本資料について

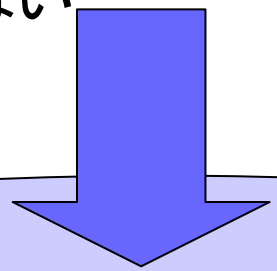
- 本資料は下記論文を基にして作成されたものです．文書の内容の正確さは保障できないため，正確な知識を求める方は原文を参照してください．
- 題目：定点観測によるボットネットの観測とMalwareの動的挙動解析システムの提案
- 著者：堀合　啓一，今泉　隆文，田中　英彦
- 出展：情報処理学会論文誌　Vol.49 No4
  1680-1691 （Apr.2008）

定点観測によるボットネットの観測とMalwareの動的挙動解析システムの提案

名城大学　理工学部
平田　祐二

はじめに

- ボットネットによるスパムメール送信やDDoS攻撃，情報の奪取などが問題となっている
- ウイルス対策ソフトウェアのパターンファイル更新で対応できないケースが増加
  - 新種や亜種の大量発生
  - 愉快犯から犯罪目的に変貌
  - 感染活動が目立たない



- Malwareの収集から解析までの一連の流れを自動化するとともに解析結果を表示し，Malwareの対策を立案する際に必要な情報を提供するシステム

システムの要件1

- インターネットの定点観測システムでは以下の2つが最低必要な機能となる.
  1. 情報を収集する機能
     - センサはハニーポットを利用し，IPアドレスに複数個のセンサを設置
  2. 収集した情報を集約して表示する機能
     - イベント発生状況の全般的な傾向を把握するために，横軸を時間軸とし，縦軸を何らかのイベント件数としてグラフ化して表示する

システム要件2

- ボットネットの挙動観測という観点から，全般的な傾向の把握に加えて，さらに詳細な情報が必要となる.
  1. いつ活動したか.（発信元IPアドレスやMalwareバイナリの種類ごとの期間・時間帯などの観測履歴）
  2. どこから来るか.（発信元IPアドレスの利用者などに関する情報，IPアドレスの分布）
  3. 感染の広め方.（狙われるポート番号）
  4. Malwareの種類.（Malwareの名称）
  5. どこからどんな指令を受けるか.（指令サーバのアドレスと指令内容）
  6. どんな種類の攻撃か.（スキャンのアドレス範囲，プロトコル，ポート番号）

システム要件3

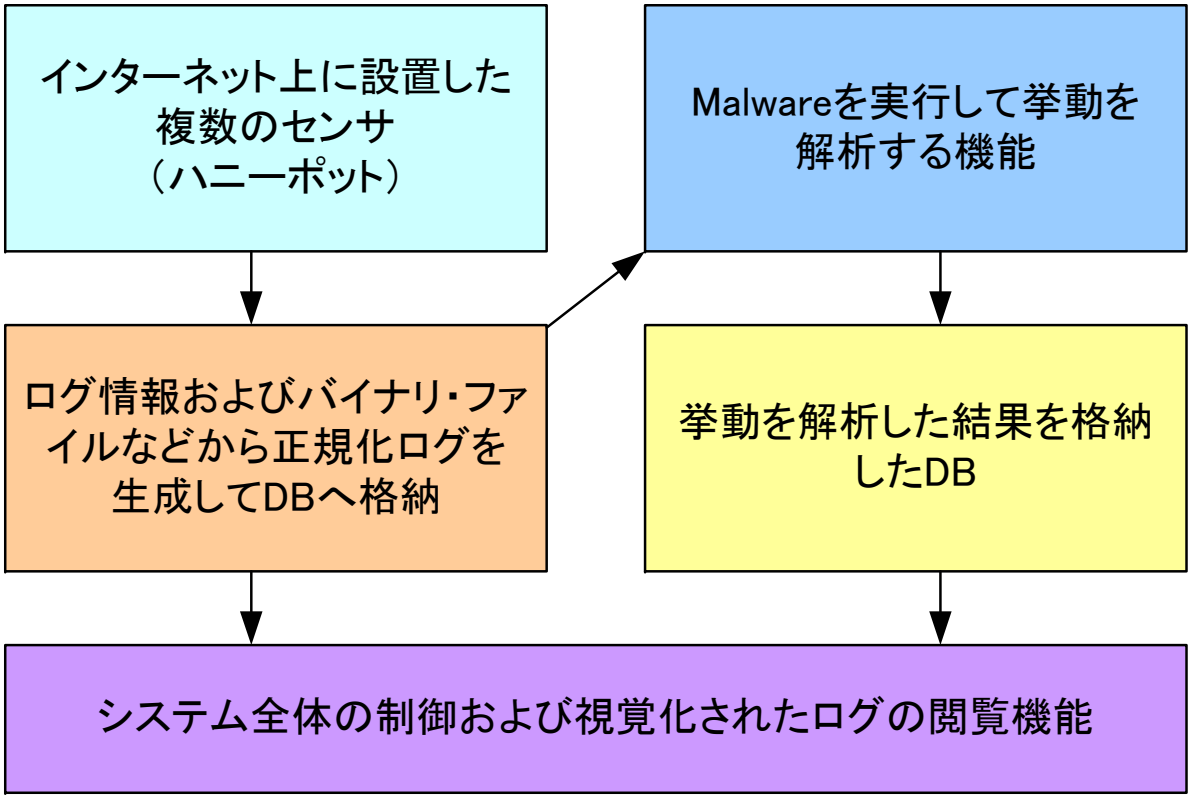
- 定点観測で捕獲したMalwareを仮想マシンの一種であるVMWare上のWindowsXPで実行し，その挙動を観測する.
- 必要な要素
  - 指令サーバと交信可能なネットワーク環境
  - DNSサーバ
    - ボットのMalwareは，バイナリの中に指令サーバなどのアドレスがFQDNの形式となっている場合が多い.
    - FQDNからIPアドレスの名前解決を行う.
  - 指令サーバとしてIRC，HTTP，SMTPを含む.
  - 実ネットワークには接続せず、クローズドな環境
    - 感染拡大がインターネットに波及させないため.

