- 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。

文献：An Advanced Hybrid Peer-to-Peer Botnet

著者：Ping Wang Sherri Sparks Cliff C. Zou
School of Electrical Engineering and
Computer Science University of
Central Florida, Orlando, FL

URL：http://www.usenix.org/events/hotbots07/tech/tech.html

An Advanced Hybrid Peer-to-Peer Botnet

名城大学　渡邊研究室

間宮　領一

近年

- インターネット上のマルウェアによる攻撃
  - 組織化
  - 利益優先
- ボットネットがインターネット攻撃の根本的原因
  - DoS攻撃
  - スパム送信
  - クリック詐欺

将来のために重要なこと

- 将来のあらゆる攻撃に対する準備が必要
- 攻撃者によって開発される高度なボットネットの設計を検討するべき

- この論文では高度なハイブリッドP2Pボットネットのデザインを示す

C＆C ボットネット

- IRCサーバによるコマンド＆コントロール（C＆C）が制御の中心
- クライアントボットは直接C&Cサーバに接続

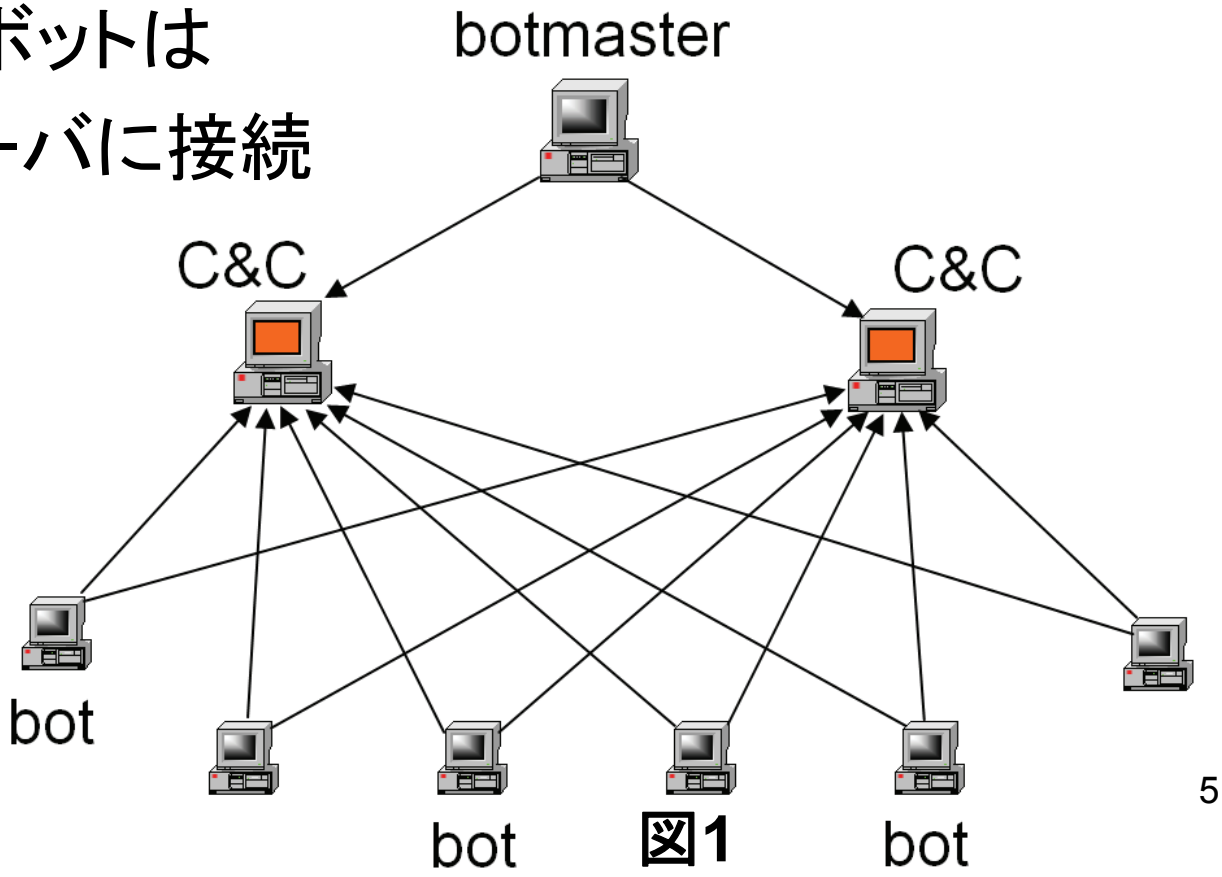
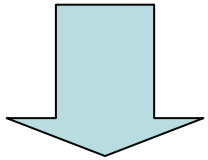


