- 本資料は下記論文を基にして作成されたものです。文書の内容の正確さは保障できないため，正確な知識を求める方は原文を参照してください。
- Botnet Tracking: Exploringa Root-Cause Methodology to Prevent Distributed Denial-of-Service Attacks

著者 Felix C. Freiling, Thorsten Holz, and Georg Wicherski

- JPCERT CC

ボットネットの概要～報告書～

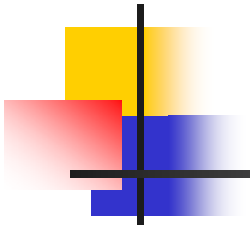
有限責任中間法人JPCERT コーディネーションセンター

- 【特集】ハニーポットを利用したネットワークの危機管理
  ～おとりサーバで侵入者、攻撃者の手法を分析～

  田原祐介
  株式会社ラック
  ／不正アクセス対策事業本部

Botnet追跡
～分散型サービス妨害攻撃を防ぐ～

渡辺研究室
040427493　間宮領一



はじめに

- DoS (Denial of Service)攻撃

  インターネット犯罪で増加しているのは、サービス妨害と呼ばれている。

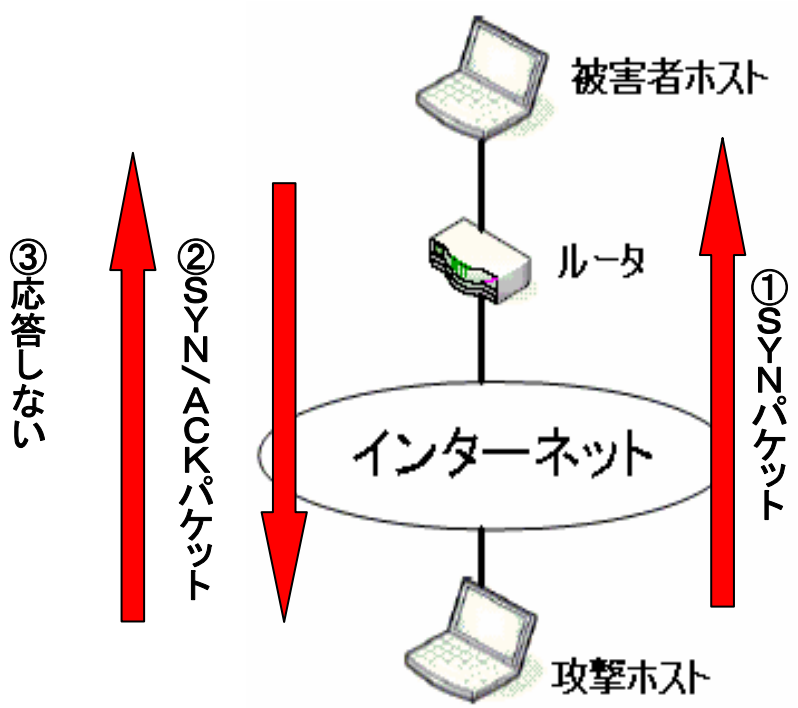
  DoS攻撃はユーザに対しコンピュータのリソースをたくさん積み上げることにより接続性を損失させネットワークの帯域幅を消費させるネットワークへの攻撃。

