランダム型のC&Cモデルに移行している。その一方で、その構築と維持は複雑になる。このように、有効性、スケーラビリティ、遅延が

ある程度保証される局面では、より良いC&Cモデルに移行することが、頑健性と、構築及び維持の容易さとの間の最良のトレードオフになる。

文献[48]には混成P2P型のボットネットが提唱されている。これは一組のセンサホスト(下位ボット)を用いることでC&C機構を不要にする。センサホストはボットのピアリスト(規模一定)に掲載される。ボットマスタとボット間の通信は下位ボットによって中継される。また、この下位ボットはネットワークメンテナンスとボットのアップデートも請け負う。通信をセキュアにするため、各下位ボットは他のボットからの入接続に対して自分の共通鍵を生成する(共通鍵暗号方式)。このようなスキームの下位ボットはC&Cサーバの役割を果たす。その大前提は、その種のボットが固定的にコーディングされ、インターネットからアクセス可能なIPアドレスを持つことである。これは従来のC&Cサーバと基本的に変わらない。このスキームの有望な点は、各ボットが管理するC&Cサーバリストについて定期的な更新や他のボットとの交換が可能な点である。それによって、ボットネットは一部の下位ボットの障害によって影響を受けなくなる。また、ピアリストにはC&Cサーバに関する一部の情報が登録され、1回に交換される量が少ないため、一部のボットが捕捉された場合でもボットネットは追跡から逃れやすい。そのようなボットネットは分かりやすいC&C機構を採用するボットネットに比べて頑健性が高いことは確かだが、他のP2P型ボットネットと同様、スケーラビリティに乏しく遅延が大きいという問題が残る。また文献[27]で報告されているように、現実的には下位ボットの増加性がボットネットの成長に大きく影響する。C&Cサーバの数はせいぜい1日数百である。

ツリー構造のアルゴリズムが文献[46]において開発されている。このアルゴリズムによって、独立したC&Cサーバによって制御される小規模ボットネットを幾つか作成し、それを統合することによって一つのスーパーボットネットを構築する。特に、ボットネットの作成にあたってはボットマスタによって三つのパラメータが事前に設定される。具体的には、サブボットネットの数、サブボットの規模、そして一つのボットが新たに作成するボットの数である。このアルゴリズムは本質的に2段階で構成される。新しいC&Cサーバの作成(それぞれ一つのサブボットネットを制御する)と、各サブボットネットにおけるサブボットの作成である。スーパーボットネットの頑健性を高めるため、ツリー構造のバランスが維持される範囲内でC&Cサーバを意図的に孤立させ、互いに距離を置いて設置する。ボット感染率が高く、C&Cサーバが容易に使用できることを前提とすれば、このアルゴリズムは、理論上十分に機能する。ボットマスタはボットネットの全体像を知ることができないため、指令はボットネット全域を直接横断するのではなく、サブボットネット間をルーティングされる(そして各サブボットネット内のボットに到達する)。このプロセスをセキュアにするため、サブボットネット間通信に公開鍵暗号方式を使用し、サブボットネット内通信に共通鍵暗号方式を使用する。そのため、ボットネットの維持及び更新はその構築ほど容易ではない。また、常に遅延が大きく、サブボットネット同士が十分に協調しなければ有効な攻撃が実施できないことは明らかである。

この2種類の構想は、次世代ボットネットの意図に関する明確な見解を私たちに与えてくれる。それは、C&C機構によって生じるボットネットの弱点をなくすことである。そこで、より高度なC&C設計ができれば、耐障害性に優れたネットワーク接続機能、制御トラフィックの分散及びトラッキングの回避が実現するとともに、ボットマスタによる監視と保守が容易になると考えられる。ただし、IRCベースの中央管理型ボットネットは(表1に示すように)構築と維持の容易さ及び有効性によって、依然として有力な形態になるだろう。他方、それが将来のC&C機構と統合されれば、より大きな脅威になる。

3.2 通信チャネルの難読化

ボットネットがどのC&Cモデルを使用した場合でも、ボットマスタとボット間の通信チャネルはボットネットにとってもう一つの脆弱点である。これは、ボットトレースの露見や指令メッセージの傍受、解釈、改ざんにつながる可能性がある。これを回避するため、高度なボットマスタは通信チャネルを難読化して通信を秘匿すると考えられる。多くの場合、通信の難読化には認証、

権限確認、暗号化が用いられるが、詳細はC&C構成によって異なると思われる。非常に単純なケースの一つは、ボットが最初にIRCサーバに対して自分の認証を行い、次に通信チャネルの使用にパスワードが要求されるようなIRC型ボットネットである。ボットネットが他のボットマスタに乗っ取られるのを防止するため、ボットマスタのコマンド発行時に権限確認を必要とする場合もある[42]。

