2W-08

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

杉井　俊也†　　後藤　厚宏†
情報セキュリティ大学院大学†

概要

昨今、マルウェアによる被害は企業・団体における継続的な脅威であり、企業に侵入したマルウェアを早期に検出することは重要である。

本研究では、システム管理の観点から、エンドポイントコンピュータを管理することで複数の管理対象エンドポイントコンピュータの変更履歴から異常値を検出する検知法によるマルウェア検知を検討する。ソフトウェア、レジストリ、プロセス、タスク、ディレクトリなどの情報から正常を定義して異常を検知する。また、低コストで実装が容易な手法を目指す。

１．従来のマルウェア対策改善について

従来、マルウェア対策としては、アンチウイルスソフト等が普及しているが、従来の対策では新たなマルウェア脅威の検出について高い精度を達成することはできない[1]。また、2016 年に標的型攻撃を受けた事例においても、自組織では発見できない、または発見に時間を要した事例が多い[2]。以上の通り、今日のマルウェア対策システムのみでは、マルウェアを早期に検知することは困難である。

表１　2016 年に確認された標的型攻撃[2]

#	公表月	組織	発覚	内容
1	6 月	旅行会社	自組織で確認	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	自組織で確認	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	外部からの指摘	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	外部からの指摘	2015年11 月にメールから侵入、侵入から6か月以上経過
5	11 月	金融機関	自組織で確認	メール開封当日に不正プログラムダウンロードに気づく
6	11 月	経済団体	自組織で確認	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	外部からの指摘	侵入時期不明

そこで本稿では、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。本手法では、既存のマルウェア検知システムと併せて、マルウェア対策の多層防御を実現し、最小限の追加対策コストによって、マルウェア検知率を向上させることを目指す。

Study on system management method for malware detection
†Toshiya SUGII、Atsuhiro GOTO
†Institute of Information Security

２．システム管理によるマルウェア検知の検討

本稿では、システム管理によってマルウェアを検知する手法を検討する。

まず、組織内に標準の構成となるエンドポイントを定義・作成し、組織内にて利用するエンドポイントは作成した標準構成のエンドポイントを利用する。また、利用者が利用するエンドポイントとは別に標準構成のエンドポイントを、リファレンス端末として運用をする。リファレンス端末はその組織内エンドポイントにおける正常の定義を担う。

上記前提の元、各エンドポイントの変更特徴を記録し、リファレンス端末とその他の利用者が利用するエンドポイントを比較することで、差分の検出を行う。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。

尚、本手法の対象は企業団体で一般的に利用されている、WindowsOS とする。

３．マルウェア検知システムの構成

本手法で想定するシステム構成は以下の通りである。

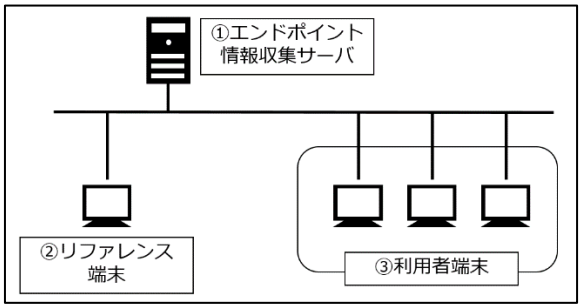

図１　システム構成図

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利用者端末と同様の構成のり端末、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

４．エンドポイント情報の取得と比較

本手法では、エンドポイントの変更特徴を利用して、マルウェアの検知を実施する。しかし、エンドポイントの変更特徴を全て記録するのは、現実的ではない。従って、本手法における検討では、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ことにした。尚、レジストリ情報とディレクトリ情報においては、一部情報のみを取得する。

各利用者端末より収集した上記情報をリファレンス端末の該当箇所と比較することで、差分情報を抽出する。差分情報において、正常か異常かを定義することでマルウェアを検知する。

５．マルウェアの動作特徴

４章にて取得する５つの情報について定義したが、本情報を取得し、リファレンス端末と比較することでマルウェアの検知が可能か、マルウェアの動作特徴から、検討を実施した。

マルウェアの動作について纏めた Ulrich Bayer 等の研究[3]では、レジストリ登録を実施するマルウェアが全体の約 65%（うち特定のキーに登録するものが最大で約 17%存在する）存在すること、また、何かしらのファイルを作成するマルウェアが約 71%あることが確認できる。

同様に、株式会社 FFRI が 2017/3～2017/4 に収集した PE 形式かつ実行可能マルウェア 6251 検体の動的解析ログである FFRI Dataset 2017[4]の分析を実施した。結果として特定のレジストリに書き込みを実施する検体が最大で約 32%存在し、ディレクトリにおいても特定のディレクトリにファイルを作成するものが最大で約 22%存在する。この結果は Ulrich Bayer 等の研究[3]と類似しており、マルウェアが利用する動作特徴は本検知法で利用する箇所において、経年的に変化していないことが伺える。

これ等の結果から４章で定義したエンドポイントの取得情報を用いて既知・未知を問わずマルウェアの検知に有望であると考えられる。このため、未知のマルウェア検知に限界のある既存のマルウェア対策に加えて本手法を実施することで、多層防御を実現し、マルウェア検知率が向上することが期待できる。

６．差分情報における正常の定義

本手法ではリファレンス端末と利用者端末を比較し、差分において、異常であるか、正常であるかを分別する必要がある。これにあたり、異常（マルウェアであると想定されるもの）を検知するため、エンドポイントの差分において正常を定義する必要がある。

しかし、利用者端末は一般業務用 WindowsOS であることから、様々な業務が実行され、端末内のデータが作成・更新・削除されること、また、ソフトウェアアップデート等が実施され、都度端末の情報に変更が発生することを考慮しなければならない。このため、以下の形で正常を定義する。

①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。

②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。

③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。

④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。

⑤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。

上記を定義することで、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、差分情報から悪性のものの検知が可能となる。

７．まとめと今後の予定

本稿では、マルウェアを検知するためのシステム管理手法について検討し、その概念を示すと共に、既存のマルウェア対策との多層防御によるマルウェア検知率向上の可能性を示した。

今後は本検知法の有用性・実効性の検証を実施する。尚、検証にあたっては、実際の企業の１部門（１０端末を想定）からログを取得し内容を検証する予定である。また、本検知法を実装するためのガイドを提示する。その後、本検知法を実装した際に内容を視覚的に確認できるツールを開発する予定である。

参考文献

[1] 独立行政法人情報処理推進機構：NIST SP-800-83 マルウェアによるインシデントの防止と対応のためのガイド IPA 翻訳

[2] Trend Micro : Trend Labs 2016 年 年間セキュリティラウンドアップ

[3] Ulrich Bayer 他 : A View on Current Malware Behaviors、LEET ‘09 Proceedings of the 2nd USENIX conference on Large-scale exploits and emergent threats: botnets, spyware, worms, and more (2009)

[4] 株式会社 FFRI:FFRI Dataset2017 のご紹介, MWS2017 意見交換会, 2017.