ボットネットのメカニズムについて

株式会社セキュアブレイン
星澤　裕二

2005.4.27

SecureBrain

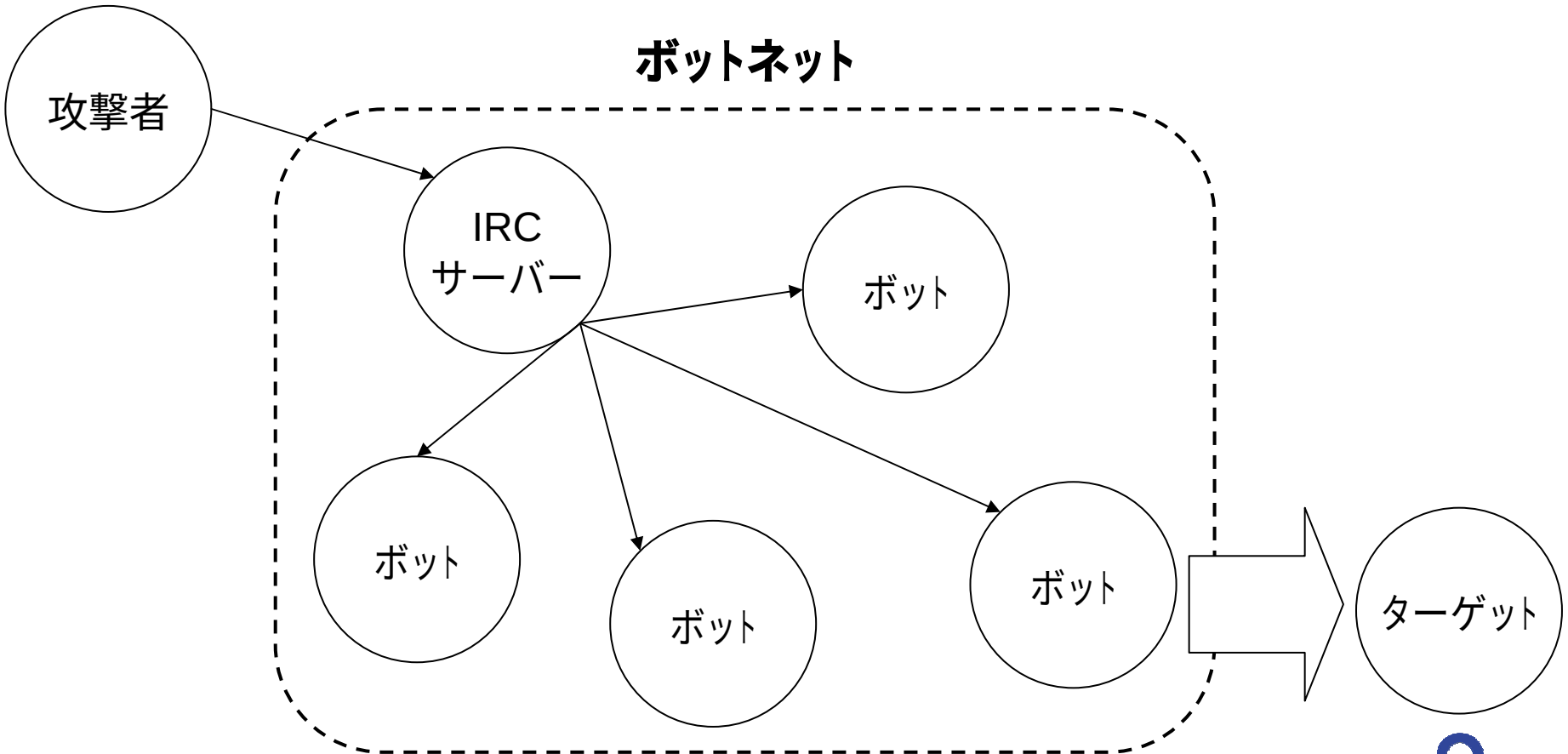
ボットネットとは

- 外部からの命令を待ち、その命令に従って何らかの動作をするプログラムを「ボット（bot）」と呼ぶ
- ボットは「ロボット（robot）」の略
- Gaobot（Agobot）やSpybotのようにプログラム・ソースが公開されているものがある
- 攻撃者はIRCなどを使ってボットに命令を出す
- 複数のボット・マシンで構成されたネットワークを「ボットネット（botnet）」や「ボット・ネットワーク（bot network）」と呼ぶ
- ゾンビクラスタ（Zombie Cluster）とも呼ばれる

SecureBrain

Copyright (c) SecureBrain Corporation. All rights reserved.

ボットネットのイメージ



SecureBrain

Copyright (c) SecureBrain Corporation. All rights reserved.

ボットの感染方法

- P2Pファイル共有
- Windows ファイル共有
- Sub SevenやKuang2などのバックドアを利用する
- セキュリティホールを利用して侵入
- マスメーラー型ワームによって投下される
- ソーシャルエンジニアリング（人の心理を突き、うっかりファイルを開いてしまうように仕向けるテクニック）

SecureBrain

Copyright (c) SecureBrain Corporation. All rights reserved.

攻撃の種類

- フィッシングサイトなどを開設
- スパムメールやフィッシングメールの送信
- DOSコマンドの実行
- キーボード入力の記録
- ファイルの送受信
- プログラムの実行
- DoS攻撃（SYNフラッド、ICMPフラッド、UDPフラッドなど）

SecureBrain

Copyright (c) SecureBrain Corporation. All rights reserved.

Gaobotのコマンド例

command.list: コマンド一覧の表示

bot.quit: ボットを終了

irc.server: 接続するIRCサーバーを変更

http.update: Webサイトに接続してボットを更新

ftp.download: FTPサイトからファイルをダウンロード

scan.netbios: アクセス可能なネットワーク共有を探す

ddos.synflood: SYNフラッドの開始

cdkey.get: プロダクト・キーを取得する

SecureBrain

Copyright (c) SecureBrain Corporation. All rights reserved.

Spybotのコマンド例

uninstall: レジストリのスタートアップキーから削除

httpserver: HTTPサーバーを起動

list: ファイルリスト表示

execute: 指定プログラムの実行

sendkeys: キーボード入力をシミュレートする

syn: SYNフラッド

startkeylogger: キーボード入力を記録

killprocess: プロセスを終了する

SecureBrain

Copyright (c) SecureBrain Corporation. All rights reserved.

問題点

- ソースコードが公開されているものもあり、亜種を作りやすい状況になっている
  - アンチウイルスベンダーのデータファイルの更新が間に合わない
- パッカー (packer) を利用
  - プログラムの解析を困難にする
  - 亜種が簡単に作れる
- IRCサーバーはダイナミックDNSを利用

SecureBrain

Copyright (c) SecureBrain Corporation. All rights reserved.