ネットワーク通信アラートを用いた攻撃予測に関する研究

森 俊貴 (1210055)

北陸先端科学技術大学院大学 情報科学研究科

2014 年 2 月 12 日

キーワード: マルウェア，IDS，攻撃予測.

近年サイバー攻撃の数が増大している．特に，マルウェア等の自動プログラムを用いた攻撃が増加しており，その被害が深刻である．侵入検知システム（IDS）は，マルウェアに対する有効な対策の一つであると考えられている．しかし，実際は IDS は膨大なアラートを発生させることがあるため，管理者はこのアラートに対してどのように対処すればよいかの判断が難しい．これに対して，IDS のアラートを学習して攻撃を予測する手法（Nexat）が，Cipriano らによって 2011 年に提案された．この著者らは，カリフォルニア大学で開催されたハッキングコンペにおける攻撃ログを分析・評価し，Nexat の有効性を示した．しかしながら，この Nexat が IDS のアラートが必ずしも発生するとは限らないマルウェアの予測に使えるかどうかは不明である．

そこで，本研究では，まず Nexat がマルウェアの予測にどの程度有効であるかを評価した．IDS ではマルウェアダウンロードをアラートとして出ないため，マルウェアダウンロードを検知するためのローカルルールを作成し，学習に利用した．一方，予測に利用するアラートにはローカルルールを含ませない．このことにより，マルウェアに特化した学習に対し，通常の IDS アラートのみを用いた性能評価を実施した．この結果，およそ 7 割の確率でマルウェアダウンロードの予測を実現することができた．しかし，Nexat はネットワーク全般の攻撃予測をアラート単位で行うものであり，攻撃手法がある程度定例化されているマルウェアに対しては冗長であることが考えられる．

本研究ではさらに，Nexat における予測アルゴリズムをマルウェアに特化した簡易化を行った．これは，マルウェアがロボットプログラムであることを考慮して，主に予測フェーズを改良した．その結果，およそ 9 割の確率でマルウェアダウンロードの予測を実現することができた．