→指令の内容や指令に対応した挙動の解析は不可能.

→IRCサーバへのログインの経過を観測し，すでに知られている指令文字列などから類似して解析する.

システム要件4

- Malwareを実行して取得が必要な情報として，リソースの変化，プロセスの名称，システム関連のファイル改ざん・削除・生成などがある．
- システムの全体構成



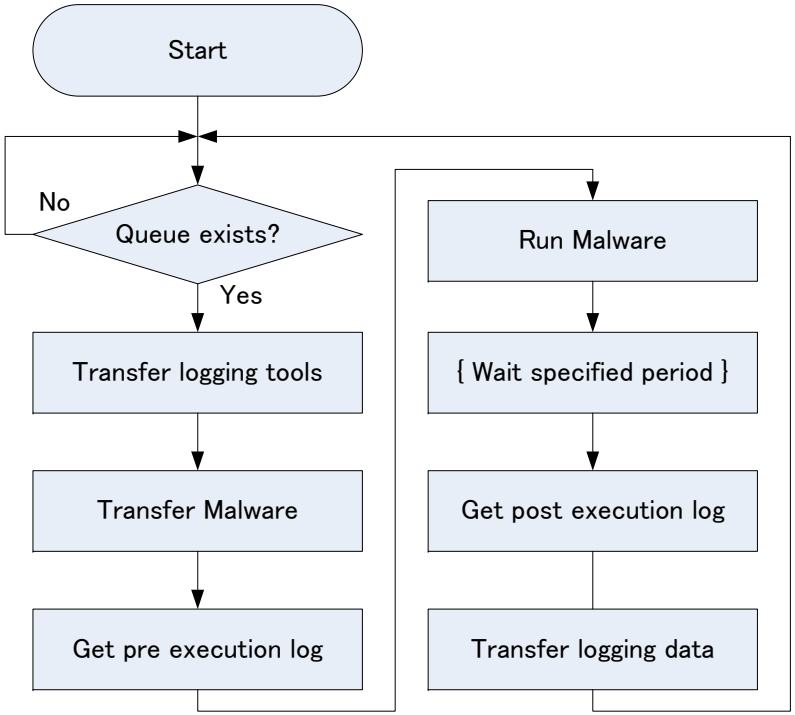
Malwareの実効制御1

- Malwareの挙動解析は，Linux（ホストOS）とこのホストにインストールした仮想マシン（VMWare Server）上で作動しMalwareを実行するWindows XP（VictimPC）で構成される.

1. ホスト内のディレクトを監視し，そこにファイルが置かれていれば解析を開始
2. VictimPCのOSが起動するとホストからスクリプト（scVictim）をダウンロード
3. VictimPCはscVictimを実行し，Malware実行前のログを取得
4. 解析対象のMalwareをホストから受信してこのMalwareを実行し，Malwareの実行後のログを取得
5. 取得したログはVictimPCからホストへと転送され，転送されたログをDBへ蓄積

