C&C セッション分類によるボットネットの検出手法の一検討
An investigation of Botnet Detection Techniques by C&C Session Classification

阿部　義徳†　　田中　英彦†
Yoshinori Abe　　Hidehiko Tanaka

１．　まえがき

OS やソフトウェアの脆弱性を利用し感染を拡大する有害プログラム（ワームやウイルス等）による被害が増加している．特に近年，ボットに関する被害が拡大しており，ウイルス対策ソフトのシグネチャベースの検知では防ぐことは難しいと指摘もされている．ボットの感染/伝播活動を検出する有効的な手段として，ボットの協調動作を要素に検出する手法[1],および SVM を用いた C&C セッション分類による検出方法が提案されている[2].

本研究では,実際にボットの検体を捕獲し，捕獲した検体を安全な環境で実行する．そのときボットが行う通信を採取し，C&C セッションの応答時間，パケットバイト数等を特徴とする以外に，ボットの特徴である短時間におけるプロトコルの変化を特徴とし，正常な通信との比較分類によりボットの検出を行う手法を検討する．

２．ボットとボットネットとは

ボットとは，攻撃者がある目的のために，他人のコンピュータに忍び込ます悪性プログラムの事を示す．また，インターネットを介して他人のコンピュータを複数台同時に操作することも可能であるため，このような構成をボットネットワークという．

一般的には,多くのボットは IRC(Internet Relay Chat)プロトコルを使用し構成される．IRC の特徴である同一チャネル内においては，一斉にメッセージを配信する仕様を利用することで，攻撃者はボット感染端末に命令を送る．また,この命令を送るサーバを C&C (Command & Control)サーバと呼び，感染端末と C&C サーバ間の通信を，C&C セッションと呼ぶ．

ボットは，無差別に被害が拡大する従来のウイルス/ワームとは異なり，攻撃者の目的に合わせた有害プログラムであることが特徴である．攻撃者の目的は，DDos 攻撃/スパム送信/トラフィック盗聴/キーロギング等が確認されている．また，インターネット上では，有害プログラムのソースコードの公開，ボット生成ソフト公開などにより，日々攻撃者により新種/亜種のボットが開発されている．

３．ボットの動作

一般的にボットは，他の端末に OS /ソフトウェアの脆弱性や SPAM メールを利用することで，ボット本体をダウンロードするファイルサイズの小さなシェルコードを忍び込ませる．感染端末はこのコードにより，ボット本体を TFTP/HTTP プロトコルなどを使用しダウンロードする．その後，IRC 通信を行う場合と，他のコンピュータへ感染活動を行う場合がある．前者の IRC 通信の場合は，HTTP を利用してボットプログラムの更新を行い，その後，攻撃者の命令を待つ状態になる．感染活動を行う場合は，自身のＩＰアドレスに近いアドレスに対しスキャンを行い，応答があったコンピュータに対しエクスプロイトコードを送りつけ感染拡大活動を行う．

４．既存のボット検出手法

既存のボット検出手法ならびに関連研究を紹介し，それらの課題を示す．既存のボット検出手法には以下の６点が挙げられる．

A)　シグネチャによるボット検知手法
B)　ブラックリスト方式によるボット検知手法[3]
C)　ネットワークトラフィック異常による検知
D)　制御コマンドによる検知手法[4]
E)　ボットの協調動作による検出方法[1]
F)　C&C セッションの応答時間による検知[2]

A)，B）の検出手法では，前述したようにボットは日々亜種が発生しており，その都度分析をする必要があるため,未知のボットについては検知出来ないことが推測できる．C）については，現在のボットはネットワークトラフィックの流量を考慮したものあり，検知出来ないことが推測できる．また，D）ではボットの通信であると判断する項目として以下の点を挙げている．

・急激に参加者が増えた IRC チャネルの通信
・長時間 IRC チャネルに参加しているクライアント
・チャット通信とは思われないレスポンスの早い通信

この研究では，上記の方法でボットを検出するための実験が行われていないため，本当に検出できるかどうかは不明である．

E）については，２つの検出要素を挙げている．

・大規模チャネル内における単一チャネルのみに参加している端末割合によるボットネットワークの検知
・感染端末と C&C サーバ間における通信の応答時間によるボットネットワークの検出

この２つの検知手法を，単一で使用するには見逃しや誤検知の問題があると指摘もしており，他の検知手法との組み合わせが必要であることも記載されている．

F）についてはＥ）同様に C&C セッションの応答時間やパケット数，パケットバイト数により検知を行うことが提案されている．

５．本研究における C&C セッション分類の検討方式

本研究では，ボットの検出方法として感染端末と C&C サーバ間のネットワークトラフィック内において，一定の特徴を抽出し，正常な通信との比較をすることで，C&C セッションであるか分類することを検討する．現在，以下の２つを特徴ベクトルとして分類することを検討している．

† 情報セキュリティ大学院大学情報セキュリティ研究科

A) C&C セッションにおけるパケットサイズと応答時間
４章 E）,F)，項で紹介した C&C セッションにおける IRC 通信におけるパケットサイズと応答時間には，正常な通信とは異なる特徴があると推測される．

