マルウェア検知のためのシステム管理手法に関する検討

Study on system management method for malware 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：from the viewpoint of system management, we consider malware detection by a method of detecting abnormal values from change history by managing endpoint computers. Defect normality from information such as software, registry, process, task, directory, etc. to detect abnormality. In addition, it aims at operation at low cost and easy operating.

1．現状の課題

セキュリティベンダーFireEye社によると
マルウェア等によりセキュリティが侵害されてから

- セキュリティ侵害発覚までに　：205日
- 侵害を外部から指摘される確立：69%
- 最新のシグネチャの適応状況　：100%

※サイバー攻撃による情報流出は一瞬も、発覚までは半年以上 - FireEye（出典：マイナビニュース）

２０１６年に公表された標的型攻撃においても

- 自組織で発見できない。（外部からの指摘で発覚）
- 発見に時間を要しているケースが多く見られる。

#	公表月	組織	発覚	内容
1	6月	旅行会社	自組織	メール開封から5日後に不審な通信を確認し発覚
2	6月	大学	自組織	メール開封から5日後に不審な通信を確認し発覚
3	7月	大学	外部	メール開封から1日後に外部の指摘を受け発覚
4	10月	大学	外部	2015年11月にメールから進入、進入から6ヶ月以上経過
5	11月	金融機関	自組織	メール開封当日に不正プログラムのダウンロードに気づく
6	11月	経済団体	自組織	内部調査の結果不審な通信の存在を確認
7	11月	出版会社	外部	進入時期不明

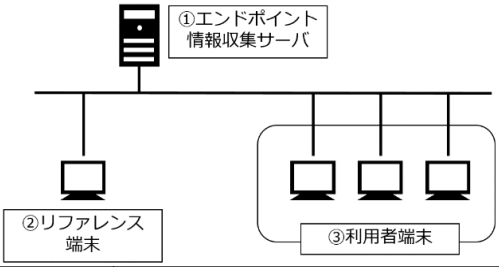
※トレンドマイクロ　2016年　年間セキュリティラウンドアップを基に作成

2．アプローチ

通常実施している**システム管理を活用したマルウェア検知手法**を検討する。
既存のマルウェア対策と併せて多層防御を実現

**最小限の追加コストで
マルウェア検知率を向上**

3．検討システム

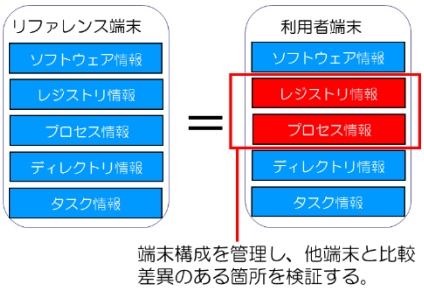


①エンドポイント情報収集サーバ	リファレンス端末、利用者端末より情報を収集・比較しマルウェアの検知を実施する。
②リファレンス端末	利用者端末との比較に利用される端末、利用者が操作しない正常な状態として定義する。
③利用者端末	端末利用者が実際の業務に利用する端末

②リファレンス端末と③利用者端末の日々の変更履歴を①エンドポイント情報収集サーバに送信、比較することで良性、悪性（マルウェア）を検出する。

4．検知手法

端末の全ての変更履歴を収集するのは現実的ではないため、ソフトウェア情報、レジストリ情報、プロセス情報、ディレクトリ情報、タスク情報の５つの情報を取得する。
（ディレクトリ、レジストリは一部のみ取得）
※マルウェアの動作実績に関する先行研究より上記の比較によるマルウェア検知は効果が期待できる。
上記情報についてリファレンス端末と利用者端末の差分を比較することで、変更を検知する。



端末構成を管理し、他端末と比較
差異のある箇所を検証する。

また、比較した差分について、良性か悪性かを判断するために、端末の動作における正常をルールとして定義または制限を実施する。
これにより、マルウェアに感染した際の関連する脅威・痕跡を目立たせることで、マルウェアの検知を実施する。

5．制御とルール

以下を定義することで、マルウェアの動作による変更とユーザによる変更を区別し、差分情報から悪性変更（マルウェア）の検知が可能となる。

ソフトウェア情報	組織内で認可するソフトウェアを定義し、配置されるファイル情報を把握し基準を作成する。
レジストリ情報	ソフトウェアの自動実行やサービス登録等の起動情報を把握し、基準を作成する。
プロセス情報	実行プロセス情報を把握し、基準を作成する。
ディレクトリ情報	プログラムフォルダやファイル保存フォルダをルール設定し、基準を作成する。
タスク情報	タスクに命名規則を設定し、自主的に登録したものか否かを判定可能にする。