図1

C&C ボットネットの問題点

- ある数のＣ＆Ｃサーバがシャットダウンされるとボットネットは制御不能
- Ｃ＆Ｃサーバに命令が集中している



- ピアツーピア（P2P）メカニズムが提案される

強固なボットネットとは

- ボットネット本質的な部分が削除されてもボットのコントロール維持が可能
- ボットが捕らえられたときネットワーク形態の重要な露出を防ぐ
- 容易にボットネットの完全な情報をモニターできる
- コミュニケーショントラフィックパターンによるボット検出を困難にする

P2P ボットネット

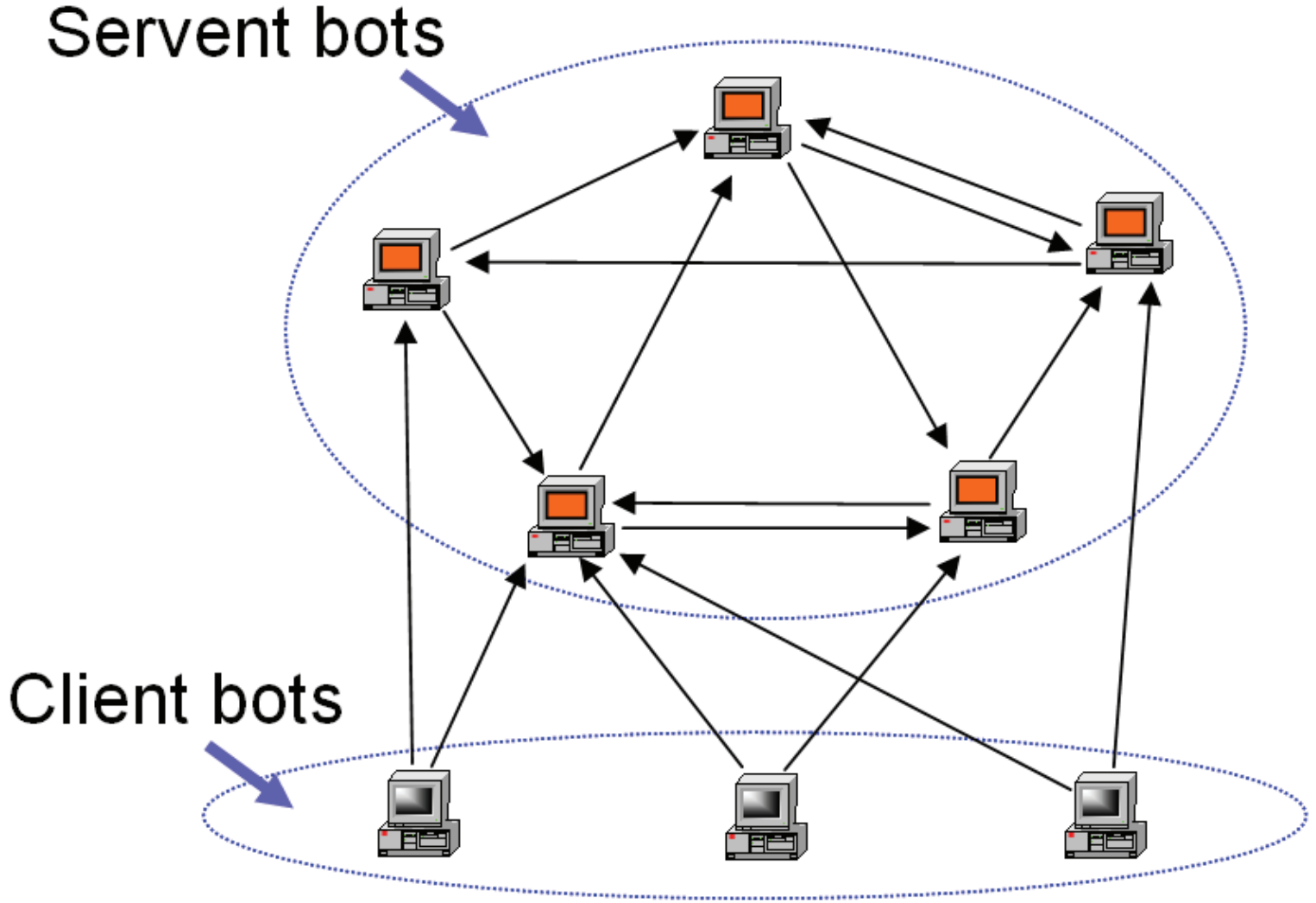


図2

ボットの種類

- Serventボット
  - 静的なグローバルIPアドレスを持つ
  - クライアントとサーバの両方として作用
- Clientボット
  - ダイナミックに割り付けられたIPアドレスをもつ
  - プライベートIPアドレスを持つ
  - ファイアウォールの後ろにある

提案されたP2Pボットネット

- 静的グローバルIPアドレスによるボットはserventボットの候補
- ボットネットは各serventボットに含まれるpeer listを通して通信(図2:peer listのサイズは2)
- 攻撃者はレポートコマンドによりボットネットをモニタ
- 自己生成対称な暗号化および自決したサービスポート設計により検知を困難にする

提案されたボットネットのC&C構造

- P2Pボットネットでは定められた場所から命令を受け取らない
- 命令を検索するため積極的にpeer list中のserventボットに接続
- 強い命令認証を実行することが重要