はじめに

- TCP SYNフラット攻撃

①SYNパケット送信
②SYN/ACKパケット受信
③応答しない

以上より被害ホストは
ACKパケットを永遠に
待ち続けリソースを無駄に
消費してしまいTCP
接続を受け付けられなくなる



はじめに

- これはIPアドレス上でパケット分配を見ることによりひとつの発生源からの攻撃を検出し特定はできる。しかし複数の攻撃ホストが連携していると特定は原則不可能。

- 複数の発生源からの攻撃を、分散型サービス妨害(Distributed Denial of Service)という。

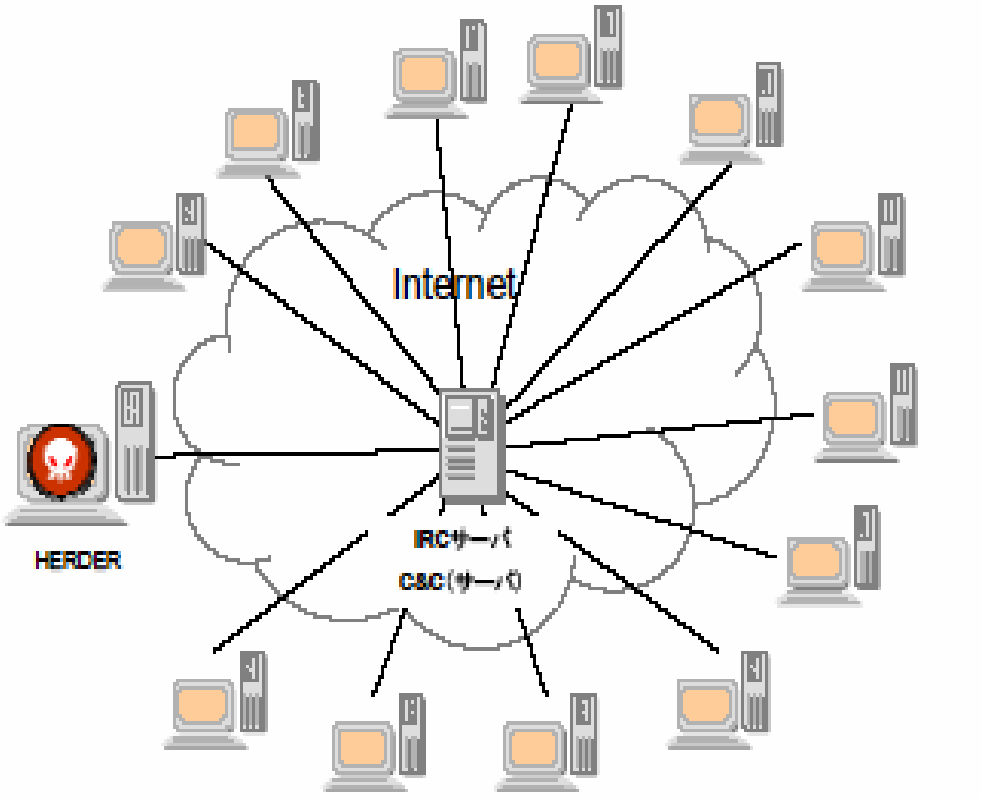
Botnetを使用するDDoS攻撃

- Botnetとは

  一般的なC&C(Command＆Control)インフラストラクチャの下でbot、ゾンビ、有人機などとよばれる遠隔操作プログラムに感染しているマシンのネットワーク。

