本資料について

- 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。

- 論文名：A Case Study of the Rustock Rootkit and Spam Bot
- 著者：Ken Chiang, Levi Lloyd
- 所属：サンディア国家研究所

ルートキットとスパムボットの事例研究について

情報工学科　渡邊研究室
070428344　阿南　宏教

導入

- ボットネットによって生じられる脅威は年々拡大
- 害を被りやすいシステムを感染，制御するために使用されるツールの洗練レベルは増加
- 感染経路はエクスプロイト型や電子メールなどに不正プログラムを添付して送りつける傾向から，Webサイト経由へ
- 感染したコンピュータは、スパム送信やウイルス拡散、個人情報などの盗聴、特定のシステムへの攻撃などを目的に使用

ボットネットとは

- ボットネットの「ボット」とは，ユーザに気付かれないようにパソコンに入り込み，クラッカからの命令を受け，その命令に従って動作するプログラム
- クラッカはボットを増やして組織化
- 組織化されたボットのネットワークを「ボットネット」と呼ぶ

ボットの特徴

- ワームやトロイの木馬に似ている
- クラッカは「裏口」（バックドア）を作成
- 裏口からボットが感染したパソコンを操り攻撃

攻撃に使用されるサーバ

IRC（internet relay chat）サーバ

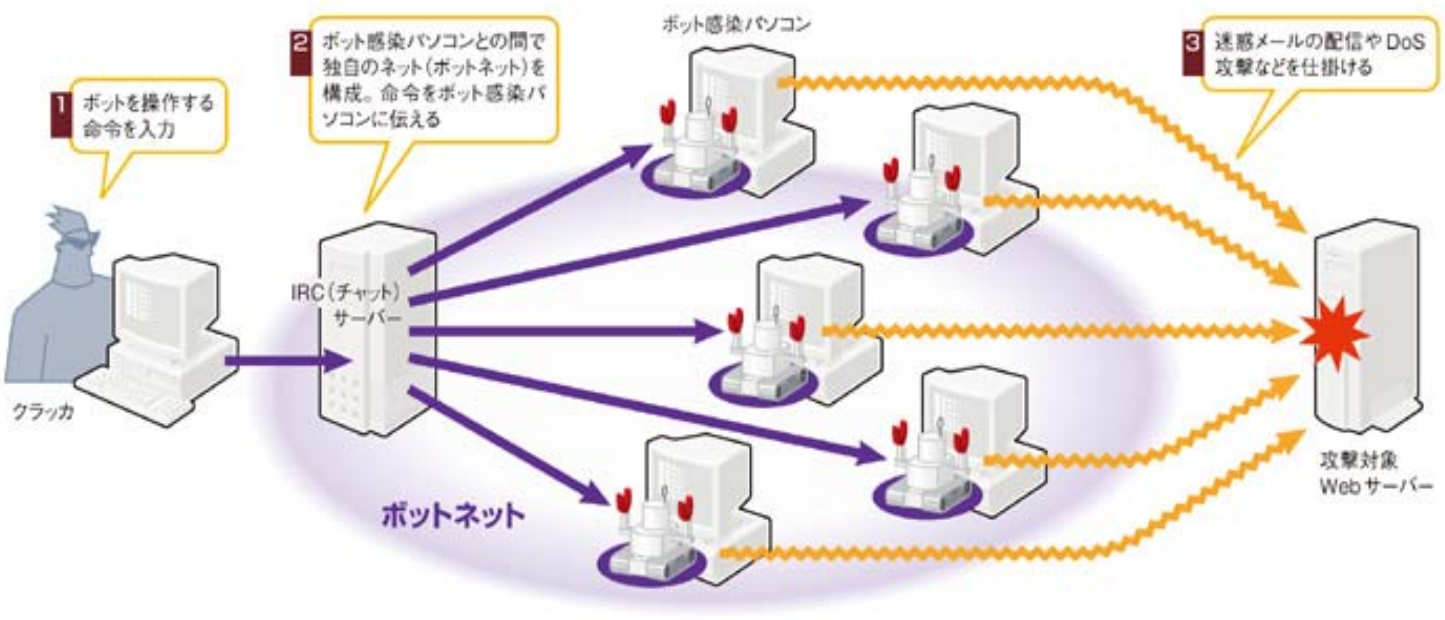
- クライアントとクライアントが会話をする枠組みの名称
- リアルタイム・チャット用のサーバ
- 文章のみをやり取りして会話を行う

