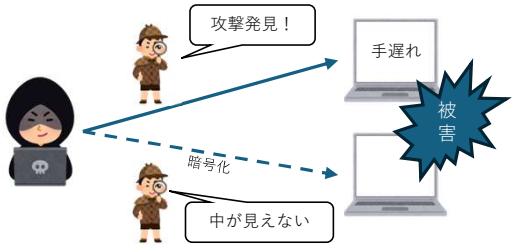
奈良女子大学 Nara Women's University 瀧本研究室の研究紹介

概 研究背景：マルウェア感染・ネットワークへの侵入を完全に防ぐことは困難
研究目標：組織への侵入・マルウェア感染による被害防止＆早期検知

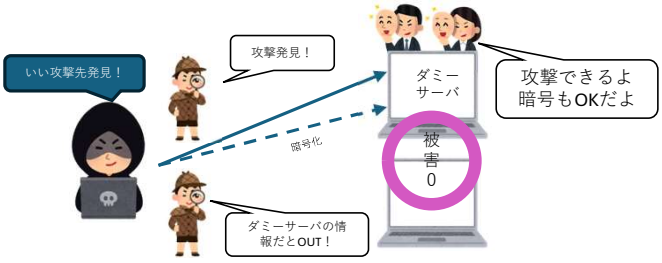
要 方 法 論 ：マルウェア・攻撃者をダマす新しい欺瞞的防御手法

ダミーサーバによる攻撃誘発技術

ラテラルムーブメント検知の課題
・暗号通信に対応不可
・検知≠被害防止



対策：ダミーサーバに攻撃させて検知
本研究の利点
・暗号通信の内容を取得可
・検知＝被害防止が可能



ダミーサーバ群の実装や実ネットワークでの運用試験などを実施中

解析環境を擬態するマルウェア活動抑制技術

マルウェア対策の課題
・感染を防ぐやり方には限界がある
・感染後の被害をどう防ぐか

着眼点
マルウェアの特徴
・解析されることを嫌う
・解析に気づくと動作停止（解析回避）

解析してる振りをしたら被害防止できる？

方策：マルウェアが嫌う解析技術の特徴を再現（擬態）しよう
デバッガ，仮想マシン，サンドボックス

CPU命令や例外処理フローといった特に擬態が難しい部分を重点的に研究中

その他の研究テーマ（ネットワーク系もやってます）
・携帯基地局間のハンドオーバ制御
  - 失敗とピンポンを防ぐ
・新しいDDoS攻撃に関する研究
  - TCPの特性を悪用する攻撃とその対策
・色調を利用した可視光通信技術
  - 色とデータをマッピング
・可視光通信の隊列走行への応用
  - 干渉のない近距離通信で車両制御

その他情報
・他大学との研究協力体制
  - 神戸大学・立命館大学・名古屋工業大学
  - 定期的なミーティング・発表会の開催
・セキュリティ人材が圧倒的不足
  - 大学・研究室での学びを社会で活かせる

・連絡・問合せ先
E-mail：takimoto [at] cc.nara-wu.ac.jp
お気軽にお問合せください.