Botnetを使用するDDoS攻撃

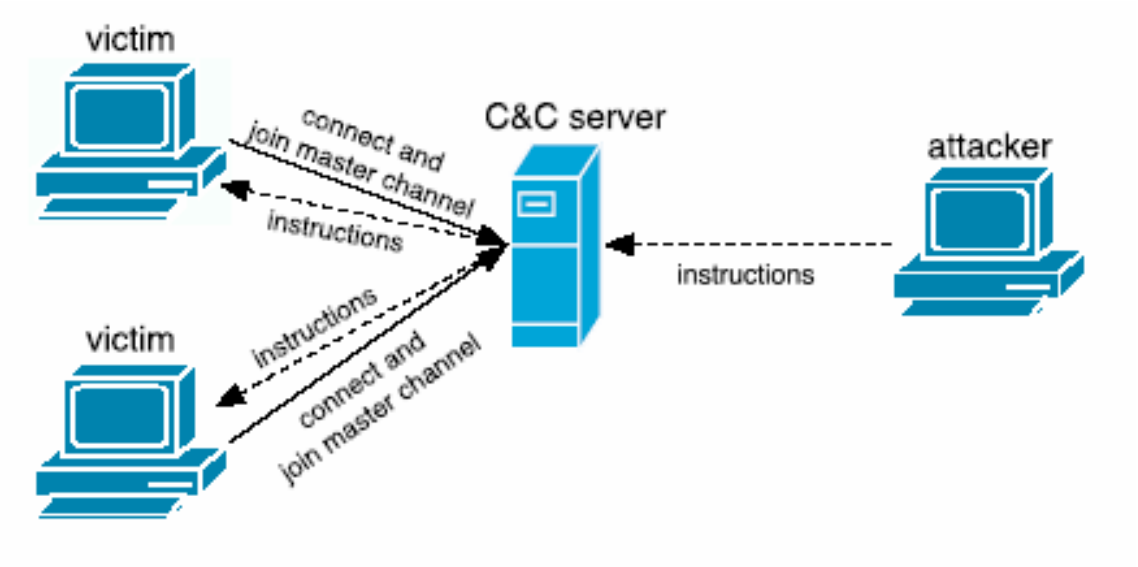
- Botnetのネットワーク構成



Botnetを使用するDDoS攻撃

- Botnetのコントローラはさまざまなツールを使用する一連のシステムに感染、次に、IRC(Internet Relay Chat)を通して遠隔操作を可能にするためにbotを犠牲者コンピュータにインストールする。
- より新しいbotは他のマシンの脆弱性と弱いパスワードを使用して自動的にネットワーク範囲をスキャンし繁殖する。
- bot自体を感染されたホストに移すためにTFTP、FTP、HTTPなどを使用。
- バイナリーは始められて、botインフラストラクチャを保護するのにサーバパスワードを使用して、事前に定義されたポート上のコード化されたIRCサーバに接続しようとする。
- このサーバはbotnetを管理するためにC&Cサーバとして機能。難しいコード化されたIPアドレスよりダイナミックなDNS名を提供するため、botは容易に移動することが出来る。
- ここで作られた名前とチャンネルパスワードを使用しbotはマスターチャンネルに合流しようとする。このチャンネルにより遠隔操作が可能。