通信難読化の目的は、一般に、ボットネットトラフィックを通常のものに見せること及び通信内容の解釈を困難にすることである[22]。その直接的な方法の一つは、ボットがC&Cサーバへの接触に使用するサービスポートをランダム化することによって、ボットネットトラフィックを分散することである[48]。そうすることで、ポート固定の検知ツールによって容易に発見される単一ポートを使うのではなく、C&Cサーバに向かうボットネットトラフィックをある範囲内のポート（通常はSSHやHTTPSなどの標準ポート）に分散させることができる。ただし、一つのボットは通常、ある特定ポートをターゲットにするため、この詐術の実行にはボットの高い能力が要求される。通信トレースを隠すためにボットマスタは、TCPとICMPのトンネリングやIPv6トンネリング[26]などのチャネル変更通信を使うという方法もある。

別タイプの高機能ボットネットは最新の暗号化技術を駆使してボット、C&Cサーバ、ボットマスタ間の通信を難読化する。このタイプの難読化技術は、C&C構成とボットマスタの意図に大きく左右される。中央管理型C&C機構の場合、公開鍵方式のほうが適切かつ効率的である。鍵のペアである〈K^+, K^-〉はボットマスタによって生成される。公開鍵K^+は伝播中にボットのプログラムに埋め込まれ、秘密鍵K^-は後続指令を送るときのシグナチャとして用いられる。分散型C&Cサーバのボットネットでは共通鍵暗号方式のほうが有利である。これは、各ボットについてリストに登録するC&Cサーバが一つだけでなく、複数必要なことによる：Server_list＝{($Server_1$, k_1), ($Server_2$, k_2), …($Server_n$, k_n)}（$Server_i$はi番目のC&Cサーバを、k_iはiによって発行される鍵をそれぞれ表す）。そのため、ボットに格納される鍵を使えばリスト内のどのサーバにもコンタクトできる上、リバースエンジニアリングの防止にもなる。なぜなら、鍵はそのサーバに対するものであり、仮にそれが漏えいしたとしてもリストにない他のC&Cサーバの識別情報は必ずしも明らかにならないからである。さらに高度な例が文献[46]に記載された。これは、ツリー構造のC&Cサーバをセキュアにするため、公開鍵暗号方式と共通鍵暗号方式を併用する。具体的には、ボットマスタと全C&Cサーバとの通信の保護には公開鍵暗号方式を使用し、C&Cサーバと配下のサブボットネットとの通信の保護には共通鍵暗号方式を使用する。指令メッセージの完全性を確保するため、C&Cサーバ間にはSecret Splittingを用いる。この方式では、各コマンドが当該サブボットネットによって正しく復号された場合にのみ、暗号化されたコマンドが実行できる（サブボットは自分の公開鍵を使わないとコマンドを復号できない）。全ボットの動作を協調させるには、指令メッセージの形でボットネット全域を横断する所定の時限爆弾が使用される。

ボットネットの昨今の増加傾向を考えると、より高度なC&C構成の出現とともにより複雑な暗号化記述が使用されるようになっても不思議はない。ただし、ボットネットに内在する不安定性によって、ボットマスタは大胆な仮定をしないと実現できないものよりも現実的なスキームを採用せざるを得ない。文献[46]のスキームを改善するため、私たちはボットエンクレーブ（閉鎖的領域）という、強固なボットネットを提唱する（この発想は耐侵入性エンクレーブ[15]に似ている）。このボットネットは、ビザンチン挙動を伴うC&Cサーバの障害に強い。ボットエンクレーブはビザンチン耐障害性のプロトコルと秘密共有技術を併せ持ち、障害C&Cサーバの数が$f < [(n-1)/3]$（nは、当該ボットマスタが所有するC&Cサーバの総数）の条件を満たすときにボットマスタは配下のボットネットを稼働状態に維持できる。また、独立した複数のボットエンクレーブを組み合わせることによって階層的なボットエンクレーブが構築できる。ただし、ボットの応答遅延とエンクレーブの保守が大きな課題になる。

ボットネットは暗号化の利用によって通信の難読化を向上できるが、表1に示される他の指標を見ると、実際には諸刃の剣である。暗号化スキー

ムが複雑になるほどボットネットのセキュリティが高まる反面、複雑な暗号化スキームを実現するためにボットマスタは適切な鍵管理方法を慎重に設計しなければならない。ボットの協調的動作を同期するために決まった時間体系が必要になることから、ボットネットの有効性及び保守が妨げられる。暗号化技術は難読化の手段としては重要だが、それがボットネット強化のすべてではない。賢明なボットマスタは通信の難読化に全精力を注いだりしない。ボットネットにおける暗号化技術の使用を決めるもう一つの重要なファクタは、ボットマスタの意図である。例えば、ボットマスタの目的が DDoS 攻撃やスパム送信にある場合、一番重要なことはボットの応答と協調であるため、簡単な難読化技術を使えば十分である。逆に、ボットマスタのねらいが経済的利益を目的とした情報収集である場合、高度な難読化を行うほど利益は大きくなる。これは、配下のボットネットが DDoS のような攻撃後にすぐ停止するのでなく、できるだけ長期間稼働して多くの情報の獲得をねらっているからである。