個別的暗号鍵

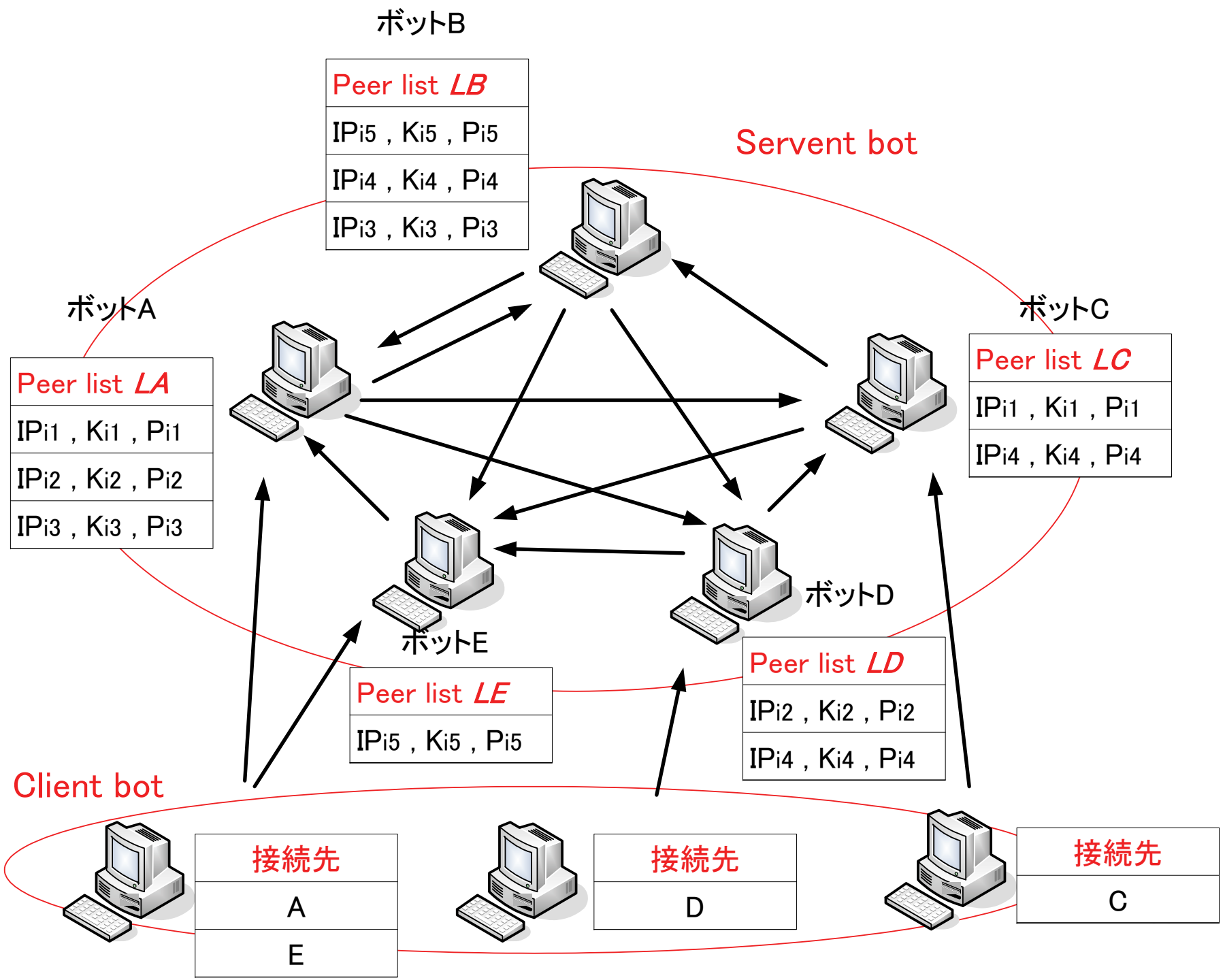
- Serventボット　i
- 任意の対称な暗号鍵 Ki
- ボットAのpeer list　LA (IPアドレスと鍵を含む)
- ボットAのpeer list

  $LA = \{(IP_{i1}, K_{i1}),(IP_{i2}, K_{i2}),\cdots\cdots(IP_{iM}, K_{iM})\}$
- ボットBがserventボットAに接続する場合
  - Bのpeer listには(IP_A, K_A)を含まなければならない

個別的サービスポート

- サービスポートを使用しpeer listに基づきコミュニケショントラフィックを分散
- Serventボットのポート番号　Pi(ボットがランダムに選択)
- サービスポート情報を含むpeer list

  $LA = \{(IP_{i1}, K_{i1}, P_{i1}), \cdots, (IP_{iM}, K_{iM}, P_{iM})\}$
- サービスポートを使用する理由
  - ネットワークトラフィックの分散
  - バックドアの維持


ボットB
Peer list LB
IPi5 , Ki5 , Pi5
IPi4 , Ki4 , Pi4
IPi3 , Ki3 , Pi3
Servent bot
ボットA
Peer list LA
IPi1 , Ki1 , Pi1
IPi2 , Ki2 , Pi2
IPi3 , Ki3 , Pi3
ボットC
Peer list LC
IPi1 , Ki1 , Pi1
IPi4 , Ki4 , Pi4
ボットD
Peer list LD
IPi2 , Ki2 , Pi2
IPi4 , Ki4 , Pi4
ボットE
Peer list LE
IPi5 , Ki5 , Pi5
Client bot
接続先
A
E
接続先
D
接続先
C