Botnetを使用するDDoS攻撃



図：botnetでのコミュニケーション流動

Botnetを使用するDDoS攻撃

- 一般的に実装されている攻撃コマンド例

①TCP SYNフラット攻撃

ddos.syn XXX.XXX.XXX.XXX 80 600

　指定されたIPアドレスに600秒間TCPポート80に対してTCP SYNフラッディング攻撃を行う。

②UDPフラット攻撃

udp XXX.XXX.XXX.XXX 18000 50000 100

　指定された目標に50000バイトのサイズを各パケット間で100msの遅れで18000パケットを送りUDPフラッディング攻撃を行う。

Botnetを分析するために

- DDoS攻撃を仕掛けるには

①多くの感染しているマシンが必要

②多くのマシンを調整するための遠隔操作メカニズムが必要

③遠隔操作メカニズムに障害があると防がれる

Botnetを分析するために

- 多くのマシンが必要な理由

攻撃者の総リソースが犠牲者のリソースより大きい場合にだけDDoS攻撃が成功。

また攻撃マシンは特定されないように、IPスプーフィングを使い攻撃マシンの実数を変装する。

Botnetを分析するために

- 遠隔メカニズム

攻撃に参加する多くのホストの動作が攻撃の時間と同様に交通(犠牲者のアイデンティティ)のタイプに関してしっかり調整されていることが不可欠。

Botnetを分析するために

- 遠隔メカニズム

攻撃開始時間や犠牲者のアイデンティティなど全ての情報を直接ネットワークを形成するゾンビに感染しているマルウェアにコード化して攻撃者を探し出すのを困難のする

Botnetを分析するために

- 攻撃を防ぐために

①遠隔操作ネットワークに浸透する。

②詳細にネットワークを分析する。

③遠隔操作ネットワークをとめる

という段階を踏む

Botnetを分析するために

- 遠隔操作ネットワークに浸透する方法

  ゾンビは自分たちと攻撃者の間の通信チャンネルを確立する必要がある。

  制御された方向でマルウェアを捕まえ情報を抜き出す。

以下にIRCベースのBotnetを浸透して追跡したかを説明する。

追跡Botnet

- 前述どおり追跡Botnetは明確に他段階操作。
- 既存のBotnetに関するいくつかのデータをBotnetの助けを借りるか、捕らえられたマルウェアを分析して集める必要がある。

追跡Botnet

- Botnetに浸透するための必要事項
  - IRCサーバとポート番号のDNS/IPアドレス。
  - IRCサーバ（オプションの）に接続するパスワード。
  - botとident構造のあだ名。
  - 合流して、パスワードを向ける（オプションの）IRCチャンネルの名前。

追跡Botnet

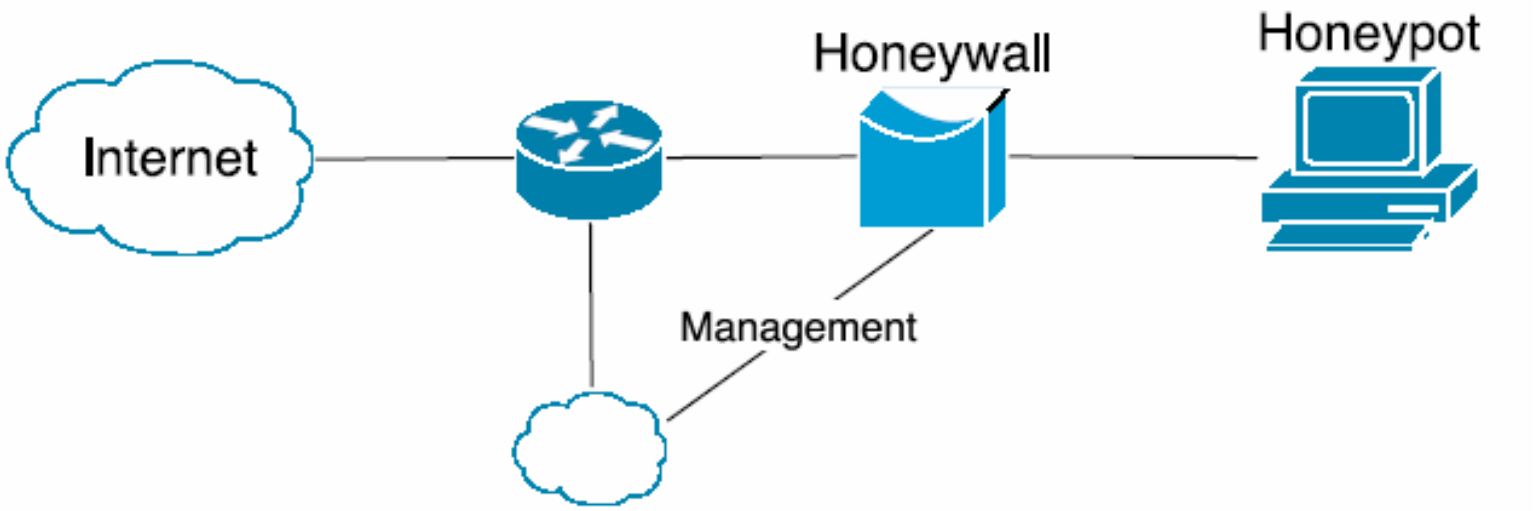
- ハニーポットでマルウェアを集める。
- ハニーポットとは

徹底調査されるために配備されて、攻撃されて、危うくされるネットワーク資源（コンピュータ、ルータ、スイッチ、その他）です。honeynetは、ハニーポットのネットワークです。