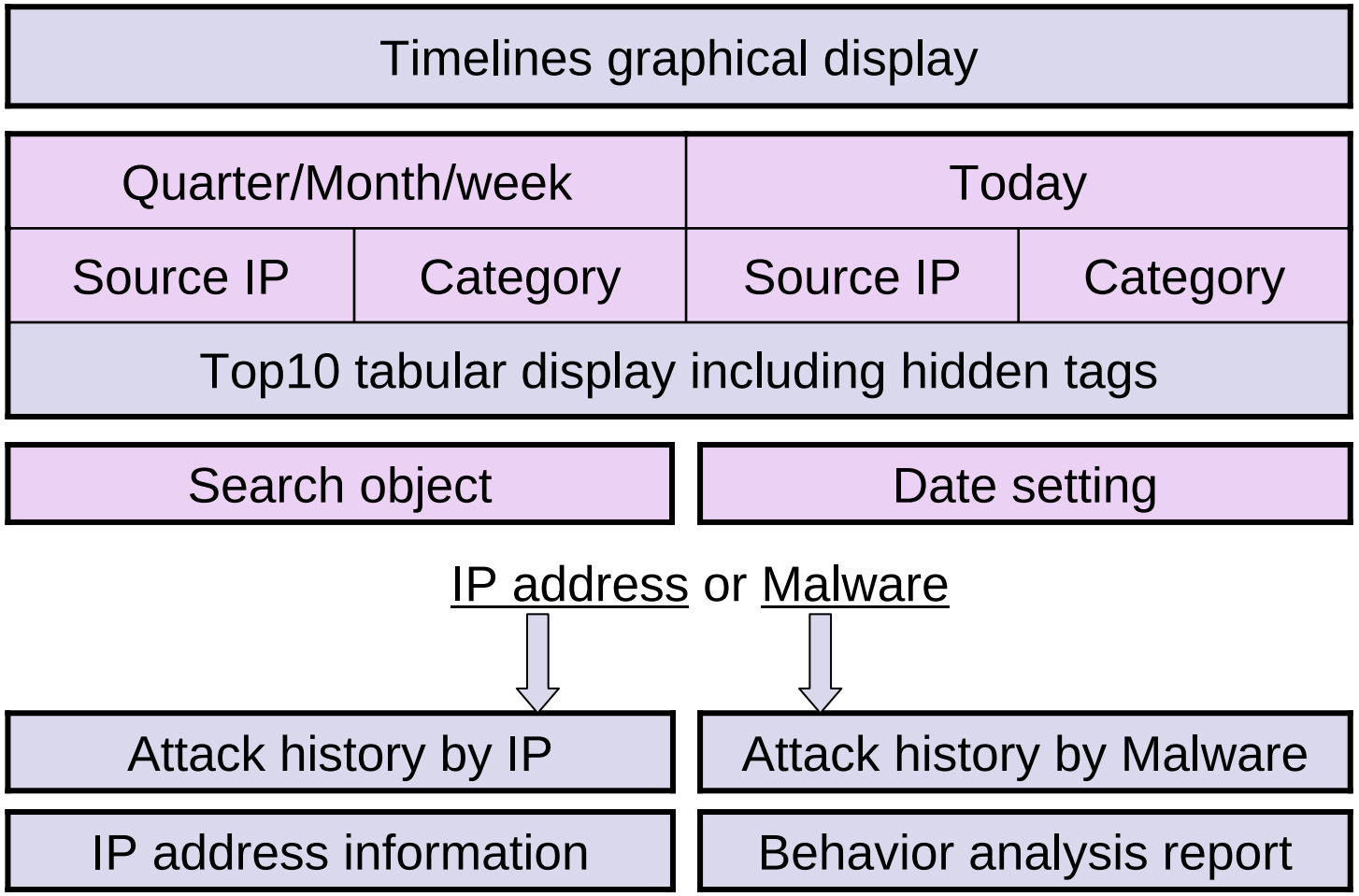
Malwareの実行制御2

- ホストからの制御が不安定になった場合
  - VMWareのホストOSとゲストOS間のI/Oポートを監視してゲストOS側の起動状態を取得
  - 一定期間にわたって状態を取得できない場合には，強制的にゲストOS側をリセットする
- 新規のハッシュ値を持ったMalwareを取得した場合
  →ファイルが自動的に解析のキューに転送され，Malwareの解析が実行される
- 1個のMalwareの解析に必要な時間は数分程度



ログ情報の視覚化

- 専用のソフトウェアの配布が不要なWebブラウザを利用
- 開発言語としてはHTMLと親和性の高いPHPを利用



模擬環境におけるMalwareの挙動解析の限界

- 一部のMalwareについてPC内からログを取得できなかった.
  - 仮想マシン上の環境では動かないもの
  - 実ネットワークと接続されているか確認し，その挙動を変化させる
- 捕獲したMalware5,158個体中，4,964個についてはベンダなどから得られる情報と同等または補完するデータの取得が可能.

表3　PC内のデータを取得できないMalwareトップ5

Ratio A/B	Malware	NoDate(A)	Sample(B)
100.0%	WORM_RBOT.EIC	14	14
91.7%	WORM_RBOT.DSU	11	12
83.9%	PE_PARITE.A	78	93
66.7%	PE_TENGA.A	4	6
52.9%	PE_VIRUT.D	9	17

（名称はトレンドマイクロ社製のウイルスバスター2007Trend Flex Securityによる）

まとめ

- 本論文では，ハニーポットを利用した定点観測によって，ボットネットを構成するMalwareを捕獲し，そのMalwareを実行させて挙動の解析を自動化するシステムの構築を行った.
- 本システムを利用することにより，Malwareの実行に伴う通信パケットやWindowsシステム内のリソースの変化など，Malwareの挙動に関する情報を得ることができる.
- 検討課題
  - 得られた情報を利用してMalware自体の詳細な分析やその分析結果を用いたMalwareの検出と種類の自動判定の手法
  - 模擬環境では実行できないMalwareの解析手法