ボットネットのモニタリング

- ボットは攻撃者によりコントロールされるデータ収集マシン(センサ)に情報を送信
- センサ
  - レポートコマンドにより命令を出す
  - センサホストのIPアドレス(又はドメイン)はレポートコマンド中で指定
  - peer listを更新するため積極的にセンサホストと連絡を取る(ボットネットの再編成に有効)

センサホストの身元が知られたとき

- センサの報告コマンドにHTTPや電子メールを使用
- レポートデータ検索直後にセンサホストのハードディスクデータを一掃する
- センサホストが捕まったことを攻撃者が知った場合レポートコマンドをキャンセル

以上の方法などをとりボットネットを保護

ボットネットの構築

- ボットネットの接続性
  - 各ボットのpeer listにより独断で決定
- peer listの構築
  - 各ボットのpeer listのサイズがMになるように構成すると仮定
  - 新規感染
    - 脆弱なホストBへボットAがpeer listを渡す
    - BがserventボットのときAはBをpeer listに加える（peer listが十分な場合任意のボットを1つ交換）

ボットネットの構築

- peer listの構築
  - 再感染
    - ボットAがボットBに二次感染可能なら、Bのpeer listからR(R≦M − 1)の任意に選択されたボットをAから提供されるpeer listに置き換える
    - peer list中のserventボットを二次感染させ、続いてそのserventボットからpeer listを得て順番に感染させる

ボットネットの丈夫さを知るためのシミュレーション

- ボットの*25%*がserventボット
- ボットネットが*500,000*の可能性脆弱な人口を持っている
- ボットネットは平均サイズが*20,000*に達すると成長を止める
- Peer listのサイズ *M=20*
- *M=21*のserventホストが感染を始める
- Peer listは常に満たされている

以上と仮定する

仮定したボットネット

- 20,000サイズに達した後に再感染イベントはめったに起こらない
- Serventボットへの接続は均衡を失う
- M=30未満を持つServentボットは80%を超える（サイズ4000）
- M=21の最初の各serventボットは14,000から17,500の間の程度を持つ
- Serventボットの最初のセットがC&Cサーバとして作用するためC&Cボットに地位が下がる

別のシミュレート

- 脆弱なホスト全てを感染させる
- シミュレーションでは210,000の再感染が発生
- 多くの再感染があるため構築されたボットネットはバランスがとれた接続をしている
- Serventボットの程度分布はおよそ正規分布に従う
- Serventボットの80%はM=30～150程度を持っている