追跡Botnet

- honeynet

いくつかのWindowsハニーポットを含んでいてGen II Honeynetを配備



図：追跡botnetsのためのセットアップ

追跡Botnet

- ハニーポットの寿命は平均10分未満
- オートメーション化したマルウェアにしばしば使用される
- botに感染した後ハニーポットを攻撃して、次にコマンドを得るためにC&Cサーバに接続を試みる
- Honeywallがプレーにはいる

追跡Botnet

- Honeywall

  2つのタスクDataControlとDataCaptureを有効にする透明なブリッジで、DataControl施設のために、外向的なトラフィックを制御する 。

botがマスターチャンネルから有効なコマンドを受け入れるのを禁止できる。

追跡Botnet

- DataControl

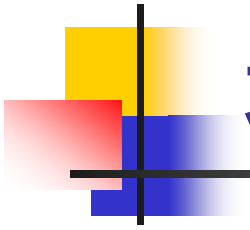
  命令と支配のための疑わしい典型的IRCメッセージを置き換える。

- DataCapture

  ボットがつながりたいDNS/IPアドレス、更には対応するポート番号を測定。

追跡Botnet

- 必要な情報を集め、ハニーポットは更なるマルウェアを捕えることができた。
- 捕えられたマルウェアを心配しないで、毎日「きれいな」システムを持つために24時間ごとハニーポットを作り直す。



追跡Botnet

- Mwcollectでマルウェアを集める。

  前のセクションで記述したアプローチには、いくつかの欠点がある。

追跡Botnet

- 欠点

①功績の範囲内の間違ったオフセットのために、botが提供されたサービスを利用できないならば、ハニーポットは定期的にクラッシュする。

②ハニーポット自体はシステム上の変化を検出するために慎重に分析しなければいけない。

追跡Botnet

- mwcollect

  非ネイティブ環境でマルウェアを捕らえる 。

  いくつかの傷つきやすいサービスをシミュレートして、それらが利用されるのを待つプログラム。

  モジュールで組み立てられたデザインで、4つのモジュールからなっている。

追跡Botnet

- 脆弱性モジュール

  いくつかの傷つきやすいポート(例えばTCPポート135か2745)をあけてポートにしたがって脆弱性をシミュレートする。
- Shellcode構文解析モジュール

  Shellcode脆弱性モジュールのひとつで受け取られたシェルを実行するプログラムを分析。これらのモジュールはShellcodeから一般的なURLを抜粋しようとする。

