複合型手法に基づくランサムウェアのリアルタイム検出に関する研究

Research on real-time detection of ransomware based on a composite method

林 泊舟・システム分科会・情報セキュリティ大学院大学

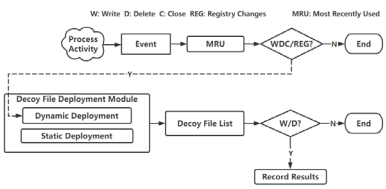
Abstract: With the rise of the Internet and cryptocurrencies, people's lifestyles have changed, and more data is being exposed to the Internet, leading to increased threats from Ransomware. Ransomware attacks have caused millions of dollars in damages since 2017, making detection and decryption a research hotspot. This study proposes a real-time ransomware detection framework based on dynamic detection of ransomware behavior using existing pattern matching detection methods, file protection, and three main detection methods: decoy file-based, behavior analysis-based, and cryptographic call-based. The study discusses improvements in detection rates and file protection evaluation.

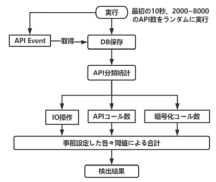
はじめに

近年、ランサムウェアが社会的な問題となっており、その対策が喫緊の課題となっている。それで、リアルタイム検出・防御、ファイル保護が必要である。そして、ほとんどの研究は機械学習を利用するという状況になって、従来手法の再利用可能を検討する必要と考えられる。

提案手法

- デコイファイル分析モジュール、挙動分析モジュール、暗号化分析モジュール、三つに分けられる。
- デコイファイル分析モジュールは、事前に設定したディレクトリにデコイファイルを配置しておく。デコイファイルリストの変更を監視する。
- プロセスイベントログを取得してから分析する。IO操作、通常API操作、暗号化APIに分けられる。ランサムウェア起動時に大量のAPIを呼び出す特性により閾値を設定する。
- 検出後追跡し、プロセスを中断させる。

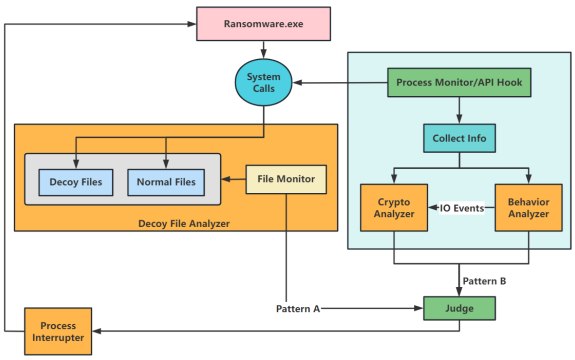


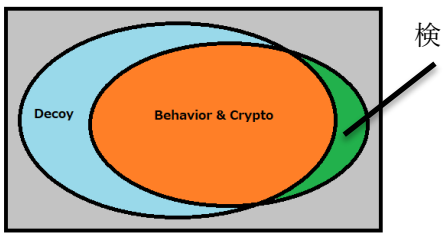


実験結果

組み合わせた後、平均2%程度精度が向上している。ファイル平均損失率は0.2となる。一定程度保護することができる。

	デコイファイル	併用
平均 Accuracy	92.80%	95.22%(+2.42%)





まとめと課題

本研究で提案するフレームワークは、機械学習を用いずに従来の複数の検知方法を組み合わせることで、検出率を向上させ、ユーザーファイルをある程度保護することができる。

- シミュレーション環境で、実際の状況とギャップがある
- デコイファイルはユーザーにとって負担になる。
- ランサムウェアは通常暗号化ライブラリを使用しない可能性がある。