DCC(Direct Client-to-Client)サーバ

- IRCにおける、サーバーを経由しない利用者同士の直接通信を定めたプロトコル
- ファイル転送を可能

攻撃に使用されるサーバ

- IRCサーバとDCCサーバに参加するボット群で構成
- 命令を出すと攻撃を開始する



ボットの動作

- 他の端末にOS/ソフトウェアの脆弱性やSPAMメールを利用
- 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
- IRC通信を行う場合と,感染活動を行う場合がある
  前者⇒更新を行い、その後攻撃者からの命令を待つ状態
  後者⇒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
  感染拡大活動を実施

ボットの機能

- Webサーバーからファイルをダウンロードする機能や，指定したファイルを実行する機能

- ウイルス対策ソフトの網の目をくぐり抜けるために，自分自身をアップデートする機能

⇒更新命令によりプログラムをダウンロードして自分自身を更新

ボット検出手法

- シグネチャによるボット検知手法
- ブラックリスト手法によるボット検知手法
- ネットワークトラフィック異常による検知手法
- 制御コマンドによる検知手法
- ボットの協調動作による検出手法
- Ｃ＆Ｃセッションの応答時間による検知手法

ボットの協調動作による検出手法

- ２つの検出要素

Ⅰ 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

Ⅱ 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知

- 単一で使用するには見逃しや誤検知の問題あり

  ⇒他の検知手法と組み合わせが必要

Ｃ＆Ｃセッション分類の検討方式

- ボットの協調動作による検出手法と同様に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する方法
- ボットネットにおけるＣ＆Ｃサーバと感染したPC間の通信や感染後のDNSクエリの異常に着目

⇒トラフィックデータの異常を用いることによって検知

C＆Cセッション分類の検討方式

A)C&C セッションにおけるパケットサイズと応答時間と,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

