4ZD-04

正常ログ残存を前提とするサイバー攻撃推定手法の性能評価

熊崎 真仁† 長谷川 皓一† 山口 由紀子† 嶋田 創† 高倉 弘喜‡

名古屋大学† 国立情報学研究所‡

1. はじめに

企業などの組織を狙った標的型攻撃の被害は年々拡大し、社会問題となっている。これらの攻撃による被害を低減するためには侵入の防御だけではなく早期対応が重要となる。その一方で、組織のネットワークは国際化や通信技術の発展により、複数拠点に跨る大規模なネットワークが構成されることが多い。このような組織の場合、各拠点にネットワーク管理者が配置されることが一般的である。しかし、コスト等の都合により、本社はサイバーセキュリティに熟達した管理者やCSIRTのような専門のセキュリティ対応チームが配置される一方で、他拠点の管理者はセキュリティインシデントに対応できるレベルに達していないことも多い。そのため、インシデントの調査や対応方法の確認に長い時間を要することが考えられ、インシデント対応が遅延することが懸念される。

この問題の解決策として、脅威情報を組織内で共有するシステムが提案されている[1]。しかし、前述の通り管理者のスキルには差があるため、脅威情報の共有だけでは支援不足であることが予想される。そのため、我々はスキル差を吸収する細やかな対応支援を実現するシステムを提案した[2]。提案システムは組織内の生ログから攻撃に関連するログを抽出し、その攻撃手段や活動時間の推測を行うことで攻撃の全貌の俯瞰を可能にする。

本稿では提案システムにおける攻撃に関連するログの抽出で要求される正確性を確認するため、正常ログが大量に存在する状態で攻撃手段の推測を行い、正常ログが推測に与える影響の評価を行った。

2. サイバー攻撃推定手法と入力ログの作成

我々は以前、サイバー攻撃推定手法について提案した[2]。本手法では、MITRE ATT&CK などのサイバー攻撃フレームワークなどで記述されるサイバー攻撃手法を元に、重要度などの情報を付加した「攻撃シナリオテーブル」と、サイバー攻撃によって発生した各種ログを時系列順に並べた「攻撃ログ」を利用する。攻撃ログを参照し、攻撃シナリオテーブル中の攻撃手法について、各手法に対応するログやその重要度からスコアを算出し、攻撃で利用された手法や実行時間を推定する。図1に手法の概要を示す。

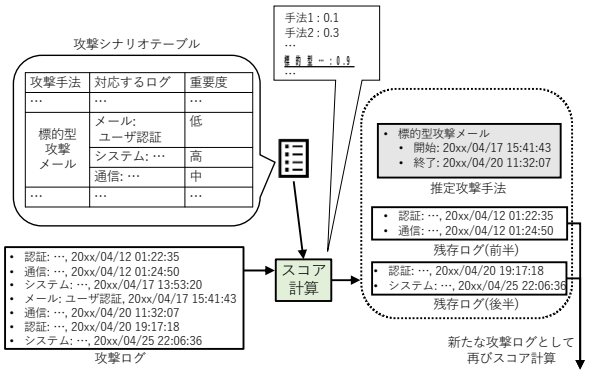

図1: サイバー攻撃推定手法

提案システムは、サイバー攻撃推定手法で利用する攻撃ログの作成機能を持つ。各種ログについて、その種類ごとに対応したホワイトリストを生成し、リストを用いて正常ログを除去する。例として、通信ログの場合、通信の周期性を利用したホワイトリストを生成する。正常な通信と比較して、サイバー攻撃による通信は周期的である傾向がある。そのため、長期間のログにおいて通信間隔に周期性が見られない通信先を正常な通信とし、ホワイトリストに登録する。このようにして作成したホワイトリストによって生ログから正常ログを除去することで、正常ではないログのみが残ったログを作成し、これを攻撃ログとして用いる。

3. 正常ログ混在時の性能評価

提案手法で利用する攻撃ログはサイバー攻撃によって発生したログであると定義しているが、実際に抽出して攻撃ログを作成する場合、正常な活動によって発生したログが混入することが想定される。そこで、実験環境において模擬サイバー攻撃と正常な業務活動を同時に行うことで、攻撃に関連するログと正常ログを同時に生成し、これらを混合したログを攻撃ログとして提案手法による攻撃手段の推測を行った。

Performance Evaluation of a Cyber Attack Estimation Method in the Presence of Legitimate Logs, Masahito Kumazaki†, Hirokazu Hasegawa†, Yukiko Yamaguchi†, Hajime Shimada†, Hiroki Takakura‡.