B) C&C セッションにおけるプロトコルの変化
図１に「Win32/IRCBOT」と「Win32/RBOT」ボットを実行させた際の通信プロトコル変化を示す．これは後述する C&C セッション観測環境にて取得した情報である．ボットを実行してから約 1〜2(sec)の間に，ボットが使用する通信プロトコルの変化読み取れる．このような通信は，明らかに機械的な通信であり，人間が操作したトラフィックとは考えにくい．このようなプロトコルの変化を特徴ベクトルとすることを検討している．

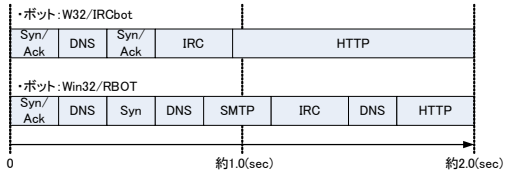

図 1. 「Win32/IRCBOT」「Win32/RBOT」のセッション

本研究では，関連研究[2]同様に，C&C セッションの特徴として，パケットの送受信間隔ならびにパケットサイズのみに注目し特徴抽出を行った．図 2 にボットに感染した端末と C&C サーバ間の一般的なセッションを示す．

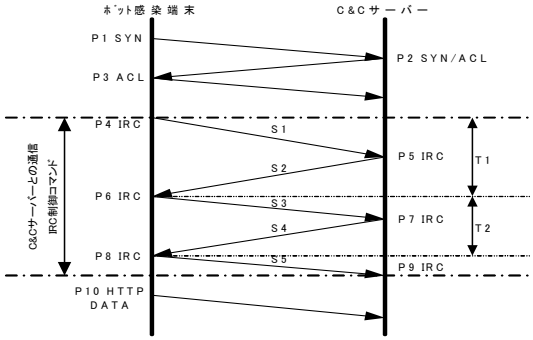

図 2 一般的な C&C セッション

C&C セッションの特徴は，ボット感染端末から C&C サーバーへ IRC で送信されたパケットバイト数 Sn，到達間隔 Tn とした．

本研究では，ボットの C&C セッションを観測するため，ボットの検体捕獲から行い，安全な環境で実際にボットを実行し C&C セッションを観測した．観測から C&C セッションを観測した環境を図 3 に示す．

ボットをハニーポット (Nepenthes)で採取し，仮想 OS(VMware)上でボットを実行し，C&C サーバとのネットワークトラフィックを tcpdump で採取した．その際，実行したボットが他の端末に感染活動をしないように，ファイアウォールにてフィルタリングを行った．C&C セッションの tcpdump データ内からボットが使用する制御コマンド”USER”,”NICK”,”PASS”,”JOIN”” MODE” が使用されているセッションのみ抽出し，パケットサイズ Sn，到達間隔 Tn を抽出した．

抽出したデータをプロットした結果、C&C セッション

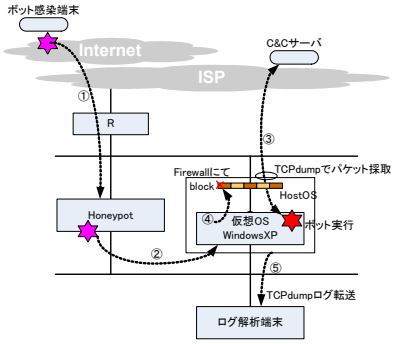

図 3 ボットの検体捕獲と C&C セッション観測環境

において送受信共にパケットサイズが小さいことが読み取れた．また通常の通信と比較するため，IRC チャットを行ったネットワークトラフィック及び Web 閲覧を行った HTTP ネットワークトラフィックと比較検証を行った．C&C セッション送信パケットについては，通常の IRC 通信と比較し応答時間が短いことが判明し，また，Web 閲覧と比較した結果送受信パケットサイズの違いが顕著に現れた．これらのことから C&C セッションには一定の特徴があることが確認出来た．

今後はプロトコルの変化についても特徴抽出を行い，応答時間の特徴と組み合わせて，１つの C&C セッション特徴ベクトルとする予定である．また，ボットの C&C セッションと正常な通信と識別するため，SVM(Support Vector Machine) 等のパターン分類手法を検討している．

6. まとめ

C&C セッションには，固有の通信上の特徴が存在するという仮説をもとに”応答時間”,”プロトコルの変化”の２つの要素をいれた特徴ベクトルを提案した．前者については実際の通信を確認し,後者については今後実データにより特徴抽出を行う予定である．

また、前述した２つを組み合わせた１つの特徴ベクトルとして，ボットの C&C セッションと正常な通信の分類を行う予定である．本手法はシグネチャ方式やブラックリスト方式によらない検出のため，日々，亜種が開発されるボットへの対応策として，有効であると推測される．

今後はさらにボットの特徴ならびに挙動について分析を行い，提案手法の有効性を評価する予定である．

＜参考文献＞
[1] 山口 英,河本 貴則,秋山 満昭,横山 輝明,門林 雄基,”ボットネットの協調動作に注目した検出手法の一検討”,SCIS2007.
[2] S.Kondo and N.Sato,"Botnet Traffic Detection Techniques by C&C Session Classification Using SVM," to appear in IWSEC2007, Oct. 2007.
[3] 朝長 秀誠,田中 英彦,”Botnet の命令サーバドメインネームを用いた Bot 感染検出方法”,情報処理学会 CSS2006,pp.13-18(2006 年 12 月).
[4] Jonas Bolliger, Thomas Kaufmann, “Detecting Bots in Internet Relay Chat Systems”, Master’s thesis, Swiss Federal Institute of Technology Zurich,May,2004.