3.3 その他の発見回避方法

上述した発見回避方法は予防的である。なぜなら、ボットマスタは実際に攻撃を仕掛ける前にボットネットを信頼可能かつセキュアにしておくことを意図しているからである。別タイプの発見回避方法は本質的に事後的である。その場合、ボットマスタはボットネットを事前に積極的に強化するのではなく、実行中の攻撃に対するボットネット対策技術を回避・処理する対策を取らざるを得ない。

ボットネット解析を行う最も一般的で効果的な方法の一つにハニーネット[24]がある（これについては **4.1** で取り上げる）。これはセキュリティ専門家だけでなく攻撃者の注目を集めている。高度な攻撃者は、捕捉・解析された場合、ハニーネットなどインターネットセキュリティセンサの存在に気付くボット群を開発したいと考える。様々なハニーポット対策技術については文献[23][37]において幅広く議論されている。一般に攻撃者の立場からすると、検知ターゲットは VMware などのエミュレート仮想環境を備えたハードウェア[9]か、またはハニーポットプログラムの誤応答のような動作を行うソフトウェアである。例えば、市販のスパム対策用ハニーポットツールが文献[33]に提唱されている。これは、リモート側の公開プロキシがスパム送信者に電子メールを返信可能かどうか試験することによってハニーポットを検知しようとするものである。また、文献[4]にはプローブ応答攻撃法が提唱されている。これは、自分たちの公開データを使ってインターネットセンサの位置を特定するものである。攻撃者のもう一つの攻撃点は、ハニーポットの利用が法的問題となる可能性がある[44]ことだ。そのため、プライバシー及び法的責任の制約から、ハニーポットは攻撃用トラフィックを実際に送出することができず、通常はそれが外に出て行くこと、またはある特定のターゲットに向かうことを阻止するだけである。この観察結果を受け、ハニーポットを意識した高度なボットネットが文献[53]に考案されている。具体的に、ボットマスタは他の感染ホスト（ボットネットセンサ）に悪意あるトラフィックを積極的に送出するよう配下のボット（特にハニーポットが疑われるもの）に指令し、被疑者ボットから送出されるトラフィックを観察することによって、あるボットがハニーポットか本当の被害者かを判断することができる。

別のタイプの発見回避方法は検知システムをターゲットにする。これはボット（より一般的にはマルウェア）作成者がホストレベルでよく使用する。その単純なものは、実行時にある特定の環境もしくは指示に合致した場合に、コンピュータにインストールされているウイルス対策ソフトを無効にする。もう少し高度なマルウェアであれば、検知ツールの動作アルゴリズムを改変しようとする。具体的に、マルウェア検知ツールはシグナチャ照合方式かアノマリー検知方式のいずれかが可能であり、攻撃者はいずれのタイプも回避できる。すなわち、プログラムの難読化によって、マルウェアはポリモーフィックでもメタモーフィックでもよいことになる[10][36]。攻撃者は検知ツールのシグナチャ生成を、意図的に誤らせることもできる[38]。アノマリー検知方式の検知ツールは模倣攻撃に弱い[5][32]。これは攻撃トレースに通常トレースを混在させるか、または通常のユーザ挙動を装う。ボットマスタは発見回避可能なボットを用いることで、新たなホストの感染成功率を

高めるとともに、ボットネットの稼働寿命を延ばすことができる。

4　ボットネットの制止

今日のコンピュータシステムにおける接続量と複雑さの増加及び各種マルウェアの急激な出現を考えると、私たちのコンピュータネットがボットネットに対して完全な抵抗力を持つことは不可能である。これまで多くのボットネット対策技術が開発されてきたが、いずれも決め手に欠ける。したがって、実用的な代替策は、適切な方法を組み合わせて強固なディフェンスラインを築くことである。対ボットネット防衛上の役割から、対策技術は基本的に予防技術、検知技術、トラッキング技術に大別される。検知技術は、観測のデータ源によってネットワーク型検知システムとホスト型検知システムの2種類に大別される。また、その設計スキームによってシグナチャ照合方式（パターンマッチング方式）とアノマリー検知方式（発見的検知方式）に分かれる。この節では、様々な課題を念頭に置きながら、既存のボットネット対策技術に関する比較研究及び批判的評価の基礎として、トップダウン解析の枠組みを作成したい。さらに、それを基にボットネットを制止する総合的方法を提唱する。