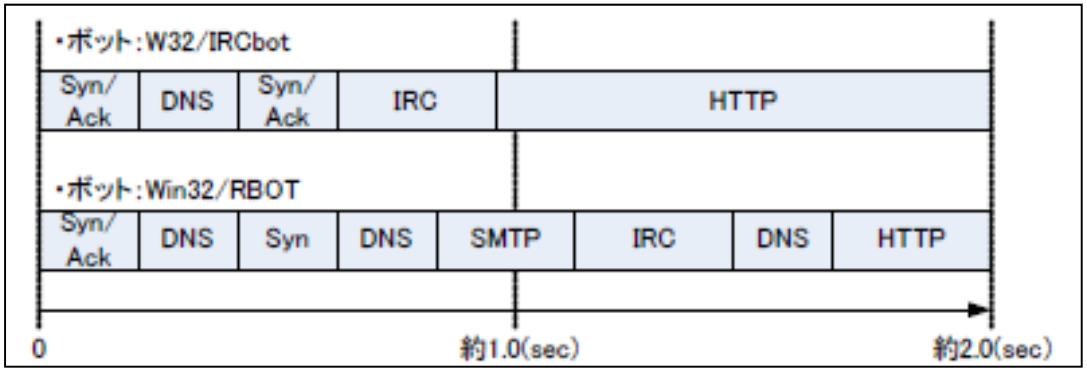


図 「Win32/IRCBOT」「Win32/RBOT」のセッション

C＆Cセッション分類の検討方式

- 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

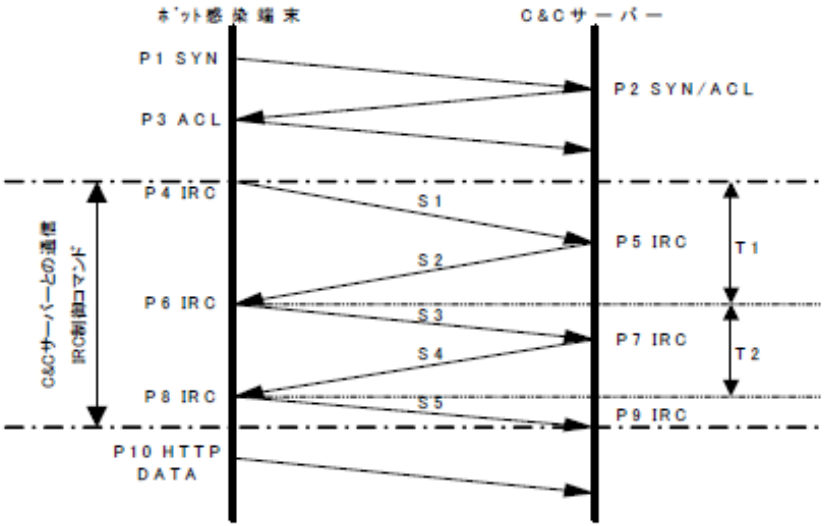


図　一般的なC＆Cセッション

※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とする

C＆Cセッション分類の検討方式

- 制御コマンド”USER”,”NICK”,”PASS”,”JOIN””MODE”
- 使用セッションのみ抽出
- パケットサイズSn, 到達間隔 Tn を抽出

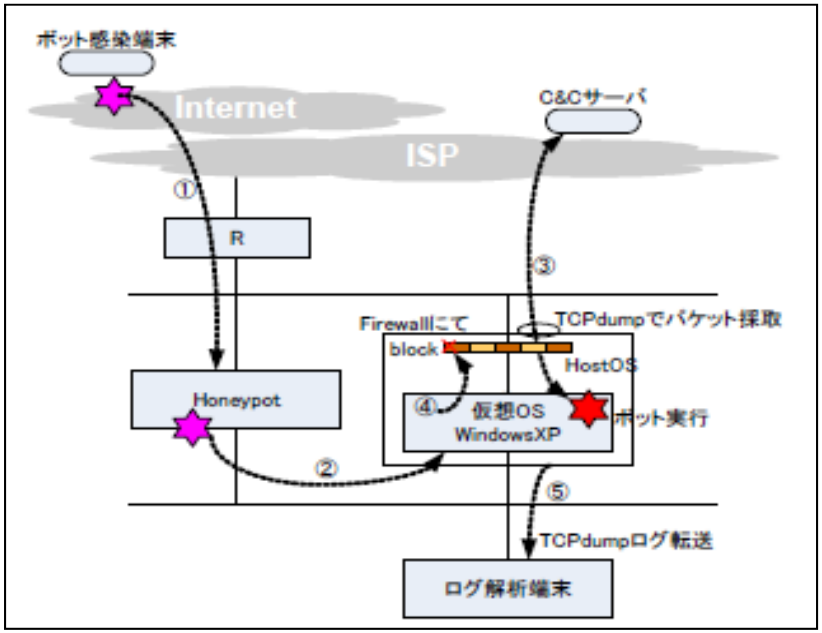


図　ボットの検体捕獲とC＆Cセッション観測環境

ボットの難読化

```
.text:000114AF      test    eax, 1789F30Ch
.text:000114B0      or      al, 0F3h
.text:000114B1      rep mov [edi], edx
.text:000114B6      shr     byte ptr [eax+5CFB5080h], cl
.text:000114BC      call    far ptr 90B6h:79C35C2Bh
.text:000114C3      shl     dword ptr [ebp+0Fh], 1
.text:000114C6      db      67h
.text:000114C6      daa
.text:000114C8      push    eax
.text:000114C9      push    cs
.text:000114CA      jmp     near ptr 0E0896CB5h
```

De-obfuscate

```
.text:000114AF      pusha
.text:000114B0      call    $+5
.text:000114B5      pop     ebp
.text:000114B6      sub     ebp, 6
.text:000114B9      mov     eax, large fs:30h
.text:000114BF      mov     eax, [eax+4]
.text:000114C2      xor     al, al
.text:000114C9
```