追跡Botnet

- 獲得モジュール

  単にURLによって指定されるファイルをダウンロードします。

- 服従モジュール

  うまくダウンロードされたファイルをたとえばディスクにそれを書くかそれをデータベースに提出することによって、処理します。

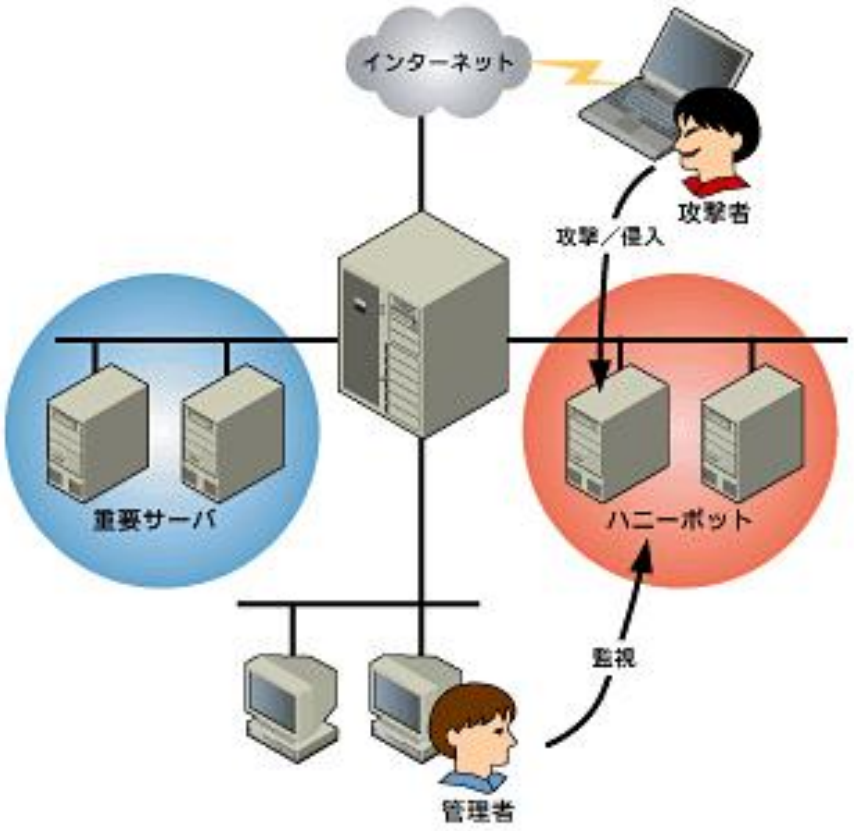
追跡Botnet

- マルウェアを集める
- シェルエミュレーション

シェルを通してホストを感染させる。

一時ファイルにマルウェアをダウンロードして、実行するためのコマンドを書いて、ファイルを実行する。このタイプの攻撃を可能にするため仮想ファイルシステムが使われた。

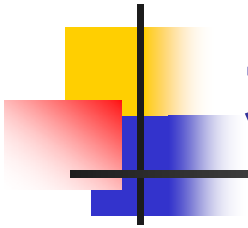
追跡Botnet



追跡Botnet

- マルウェアから情報を抜粋する

時間がかかるが、リバースエンジニアリング(ソースコードを持たずプログラムを分析する)を使う。



追跡Botnet

- Honynetを使う

Windowsハニーポットはインターネットのどこかに位置したデータベースから一片のマルウェアをダウンロード。それはファイルを実行し数分後にそれを自体をリブートする。

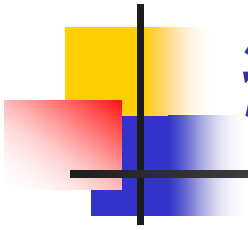
このタイムスパンの間にbotはハニーポットにインストールしC&Cサーバに接続する。

追跡Botnet

- Honeywallにより必要事項を抜粋
- また、ハニーポットが各リブート間ハードディスクをリセットする
- botを実行する仮想環境により清潔なイメージをその都度、起動。
- よって効率的にマルウェアを分析することが出来る。

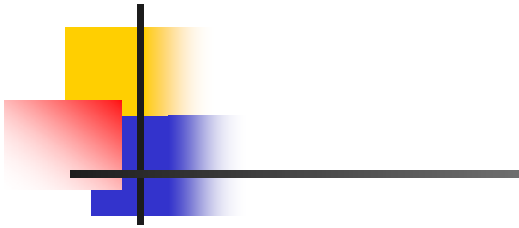
BotnetによるDDoS攻撃を防ぐ

- C&Cサーバを修正することによって混乱しない限りbotのIPアドレスを観察できる。
- Botnetをとめるためには C&Cサーバをとめる。
- 個人サブネットでIPアドレスに分解するようにDNS名が変わるならばbotは中心サーバに接続できなくなり、遠隔操作ネットワークは能率的に閉鎖される。しかしDNSプロバイダの支援が必要。



結果

- 5ヶ月で180botnetを追跡。
- １００万人以上のホストが危うくされて、悪意のある攻撃者によって制御されていることがわかった。
- 自動的に集めたファイルを分析するためにいったん仮想メカニズムを実行。C&Cサーバをとめることによって攻撃を防ぐのにこれを使用できる。



- おわり