4.1　ボットネットの予防

今日のコンピュータネットワークにおいてハニーポットは、ファイアウォールやIDS（侵入検知システム）と並ぶセキュリティ対策の一つだと考えられている。これはセキュリティ管理者が意図的にトラップを設定するものである[2][12][16][29]。その目的は一般に次の三つである[41]。(1) ネットワーク上の相対的に重要なマシンから敵の注意をそらすこと、(2) 新たな攻撃トレンドについて早期に警告を発すること、(3) ハニーポットに対する脆弱性攻撃の最中及び終了後に徹底した調査を可能にすること、である。複数のハニーポットはハニーネットを構成する。認証、権限確認及び暗号化の諸技術は従来からセキュリティ対策と考えられているが、私たちの総合的なボットネット防衛法では、ハニーポットがボットを引き寄せて捕捉する作用を持つことから、ハニーポットを最初のディフェンスラインと位置付けている。

ハニーポットはワームの検知に成功してきた[12][45]が、ボットネットなど他種のマルウェアの増加に伴ってその役割がやや変化している。これまで、honeyd[41]、mwcollectとnepenthes[34]（両者は統合された）、honeytrap[25]など、多種多様なハニーネットのデーモン及びツールが開発されている。具体的に、honeydは仮想コンピュータシステムをネットワークレベルでシミュレートするための基盤を提供し、各種OSのホスト及び任意のルーティングトポロジーを持つネットワークに対して、大規模なハニーネット監視を実施することができる。また、mwcollectとnepenthesは主にマルウェアの収集に用いられる。これは、既知のパターンを使ってサンプルをダウンロードし、攻撃ペイロードからマルウェアバイナリを抽出する。それに対し、honeytrapはポートリスナを動的に作成してTCP接続のための試行動作を重点的に調査し、新規のマルウェアを扱う。

しかし、**3.3**で述べたように、ハニーネットは攻撃者のターゲットの一つになっており、高度なマルウェアであれば回避できる。この問題が未解決の場合、これに対処するためにはハニーポットをマルウェア自動検知ツールと統合し、ハニーポットの出力を使って攻撃シグナチャを生成・更新するのがよい。また、マルウェア検知ツールに従って未知の脆弱性に対するデータパッチ自動生成を行うことによって、ネットワークは新規の攻撃に対して抵抗力を持つことが考えられる。このようにして、ボットの伝播と感染を防止し、条件が良ければ、ボットネットの構築と成長を抑止するディフェンスラインが構築できる。

4.2　ネットワーク型のボットネット検知及びトラッキング

NIDSは20年以上も発展を続けている。NIDSのねらいは、ネットワークトラフィックのパターンの監視とネットワークパケットの検査によって攻撃を検知することにある。しかし、**2.3**で述べたように、ボットネットによって生じる観察結果は特別な特性を持つため、専用に設計されたNIDSが必要になる。

ボットネットはインターネット規模の問題であるため、ボットネットの検知とトラッキングには

当然ながらインターネット設備が最高位に置かれる。しかし、ボットネットのグローバルな動作特性は通常、ボットネットの構成とメカニズムに強く依存しており、それらはボットネットの基盤が変わらない限り変更されることはない。例えば、中央管理型 C&C ボットネットのトラッキングでは DNS サービスが重要な役割を果たす。これは C&C のアドレス及びドメインをボットが頻繁に変更するため、異常なアドレス照会やトラフィックパターンが発生するからである。興味深い発見が文献[30][42]に幾つか報告されている。一般に、関連性のあるスポットに対して監視ツールを配置した上で、監視結果を集約する分散型のアルゴリズムや技法を開発することが必要になる。設計原理を聞いただけでは実現可能に思えるが、実用的なツール、アーキテクチャ、あるいは方法はいまだ存在しない。一つの理由は、大規模なデータ収集及び解析に多くの時間と労力を要することである。もう一つの理由は、トラッキングによって無駄な保守費用が生じ、また、サービス品質に影響する恐れがあるため、かかわりたくないと考えるISP(インターネット接続事業者)が存在することである。

下位レベルでのボットネット検知は企業などのネットワークを対象とし、既存の研究の多くはこのレベルに集中している。ボットネットの検知及びトラッキング技術の設計を支える観察結果の多くは、ボットネットの特別な空間・時間特性である。それはボット、C&C サーバ、攻撃ターゲット間のトラフィックパターンから明らかにされた多段階かつ協調的な特性である。文献[20]は、ネットワークトラフィックにおける空間的・時間的相関を一連の統計アルゴリズムを用いて調査した。具体的には、協調的な通信、伝播、攻撃及び不正な活動に従事する一つのボットマスタが制御するボット群を観測した。IRC 型ボットネットに対する方法の限界を超えるため、上記の筆者らは別の検知体系を編み出した。それはボットネットの C&C 構成やプロトコルに依存せず、類似の通信トラフィック(ボットから C&C サーバへ)及び悪意あるトラフィック(ボットからターゲットシステムへ)をクラスタ化したあと、二つのクラスタの共通部に存在するボットを特定する[21]。ハニーネットはボットネット検知に加え、ボットネットのトラッキングに役立つツールの働きをする[2][16]。これを利用すれば、ボットネットの DDoS 攻撃について根本原因解析をすることが可能となる。