† Nagoya University

‡ National Institute Informatics

表 1: 正常ログを除去した場合の推測的中率

正常ログの除去率	標的型攻撃メール	特権昇格	パスワード奪取	ネットワーク探索	マルウェア拡散	特権昇格	パスワード奪取	目的情報の奪取	全体の推測的中率
100%(攻撃ログのみ)	1.000	0.483	0.994	0.702	0.002	0.133	0.994	0.008	0.476
90%	0.608	0.483	0.994	0.012	0.998	0.139	0.994	0.008	0.555
80%	0.808	0.250	0.061	0.031	0.996	0.106	0.994	0.008	0.460
70%	0.525	0.142	0.000	0.000	0.852	0.139	0.000	0.000	0.286
60%	0.783	0.483	0.111	0.010	0.852	0.106	0.000	0.000	0.336
50%	0.817	0.083	0.000	0.000	0.998	0.606	0.000	0.000	0.387
40%	0.867	0.217	0.000	0.010	0.983	0.106	0.000	0.000	0.347
30%	0.867	0.083	0.000	0.000	0.838	0.206	0.000	0.000	0.307
20%	0.842	0.083	0.000	0.000	0.983	0.117	0.000	0.000	0.336
10%	0.842	0.083	0.022	0.000	0.717	0.194	0.000	0.000	0.274
0%	0.842	0.083	0.000	0.000	0.969	0.117	0.000	0.000	0.332

3.1 実験内容

1 つの模擬サイバー攻撃シナリオと 3 つの通常業務シナリオを用意し、サイバー攻撃シナリオと 1 つの業務シナリオを同時に実験環境で実行した。これらのシナリオの実行時間は全て 30 分間であり、各業務シナリオは出力されるログに差分があるように調整した。その後、クライアントの各 Windows 端末のシステムログとセキュリティログ、ルータの通信ログ、メールサーバの認証ログ、ファイルサーバの samba ログを取得し、時系列順に整列した。これらの攻撃と通常業務が混在したログを 3 シナリオ分取得した。

このようにして得られたログを用いて 2 節で提案した手法を用いて攻撃手法の推測を行った。推測された攻撃手法と実際に用いた攻撃手法について、その手法と実行時間を照らし合わせ的中率を確認した。

また、正常ログの量による影響を確認するため、得られたログから業務シナリオによる正常ログの除去を実施した。ログの除去は一定割合になるようにランダムで行い、異なる割合毎に提案手法を用いて攻撃手法の推測を行うことで、その手法と実行時間について的中率を確認した。

3.2 実験結果

実験の結果、シナリオによる大きな差分は見られなかった。そこで本稿ではシナリオ 1 についてのみ正常ログを除去した場合の実験結果を述べる。

表 1 にシナリオ 1 について正常ログを除去した場合の推測的中率を示す。いずれのシナリオにおいても、正常ログの除去率が 80%の場合の的中率と 70%の場合の的中率に大きな差が見られた。以上より、提案手法で利用する攻撃ログについて、混在が許容できる正常ログは正常ログ全体の 20%程度であると考えられる。また、攻撃ログのみの的中率より正常ログが混在した時の的中率が高くなる場合が見られた。これは、本来の攻撃ログでは推測できていない手法を正常ログによって的中してしまっていることが原因である。このような誤検知による影響を低減するため、スコアの計算方法や攻撃手法の決定プロセスについても改善が必要だと考えられる。

4. おわりに

本稿では組織内のログからサイバー攻撃で用いられた手法や実行時間を推測する手法を提案した。また、提案手法で入力されるログについて、正常ログが攻撃手法の推測に与える影響について評価を行った。その結果、正常ログ全体の 80%以上を除去できれば、推測に与える影響が少なくなることを確認した。

今後は今回の実験結果を踏まえ、攻撃に関連するログの抽出手法を考案することで攻撃の全貌俯瞰を可能にするシステムを実装し、その性能評価を行う予定である。また、実際の攻撃では初期侵入や横展開の段階における進行速度が非常に遅いものが存在する。このような攻撃に対応するため、攻撃手法の推測プロセスにおいて時間経過によるスコアの変化の利用などを検討する必要がある。

参考文献

[1] C. Wagner, et al., “Misp: The design and implementation of a collaborative threat intelligence sharing platform,” The 2016 ACM on Workshop on Information Sharing and Collaborative Security, 2016.

[2] M. Kumazaki, et al., “Cyber Attack Stage Tracing System Based on Attack Scenario Comparison,” The 8th International Conference on Information Systems Security and Privacy (ICISSP 2022), 2022.