マルウェア早期発見のためのシステム管理手法に関する研究

Study on system management method for malware early detection

杉井　俊也・ネットワーク分科会・情報セキュリティ大学院大学

Abstract :
There are various anti-malware products, but damage by malware is still expanding. Therefore, currently there is a need for a mechanism that is not only anti-malware products, multi-layer defense, and minimizes damage when infected with malware. In this research, we consider malware infection to occur, and research on system management that can be found at an early stage when infected with malware. Utilize the change characteristics at the endpoint when infected with malware, and discover endpoints suspected of being infected with malware by configuration management and comparison with other terminals. We plan to propose a system management method to measure and realize the effect of this method.

現在のマルウェア検知技術・手法	問題点
●パターンマッチング シグネチャと対象のファイルを比較し一致するものをマルウェアと判定する手法	・新しいマルウェアに対応できない。 ・日々、大量に発生する亜種に対応できない。
●振るまい検知 対象ファイルの動作特徴から、マルウェアを判定する手法	・正常なソフトウェアとマルウェアの差分を定義するのが困難である（誤検知とのバランス）。
●サンドボックス検知 仮想的な環境にて、マルウェアを実行し、動作観測し、悪性と判断できるものをマルウェア判定する手法	・人を介す要素が加わることによる回避 ・動作環境的制約を利用された回避技術が存在
●AI・機械学習	・未知数、未成熟、過度な期待

マルウェアの完全な検知は困難であり、マルウェアへの感染は発生する

マルウェア被害を最小に抑えるためには、**マルウェアの早期発見も重要**

研究内容

・マルウェア感染時のエンドポイントにおける変化特徴を利用し、システム構成管理や他端末と比較することによって、マルウェア感染の疑いのある端末を早期に検出する。

・上記を実現、実装するための、システム構成管理手法を提案する。

今後の予定

・マルウェア検体評価の実施、及び既存研究より変化特徴情報の生成

・システム管理の現状把握とマルウェア早期検知を見据えた、今後のシステム管理のあり方の検討

・マルウェア早期発見のためのシステム管理手法の実装と検知試験