しかし、記載の検知システムが効果を持つのは、トラフィックパターンが観察可能であって、通常のパターンと大きく異なる場合に限られる。ボットネットのトラフィックパターンが例えば P2P ネットワークにおいて正常と区別がつかず、しかも転送パケットが暗号化されていれば、文献[39][50]のような更にミクロな解析・検知スキームが必要になる。

4.3 ホスト型ボットネット検知

ホストはボットネットの終端である。そのためボットネットを制止する直接的方法は、HIDS によってホストを感染から守ることである。NIDS と同様、ボットによって生じる観察結果には、他のタイプの攻撃とは異なる特徴がある。例えば、ボットとボットマスタはインタラクティブな通信を行うために従来の HIDS ではもはや役に立たず、専用のマルウェア及びボット検知ルールが開発された。

マルウェア検知ツールの設計原理は、マルウェアによってトリガされるホストにおいてシステム全域の情報フローを捕捉することである[49]。これを実現するにあたって最も有用なツールは仮想マシンである。これを使えば、ハニーポットが捕捉したマルウェアサンプルの解析やマルウェアシグナチャの生成が可能となる[5][10][38]。より具体的には、マルウェアのコード解析はスタティック及びダイナミックのいずれも可能である(マルウェアが実際に実行されるかどうかによる)[35]。言うまでもなく、マルウェア検知ツールには既知のマルウェアだけでなく、新規や回避可能なものまで検知することが期待される。

しかし、一部のマルウェア検知ツールはボットの検知に役立つものの、ボット特有の特徴に関連性がない場合、その有効性は低くなる。検知ツールがたとえボット専用に作られていなくても、基本的な考え方は文献[11]の構想のように説明できる。それは、出接続とユーザ駆動入力との関連性をプロセスレベルで調べることによって、ユーザが意図しない悪意ある出接続(extrusion)を捕捉す

る。ユーザ駆動入力はさらに文献[31]のようにシステム駆動に拡張できる。BHO とツールバーインタフェースイベントとの関係をユーザのブラウジング動作によって調査することで、スパイウェアの動作の特徴を明らかにする。同様の設計原理及びマルウェア感染の過程で発せられる観察結果の検査作業によって、Gu ら[19]は BotHunter を開発した。これは、マルウェアの異なる段階で動作する複数の IDS センサの関連性を調べることを目的とし、入力側の侵入アラームの会話痕跡と、ホスト感染を示す出力側の通信パターンとを結び付ける。

効果的なホスト型ボット検知ツールはホスト内の観察結果を必ずしも制限しないことが明らかとなった。むしろ根本的な問題を解決する必要がある。すなわち、ホスト内及び出接続リンクの観察結果をトリガしているのが本当に入接続リンクと正当なユーザ駆動及びシステム駆動の動作であるかどうかという点である。

4.4　ボットネット制止に向けた総合的方法

直観的に、ボットネットに対して有効な検知・トラッキングスキームを構築するためには、ボットネットによって生じるすべての情報フローを捕捉及び特性評価できる完璧な動作プロファイルが必要である。理想的なアプローチは、関連するすべての観察内容を各システムレベルで監視、抽出、相互の関連付けをし、さらにすべての基本特性（空間、時間、順序、秩序付けなどに関するもの）を調査することが可能なものである。ボットネットの特性を考慮に入れ、**2.3** で紹介した観察結果及びアーキテクチャの観点から考えると、各レイヤ（インターネット、イントラネット、ホスト）における観察結果及びボットネット対策ツールの結果を関連付け・統合し、ボットネットの全体的なスナップショットを得る方法を構想するのが正攻法である。最終的な目的は、ボットネットの検知とトラッキングを実現すること及びボットネット駆動攻撃に対して根本原因解析を実施することである。

ボットネット検知を実行するための総合的な枠組みを図 3 に示す。ツールやコンポーネントの表示はあくまでも説明のためのものであり、実際の環境における適用や実装を表しているわけではない。トップダウン解析方式における総合的な方法について以下に説明する。

- グローバル監視をする分散型セキュリティ検知ルールを開発・配置し、インターネット設備上で発生するクロスサイトの疑わしい観察結果を分析する分散型アルゴリズムを設計する。
- NIDS 検知ツールやハニーネット報告を解析するためのクラスタ化（クロスクラスタリング）アルゴリズム及びベイズ推論のような統計的アルゴリズムを設計・実施する。これは、感染ホストのピンポイント特定、ボットネットのトラッキング及び攻撃の根本原因（スパミング攻撃のスパム発信者など）の推論を目的と