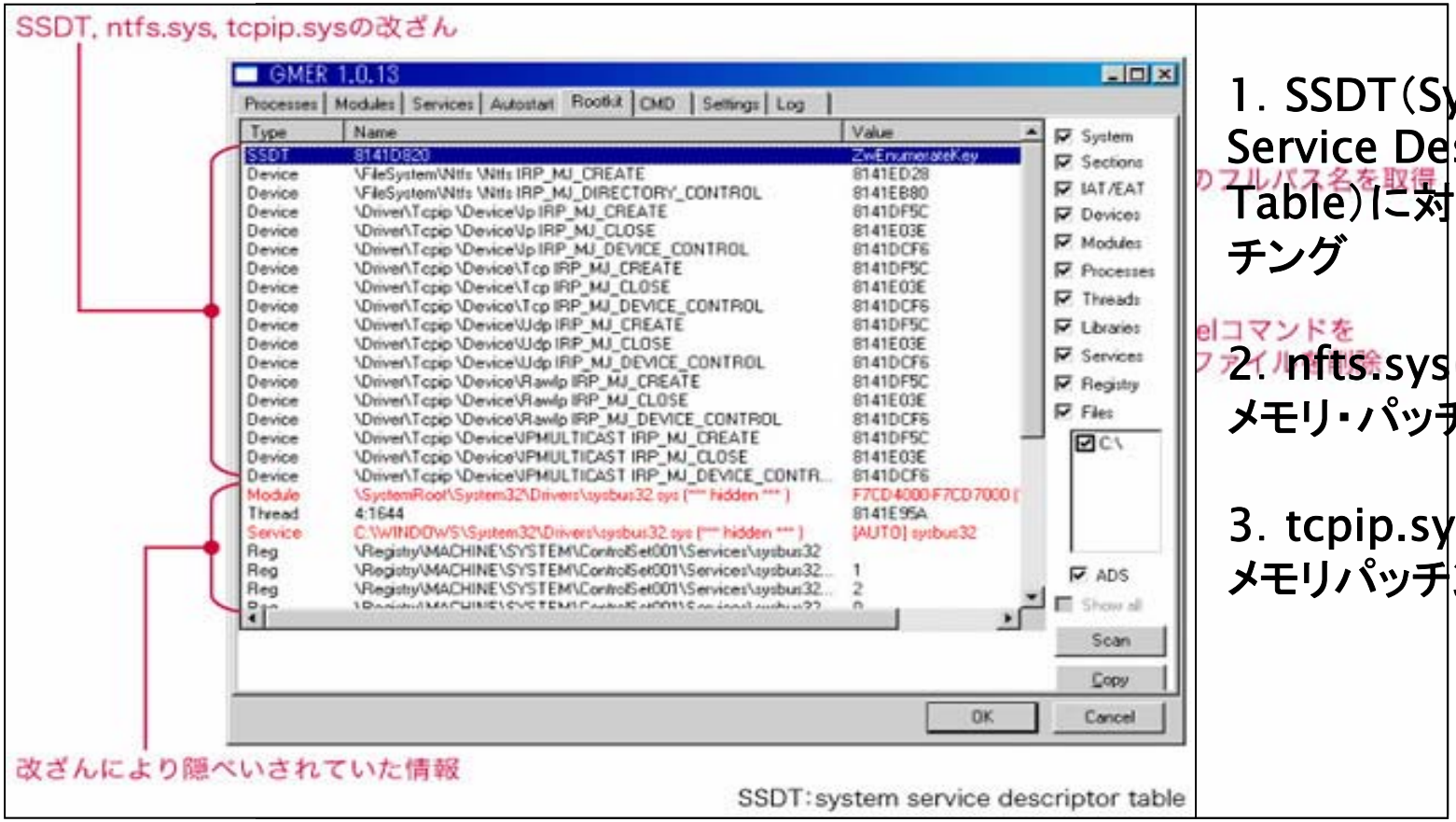
図1　C&Cサーバの生成ルーチン

".." .rdata:00402302	00000007	C	fclose
".." .rdata:00402316	00000006	C	fopen
".." .rdata:004022E6	00000008	C	fprintf
".." .rdata:0040230C	00000007	C	fscanf
".." .data:00403010	0000001D	C	http://www[redacted].txt
".." .rdata:004022C8	00000008	C	sprintf
".." .data:00403098	0000000B	C	urlmon.dll

図2　別のマルウェア検体を分析した際に特定した通信先のURL

「Obfuscation(難読化)」

ボットの動作を逆アセンブリで解析



1. SSDT(System Service Descriptor Table)に対するパッチング

2. nfts.sysに対するメモリ・パッチング

3. tcpip.sysに対するメモリパッチング

図　GMERを使った[illegible]

ボットに組み込まれたルートキットを解析

- ご清聴ありがとうございました

シグネチャによるボット検知手法

- パケットを攻撃情報データベースと比較
- 低速であり、データベースの更新が不可欠

⇒高速ネットワークに向かない上に新種や変種に非対応

- 様々な種類のネットワークトラフィックデータが存在するため、複数の時系列数値データグラフを比較,解析

⇒迅速な原因究明や攻撃対象コンピュータの特定が困難

ブラックリスト手法によるボット検知手法

- ブラックリスト・サービス・プロバイダに問い合わせ

⇒一致した場合,スパムである可 能性は高いと判断
ネットワークからそのような攻撃を排除することが可能

- 亜種が発生しているボットに対応させる必要あり

⇒未知のボットについて検知できないと推測

ネットワークトラフィック異常による検知

- ネットワーク型IDS(Intrusion Detection System)

⇒トラヒック解析によりボットのネットワーク活動を検知
NIDSははネットワーク内の複数端末を同時に長期監視可能
複雑な解析や統計や統計的手法を適用できる利点

端末より細かい粒度での解析ができない
⇒通常通信に類似した様々なネットワーク活動を行うボットに対して誤検知や検知見逃しが発生しやすいとされている

- 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もあり、検知できない可能性があると推測

制御コマンドによる検知手法

- ボットの通信であると判断する項目として以下の3つが挙げられる

Ⅰ 急激に参加者が増えたIRCチャネルの通信

Ⅱ 長時間IRCチャネルに参加しているクライアント

Ⅲ チャット通信とは思われないレスポンスの速い通信