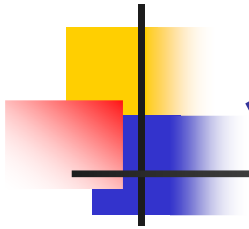
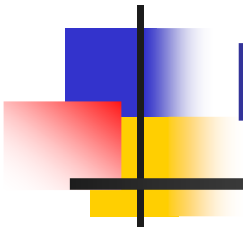


本資料について

- 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。

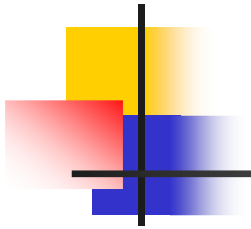
- 著者：Guofei Gu,Junjie Zhang,and Wenke Lee School of Computer Science,College of Computing Georgia Institute of Technology

- 論文名：Botsniffer:Detecting Botnet Command and Control Channels in Network Traffic



Botnet C&Cの検出

渡邊研究室
050427585 平田　祐二



はじめに

- ボット：感染したコンピュータは攻撃者の意のままに処理
  - 感染していることに気づきにくい
  - 自動で機能を追加・修正
  - 種類が多い
  - 犯罪目的

- ボットネット：ボットに感染したコンピュータによって構成されているネットワーク
  - スパムメール
  - DDos攻撃(Distributed Denial of Service)