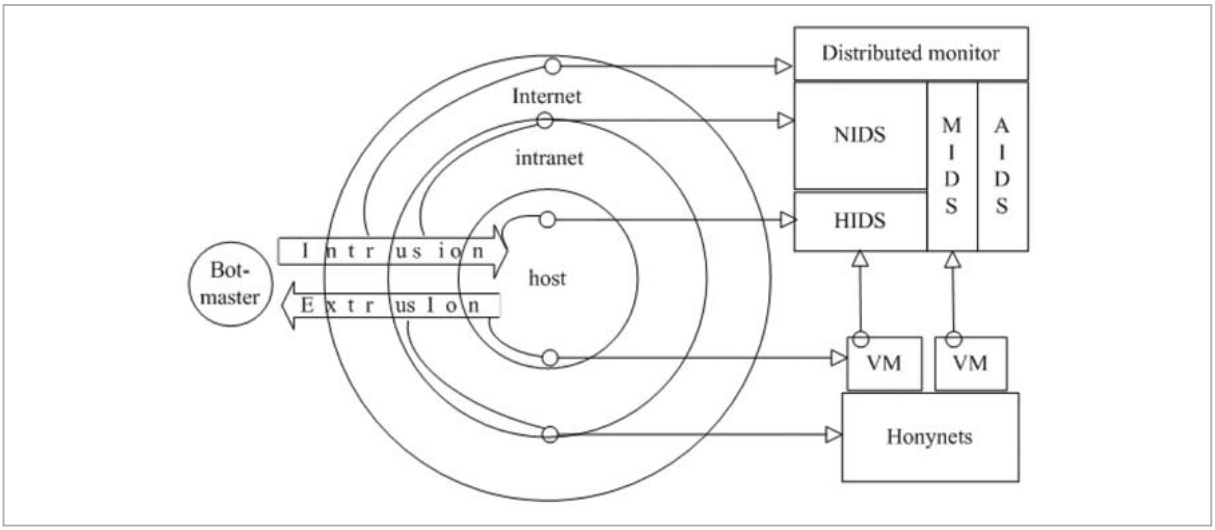

図3　ボットネット検知を行う総合的な枠組み

する。

- ミクロなホスト型ボット解析を行うマルウェア検知ツールを開発する。

このような枠組みには3層のレイヤが存在するが、ボットの痕跡及び攻撃シーケンスは3層で独立して発生するのでなく同時に発生するため、3層のレイヤは本質的に緊密に統合される。また、新規の検知スキームを常に開発する差し迫った必要性はなく、Snort[28]やPAYL[47]といった最先端のツールが、ボットに関する異常なネットワークパケットの検知に役立つ可能性がある。

もう一つの重要な課題は、発見したボットネットに対する対応である。ボットネットはいわば成長過程にあり、闇市場ではますます多くのボットネット管理者の注目を集めている[17]ため、ボットネットの検知とトラッキングを単なるセキュリティ専門家を対象にした技術問題(例：ボット、更新システムパッチ及びウイルス対策ソフトのボットシグナチャの駆除)として扱うことができなくなっており、インターネット犯罪に関する社会問題となっている。そのためボットネットに対する対応は特定の被害者におけるボット駆除には制限されない。また、ボットが様々な場所に広範囲に拡散することで、ボットネットはインターネット全体に広がる可能性があるため、ISPにまたがる国際的な協力(例：DNSサービス)や法の施行における国家間の協力が必要である。

5 まとめ

ボットネットはその耐久力、範囲の広さ、そして悪意性によって、私たちのサイバー空間にとって深刻な脅威の一つになっている。本稿ではその特性を、解析及び理解の基礎とし、次世代ボットネットの特徴や発見回避方法について探究した。次に、現在のボットネット対策技術を概観し、ボットネットを制止する強固なディフェンスラインの実現に向けて適切な技術を統合する総合的な方法を提案した。

ボットネットはますます高度化しているため、次の段階では、ボットネットの強化に使用される可能性のある手段や技術について調査したいと考えている。敵の動作を根本的に理解して事前に発見することは、いつの場合でも効果的な対策を開発・設計する王道である。私たちの最終的な目的は、ボットネットの根本原因を推論する体系的なアプローチを本稿で提示した方法に従って開発することである。その基礎となるのが、各システムレベルで収集した観察結果及び各所に配置したボット検知ツールの結果であり、それらはボットネットの抑止と法の執行に向けた説得力のある証拠を提供してくれる。

参考文献

1 M. Akiyama, T. Kawamoto, and M. Shimamura et al., "A proposal of metrics for botnet detection based on its cooperative behavior", In Proc. of the 2007 International Symposium on Applications and Internet Workshops (SAINTW'07), 2007.

2 P. Bacher, T. Holz, M. Kotter, and G. Wicherski, "Know your enemy: tracing botnet", http://www.honeynet.org/papers/bots/

3 P. Barford and V. dYegneswaran, "An inside look at botnets", In Proc. of Special workshop on malware detection, Advances in Information Security, 2006.

