[Work in Progress] 研究報告

組織における標的型攻撃に対する挙動分析システムの提案

大橋 宗治[1]　長谷川 皓一[1]　山口 由紀子[1]　嶋田 創[1]

Proposal of Behavior Analysis System for Targeted Attacks

近年、特定の組織内の情報を狙った標的型攻撃が深刻な脅威となっている。しかし日々攻撃が巧妙化する中、攻撃者の侵入を防ぎきることは難しく、侵入後の対策が求められている。攻撃者は侵入後、感染させた端末を足がかりに機密情報の入手など目的を達成するために、LAN 内の他の端末にも攻撃を行い、感染を拡大させることが多い。これに対し、ネットワーク（以下、NW）内部分離設計によってインシデント発生時に対策設計支援を行うシステム [1] の研究が行われている。組織内の端末に対して感染が発覚した場合、被害を広げないために感染端末を NW から切り離すなど、隔離処置を行う場合が多い。隔離によって攻撃者は攻撃を続けることができないため、一時的に組織を守ることができる。しかし、攻撃に関する情報は隔離を行うまでのものしか集めることができず、攻撃者がどんな情報を狙っていたのか、どのような手順で攻撃を行う予定であったのかなどを知ることができない。一般的に、標的型攻撃の攻撃者は成功するまで執拗に攻撃を繰り返すため、先の攻撃手段を知ることは、同一攻撃者からの対策を立てる上で好ましい。

そこで我々は侵入が確認された後も、組織の実 NW に大きな影響を及ぼさずに攻撃者の挙動を解析することのできるシステムを提案する。

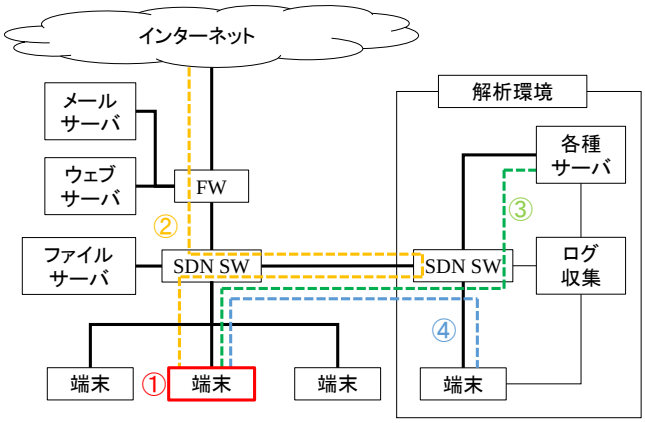

図 1　提案システム

提案システムを図 1 に示す。解析環境は仮想マシン上で動作し、内部は左側の小規模組織の NW を模したものとなっており、各種サーバや端末も実組織内の環境を模倣するように動作する。図 1①にて実 NW 内で感染端末が発見されると感染端末の通信は SDN SW(Software Defined Network Switch) によって解析環境に引き込まれる。

感染端末がインターネットと通信を行う場合は、実 NW の SDN SW によって一旦解析環境内の SDN SW に送り、再び実 NW 内の SDN SW に戻す（図 1②）。このような経路をとることで、感染端末とインターネット間の通信を遮断することなく、解析環境内の SDN SW からトラフィック情報を取得することができる。取得した情報より、攻撃者が感染端末からインターネット上のサーバに対して大量の通信を送るなど、攻撃と判断される動作が確認された場合、SDN SW によって遮断する。一方で、新マルウェアのダウンロードや C&C サーバへの通信などは遮断せず、攻撃手法に関する情報を収集する。

感染端末が組織内の各種サーバと通信を行う場合も同様に、実 NW 内の SDN SW と解析環境内の SDN SW を経由して解析用サーバと通信を行わせる（図 1③）。このサーバは、複数のサーバを 1VM 上に設置し、SDN SW 側で双方向の通信の IP アドレスを打ち替え、感染端末からは実サーバにアクセスしているように見せかける。「データベース上のどの情報を取得しようとしたのか」などの細かな挙動は、解析用の各種サーバのホストから取得する。

感染端末が実 NW 内の他端末と通信を行う場合も同様の経路で解析用端末へと送る（図 1④）。解析用端末に関しても同様に SDN SW で双方向の通信の IP アドレスを打ち替え、1VM の解析用端末で複数の実 NW 内の端末を装い、ホストベースのログを取得する。

提案したシステムで得られたログより、攻撃者の目的や挙動を把握することができ、組織が今後のセキュリティ戦略を立てる上で役立てることが期待できる。

今後は提案システムの実装と、システムの有効性を確認するため攻撃シナリオの作成、実験を行っていく予定である。

参考文献

[1] H Hasegawa, et al. An incident response support system based on seriousness of infection. *ICOIN2016*, pp. 69–74, January 2016.

[1] 名古屋大学