ボットネットの種類

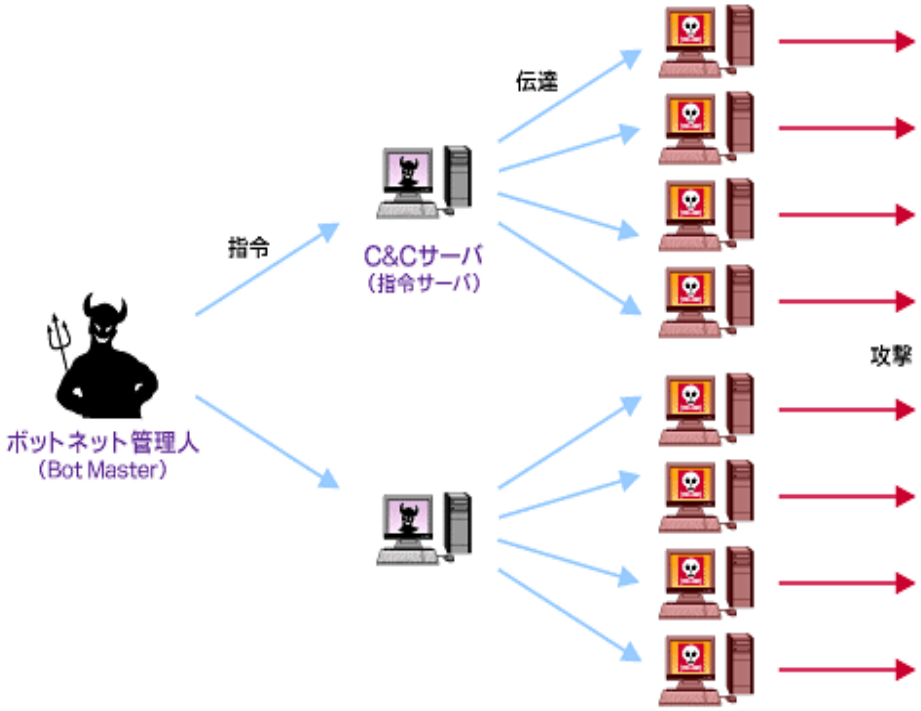


図1.C&C中心型ボットネット

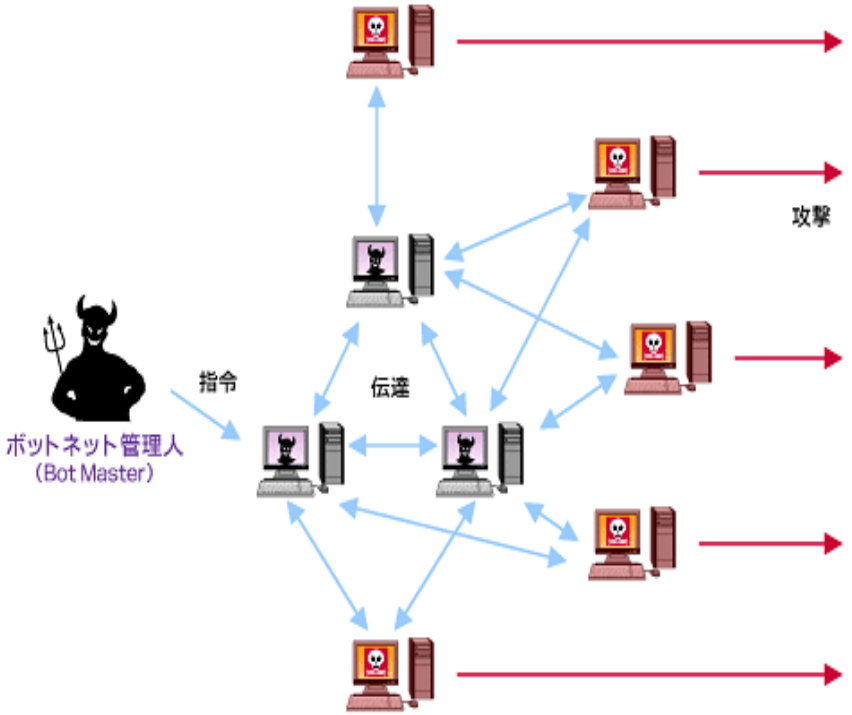
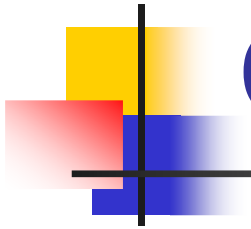
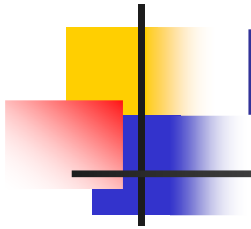


図2.ハイブリッド型ボットネット



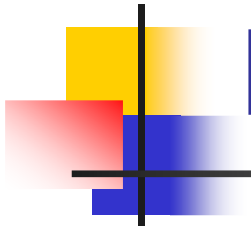
C&C (Command and Control)

- C&Cはボットネットに不可欠
  - C&Cがなければボットネットは離散的
- C&C検出は重要
  - 不変的に使われている
  - 最も弱いリンク
  - C&Cサーバと感染したボットを明らかにする
- C&C検出は難しい
  - 通常の通信と同様
  - 通信量が低い
  - コード化されたコミュニケーションを含む



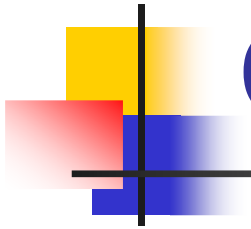
Botsnifferの概要

- ボットネットC&C検出システム
- ボットネットC&Cの相関関係と類似性の特性を利用
- 主なコンポーネント
  - Monitor Engine
    - Preprocessing
    - プロトコルMatcher
    - Activity/Message応答検出
  - Correlation Engine