4 J. Bethencourt, J. Franklin, and M. Vernon, "Mapping Internet Sensors With Probe Response Attacks", In Proc. of USENIX Security Symposium, pp.193-208, Aug. 2005.

5 K. Borders, X. Zhao, and A. Prakash, "Siren: catching evasive malware", In Proc. of IEEE Symposium on Security and Privacy (S&P'06), May 2006.

6 D. Brumley, "Tracking hackers on IRC", http://www.indonesiajakarta.org/home/

7 M. Burgess, H. Haugerud, S. Straumsnes, and T. Reitan, "Measuring system normality", ACM Transactions on Computer Systems, Vol.20, No.2, pp.125-160, May 2002.

8 E. Burgess, F. Jahanian, and D. McPherson, "The Zombie roundup: understanding, detecting, and disrupting botnets", In Proc. of the Steps to Reducing Unwanted Traffic on the Internet on Steps to Reducing Unwanted Traffic on the Internet (SRUTI 05), Jun. 2005.
9 J. Covery, "Advanced Honey Pot Identi¯cation And Exploitation", http://www.phrack.org/fakes/p63/p63-0x09.txt, Jan. 2004.
10 M. Christodorescu, S. Jha, S. A. Seshia, et al., " Semantics-aware malware detection", In Proc. of IEEE Symposium on Security and Privacy (S&P'05), pp.32-6, May 2002.
11 W. Cui, R. H. Katz, and W. Tan, "Design and Implementation of an Extrusion-based Break-In Detector for Personal Computers", In Proc. of The 21st Annual Computer Security Applications Conference (ACSAC 2005), Dec. 2005.
12 D. Dagon, X. Qin, G. Gu, et al., "Honeystat: Local worm detection using honeypots", In Proc. of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID 2004), pp.39-58, Sep. 2006.
13 D. Dagon, C. C. Zou, and W. Lee, "Modeling botnet propagation using time zones", In Proc. of the 2006 Network and Distributed System Security Symposium (NDSS 2006), pp.235-249, Feb. 2006.
14 D. Dagon, G. Gu, C. P. Lee, and W. Lee, " A taxonomy of botnet structures", In Proc. of the Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007), pp.325-339, Dec. 2007.
15 B. Dutertre, V. Crettaz, and V. Stavridou, "Intrusion-Tolerant Enclaves", In Proc. of IEEE Symposium on Security and Privacy (S&P'02), pp.216-226, May 2002.
16 F. C. Freiling, T. Holz, and G. Wicherski, "Botnet tracking: exploring a root-cause methodology to prevent DDoS attacks", In Proc. of 10th European Symposium On Research In Computer Security (ESORICS 2005), pp.319-335, Sep. 2005.
17 N. Friess, J. Aycock, and and R. Vogt, "Black Market Botnets", In MIT Spam Conference, 2008, pp.1-8, 2008.
18 D. Geer, "Malicious bots threaten network security", IEEE Computer, Vol.38, No.1, pp.18-20, Jan. 2005.
19 G. Gu, P. Porras, and V. Yegneswaran, et al., "BotHunter: Detecting Malware Infection Through IDS-Driven Dialog Correlation", In Proc. of the USENIX Security Symposium (Security'07), Aug.2007.
20 G. Gu, J. Zhang, and W. Lee, "BotSniffer: Detecting Botnet Command and Control Channels in Network Traffic", In Proc. of the 15th Annual Network and Distributed System Security Symposium (NDSS'08), Feb. 2008.
21 G. Gu, R. Perdisci, J. Zhang, and W. Lee, "BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-Independent Botnet Detection", In Proc. of the the USENIX Security Symposium (Security'08), Aug. 2008.
22 M. Handley, C. Kreibich, and V. Paxson, "Network Intrusion detection: Evasion, Traffic Normalization, and End-to-End Protocols Semantics", In Proc. of the USENIX Security Symposium, Aug. 2008.
23 T. Holz and F. Raynal, "Defeating Honeypots: System Issues (Part 1,2)", SecurityFocus InFocus Article, Sep. 2004.
24 http://www.honeynet.org/
25 http://honeytrap.mwcollect.org/
26 http://www.uscert.gov/reading room/IPv6Malware-Tunneling.pdf
27 http://atlas.arbor.net/summary/botnets/
28 http://www.snort.org/

29 X. Jiang and D. Xu, "Collapsar: A VM-Based Architecture for Network Attack Detention Center", In Proc. of the 13th USENIX Security Symposium, pp.1528, 2004.

30 A. Karasaridis, B. Rexroad, and D. Hoe°in "Wide-scale botnet detection and characterization", In Proc. of the First Workshop on HotTopics in Understanding Botnets (HotBots07), Apr. 2007.