ボットネットの接続性

- ボットが捕らえられ取り除かれる
- いくつかのボットがオフライン状態

ボットネットの接続性に影響する要素として以上の2つがある

- Serventボットを更新するため、peer listのある部分を削除されたときの接続性を確認

シミュレーション

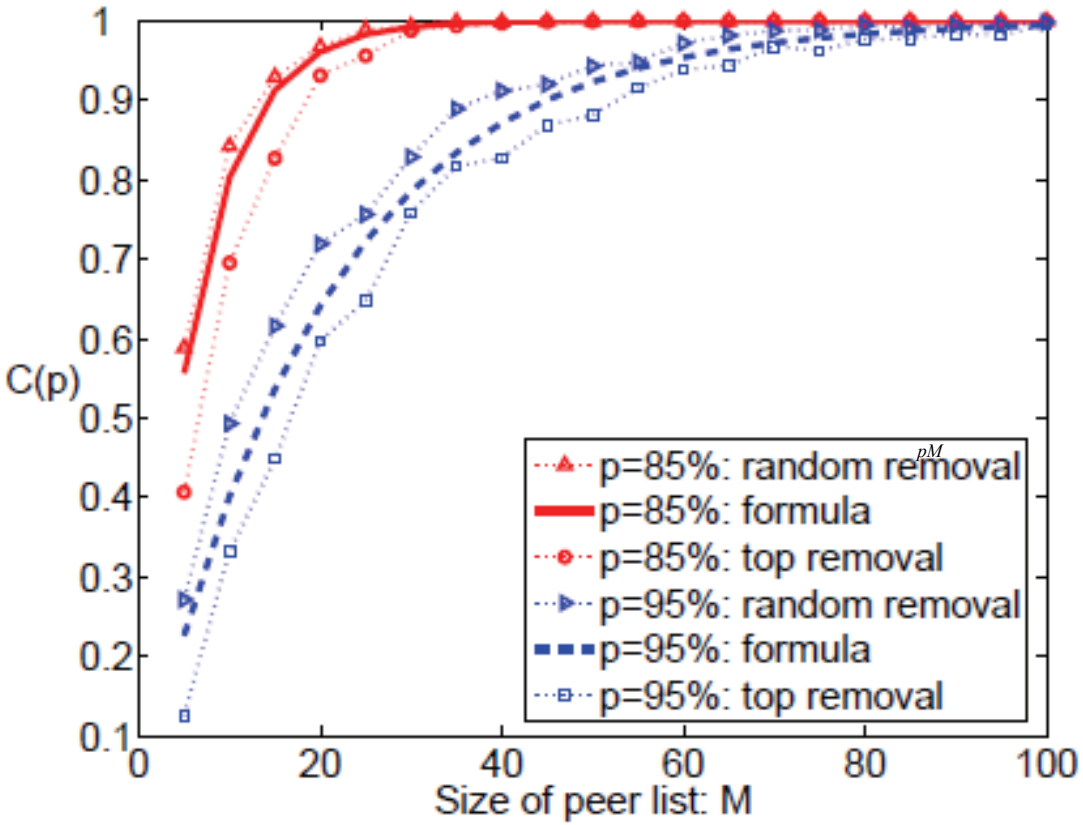
- 防御行為からの残存率 C(p)
- Peer list更新の際に削除される等確率 p

$$C(p) = \frac{\#\text{ of bots in the largest connected graph}}{\#\text{ of remaining bots}}$$

- 500,000の脆弱な人口を持ち1,000のServentボットが感染する場合peer listの更新を一度実行
- このときpeer list更新時に700未満が削除される場合(C(p)>95%)にボットネットは維持できる

分析的な定式およびシミュレーション結果の比較

- ボットが分離される確立　p^M
- 残存ボットがとどまる確立　$1-p^M$
- C(p)の平均値　$C(p)=1-p^M$



結果

- 任意の除去シミュレーション結果C(p)と比較して分析的なものが起因する
- 分析的な定式があまり正確でなくてもボットネットの丈夫さの直接評価を提供
- 図はボットネットが大規模なpeer listを必要としないことを示す

提案されたボットネットに対する防御

- 全滅させるには
  - ボットネットが多くのserventボットを得られない場合シャットダウンが容易
  - ハニーポットが静的なグローバルIPアドレスを持ちserventボットになるとpeer listから情報が得られる
  - 提案されたbotnetの強い丈夫さはpeer list更新に極度に依存します。

モニタリング

- 大きなIPスペース上のハニーポットを利用
  - 感染の試みを捕えられる
- ボットがハニーポットを検知できずpeer listを渡す場合
  - serventボットの重要な情報を得てpeer list のコピーを得ることが出来る
- ハニーポットに基づき攻撃者によって出されたコマンドの元文を得られる

報告コマンドの理解

- レポートコマンドを配信後にログが消される前にセンサマシンを捕らえた場合
  - 全ボットネットの詳細情報を得ることができる
- 攻撃が始まる直前に対策をすばやく実行することができるように攻撃コマンドの目標をしる

まとめ

- 提案されたハイブリットP2Pボットネットはpeer list を基本に接続性を保っている
- 高度なボットネットに対して防御するためにはハニーポットが重要役割を果たす