Monitor Engine

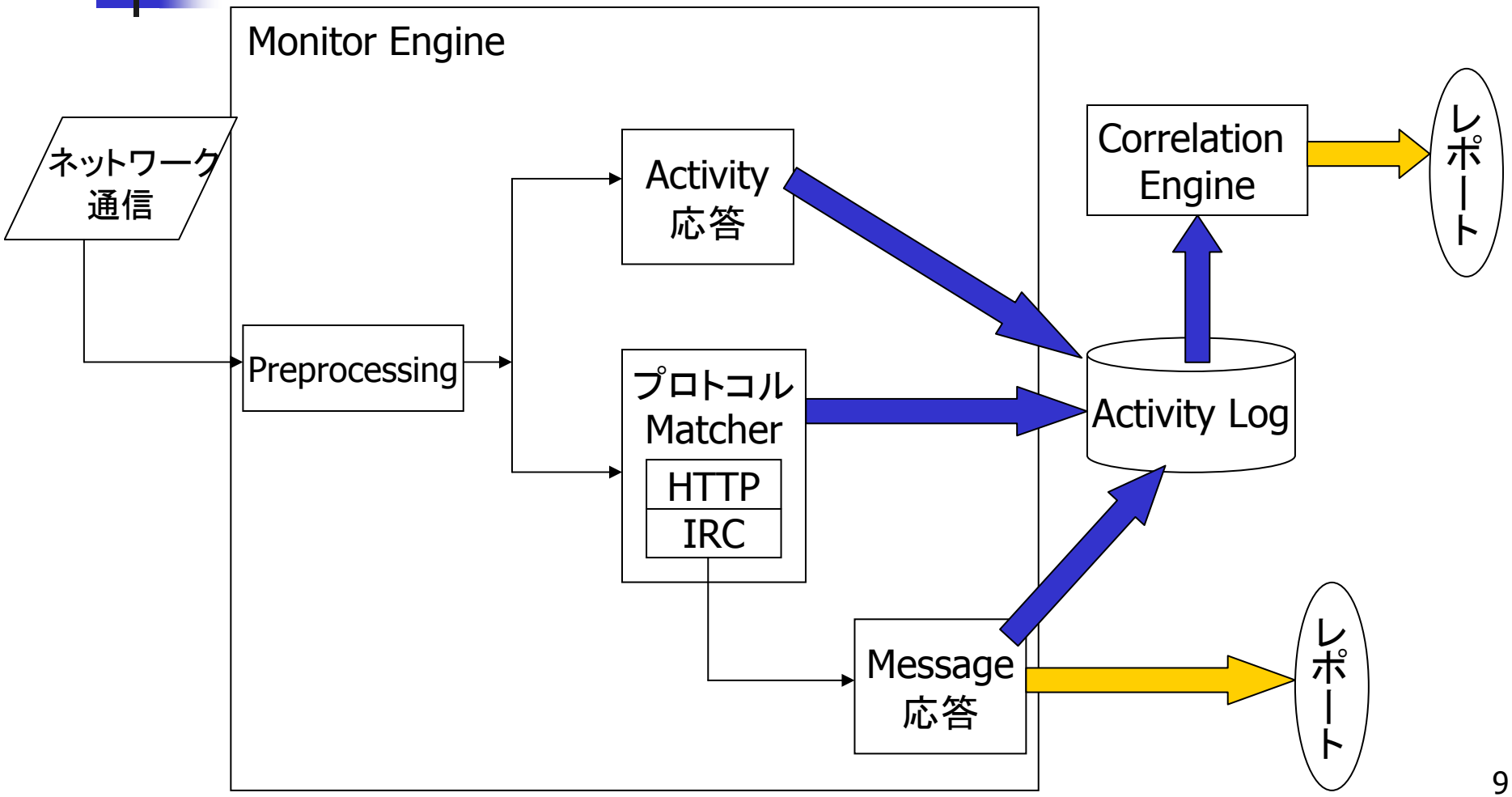
- Preprocessing
  - 無関係の通信を遮断
- プロトコルMatcher
  - 怪しいHTTPとIRC通信の検出
  - ペイロードの最初の数バイトを点検
  - ポートから独立
- Activity/Message応答検出

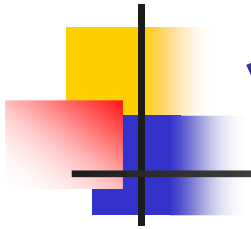


Correlation Engine

- IPとポートの宛先に従って、クライアントをグループに分類
- 時間と空間の相関関係と類似性を調べるためのグループ分析
- 怪しいC&Cを検出すると警告

Botsnifferの構造





今後の課題

- 検出精度の改良
- 独立したプロトコルの検出システムの開発
- ボットネットC&Cに使われるネットワーク構造の検出システムの開発

おわり