侵入防御のためのプロセス活動リンク付方式の提案

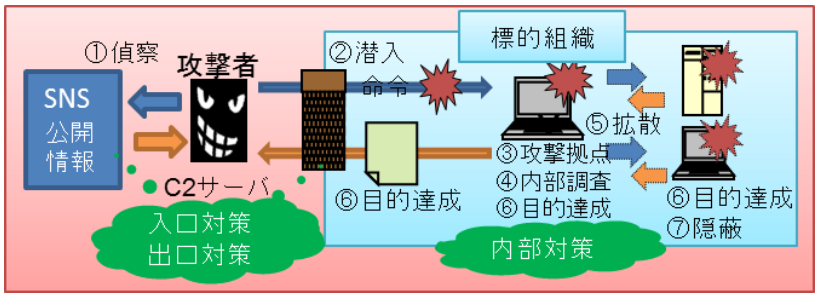
Linkage Analysis among Process Behavior for Intrusion Prevention

都丸裕大・ネットワーク分科会・情報セキュリティ大学院大学

Abstract

In this study, by using TOMOYO Linux, run the malwares that execution and creation files, they collect access information such as the communication to the C&C servers and analysis linkage with the absolute path among process behavior by malware.

【標的型攻撃概要】



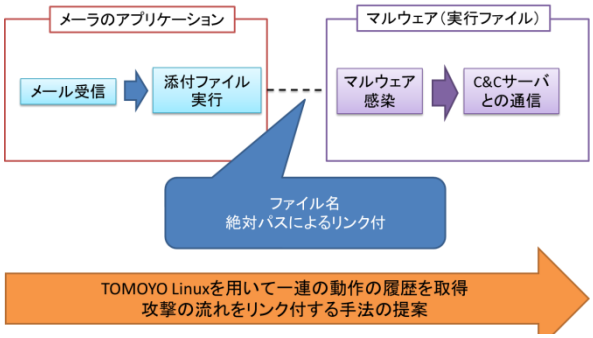
【現在の問題点】

既存の対策ではシグネチャなど瞬間的に有効である断片的な対策

【提案手法】

本提案では攻撃の流れをリンク付することでその流れを見てマルウェアであると判断し、アクセス制御を行うことを提案

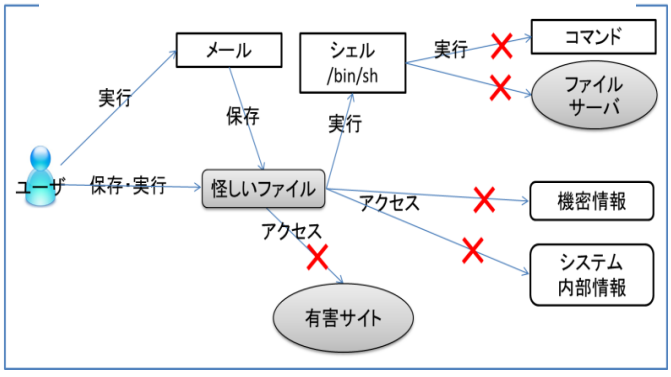
【マルウェアによる一連の動作について絶対パスでリンク付を行う手法】



【リンク付によるメリット】

- TOMOYO Linuxの学習モードにより、プログラムの実行履歴と各ドメインのアクセス要求の情報を収集できる
- その情報を基にアクセス制御するためのセキュリティポリシーの作成が可能
- ラベルとして絶対パスを使用しており、ファイルやプロセスのリンク付ができる
- リンク付により攻撃を遡って追うことができ、感染源の特定などを行うことができる

【リンク付によるアクセス制御のイメージ】



【本提案とサンドボックスの比較】

項目	提案手法	サンドボックス
対象OS	Linux	Windows
トレース機能	○	○
悪性判定機能	○	○
セキュリティポリシーへの対応	○	×

【課題】

アクセス制御の実装、総合的なシステム環境での検証、ドライブバイダウンロードなどその他の攻撃に対する有用性についての検証、C&Cサダウンロード後の動作など

【まとめ】

- TOMOYO Linuxの学習モードを活用することによりマルウェアの動的解析環境として有用
- メールの受信、添付ファイルの実行、外部との通信、ファイルアクセス等をリンク付したアクセス制御についてTOMOYO Linux上においてセキュリティポリシーを策定することにより、機械的に不正であると判断することが可能
- リンク付によりアクセス制御することで断片的な情報ではなく、流れを見て制御の可否の判断が可能
- 本提案により、監視対象となる動作の量を軽減することができ、解析者の負担軽減となる
- アクセスの流れを遡ることができ、感染源の特定や有害サイトの特定などが可能