31 E. Kirda, C. Kruegel, G. Banks, et al., "Behavior-based Spyware Detection", In Proc. of the 15th USENIX Security Symposium, pp.273-288, 2006.

32 C. Kruegel, E. Kirda, D. Mutz, et al., "Automating mimicry attacks using static binary analysis", In Proc. of the 14th USENIX Security Symposium, pp.161-176, 2005.

33 N. Krawetz, "Anti-Honeypot Technology", IEEE Security & Privacy Magazine, Vol.2, No.1, pp.76-79, Jan./Feb. 2004.

34 http://www.mwcollect.org/

35 A. Moser, C. Kruegel, and Engine Kirda, "Exploring multiple exectuion paths for malware analysis", In Proc. of IEEE Symposium on Security and Privacy (S&P'07), May 2007.

36 C. Nachenberg, "Computer virus-antivirus coevolution", Communiations of the ACM, Vol.40, No.1, pp.46-51, Jan. 1997.

37 L. Oudot and T. Holz, "Defeating Honeypots: Network Issues (Part 1, 2)", SecurityFocus InFocus Article, Sep. 2004.

38 R. Perdisci, D. Dagon, W. Lee, et al., "Misleading worm signature generator using deliberate noise ijnection", In Proc. of IEEE Symposium on Security and Privacy (S&P'06), May 2006.

39 M. Polychronakis, K. G. Anagnostakis, and E. P. Markatos, "NetworkLevel Poly-morphic Shellcode Detection Using Emulation", In Proc. of Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2006), pp.54-73, 2006.

40 R. Puri, "Bots & botnet: an overview", http://www.sans.org/reading room/whitepapers/malicious/1299.php, Sep. 2004.

41 N. Provos, "A Virtual Honeypot Framework", In Proc. of the 13th USENIX Security Symposium, Aug. 2004.

42 M. A. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, "A Multifaceted Approach to Understanding the Botnet Phenomenon", In Proc. of the 6th ACM SIGCOMM, conference on Internet measurement (IMC'06), pp.41-52, Oct. 2006.

43 M. A. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, "My Botnet Is Bigger Than Yours (Maybe, Better Than Yours): Why Size Estimates Remain Challenging", In Proc. of the First Workshop on HotTopics in Understanding Botnets (HotBots07), Apr. 2007.

44 Lance Spitzner, "Honeypots: Are They Illegal?", SecurityFocus InFocus Article, Jun. 2003.

45 Y. Tang and S. Chen, "Defending against internet worms: a signature-based approach", In Proc. of the IEEE INFOCOM, May 2006.

46 R. Vogt, J. Aycock, and M. J. Jacobson, Jr., "Army of Botnets", In Proc. of the 2007 Network and Distributed System Security Symposium (NDSS 2007), pp.111-123, Feb. 2007.

47 K. Wang and, S. J. Stolfo, "Anomalous payload-based network intrusion", In Proc. of the 7th International Symposium on Recent Advances in Intrusion Detection (RAID 2004), pp.203-222, Sep. 2004.

48 P. Wang, S. Sparks, and C. C. Zou, "An advanced hybrid peer-to-peer botnet", In Proc. of the First Workshop on HotTopics in Understanding Botnets (HotBots07), Apr. 2007.

49 H. Yin, D. Song, M. Egele, et al., "Panorama: Capturing System-wide Information Flow for Malware Detection and Analysis", In Proc. of the 14th ACM Conference on Computer and ommunications Security (CCS'07), Oct. 2007.

50 Q. Zhang, D. S. Reeves, P. Ning, and S. P. Iyer, "Analyzing Network Traffic To Detect Self-Decrypting Exploit Code", In Proc. of the 2nd ACM symposium on Information, computer and communications security (AsiaCCS'07), pp.4-12, 2007.

51 Z. H. Zhang, P. -H. Ho, X. Lin, and H. Shen, "Janus: A Two-Sided Analytical Model for Multi-Stage Coordinated Attacks", In Proc. of the 9th International Conference on Information Security and Cryptology (ICISC2006), LNCS 4296, pp.136-154, Dec. 2006.

52 Z. H. Zhang, "Adaptive Observation-Centric Anomaly-based Intrusion Detection: Modeling, Analysis and Evaluation", Ph. D thesis, JAIST, Mar. 2006.

53 C. C. Zou and R. Cunnigham, "Honeypot-aware advanced botnet construction and maintenance", In Proc. of Int. Conf. on Dependable Systems and Networks (DSN2006), pp.199-208, Jun. 2006.

張　宗華（Zhang Zonghua）
情報通信セキュリティ研究センター
レーサブルネットワークグループ専攻
研究員　博士（工学）
ネットワークセキュリティ

門林雄基（かどばやしゆうき）
情報通信セキュリティ研究センター
レーサブルネットワークグループ客員
研究員　博士（工学）
ネットワークセキュリティ