2015 年 10 月 13 日
株式会社日立製作所

標的型サイバー攻撃の拡散活動を検出する技術を開発

不審動作をする端末間の関係を可視化し、ステルス型マルウェアなどによる攻撃を検知

株式会社日立製作所(執行役社長兼 COO:東原 敏昭／以下、日立)は、標的型サイバー攻撃*1の拡散活動を検出する技術を開発しました。標的型攻撃で社内ネットワークに侵入した攻撃者は、情報漏えいやシステム破壊などを目的として、パソコンやサーバーなどの端末に次々と侵入する拡散活動を行います。本技術は、攻撃者に侵入された可能性がある端末を検出し、別の端末に侵入していく過程の端末間の関係を可視化することで、標的型攻撃を検知します。アンチウイルスソフトウェアなど従来の対策を補完し、個々の端末を個別に分析するだけでは検知が難しいステルス型マルウェア*2などによる標的型攻撃の早期検知が期待されます。

近年、情報漏えいやシステム破壊を目的とした、官公庁や企業、社会インフラに対する標的型攻撃が増加しています。警察庁の調べでは平成 26 年の発生件数は前年比 3.5 倍の 1,723 件に上っています。これに加え、攻撃方法はますます巧妙化しています。例えば、最近の攻撃には、ステルス型マルウェアに加えてゼロデイ脆弱性*3 が用いられます。さらに、端末や周囲のネットワーク状況を探索できるOS標準搭載のコマンドや、本来は攻撃用途に開発されたわけではないフリーウェアが悪用される傾向にあります。このような巧妙な攻撃は、個々の端末では明確に悪意があると判断できる動作を行いません。このため、ウイルス定義を用いた一般的なアンチウイルスソフトウェアや既知の攻撃に共通する特徴を元に個々の端末を分析して検知する技術など、従来存在していた対策では検知が困難になってきています。また、巧妙な攻撃を検知する対策の一つとして、事前に作成した許可リストに載っていないプログラムが起動すると、攻撃が発生したと判断するホワイトリスト型対策がありますが、プログラムの新規導入や更新が頻繁に起きる環境では運用しづらいという課題があります。

そこで日立は、このような巧妙な攻撃を検知するには、個々の端末単位ではなく複数の端末の動作を関連付けた統合的な分析が必要と考え、攻撃者が別の端末に侵入していく過程で、通常見られない不審動作を行う端末が次々と発生する点に着目しました。そして、(1)機械学習を活用して拡散活動に関わった可能性がある不審端末を検出し、(2)不審端末間のアクセスタイミングを分析して端末間の関係を可視化することで、拡散活動を検出する技術を開発しました。本技術により、個々の端末を個別に分析するだけでは検知が難しかったステルス型マルウェアなどによる標的型攻撃の早期検知ができます。

今回開発した技術の特徴は以下の通りです。

（1）機械学習を活用して不審端末を検出

攻撃者が侵入先の端末で行う活動の目的は情報漏えいやシステム破壊であり、ドキュメント作成やWeb閲覧、サービス提供といった、パソコンやサーバーの本来の利用目的と異なります。このため、攻撃者が端末に侵入すると、普段利用されないプログラムが起動するなど、通常見られない動作が頻繁に発生します。そこで、端末の通常動作の特徴を機械学習によりモデル化し、普段利用されないプログラムの起動や普段アクセスしない端末への通信などを不審動作として特定する、6種類のセンサーを開発しました。本センサー群が観測した不審動作の発生頻度を元に、社内ネットワークに設置した分析サーバーが不審端末を検出します。

（2）不審端末間のアクセスタイミングを分析して端末間の関係を可視化

攻撃者は、脆弱性攻撃*4 や遠隔ログインなどの不正アクセスにより、侵入した端末からさらに別の端末に侵入します。日立は、（1）の技術により不審端末と判定された端末が、過去数時間内に他の不審端末からアクセスされた履歴があるかどうかを元に、端末間の関係を、攻撃経路を示すグラフとして可視化する技術を開発しました。関係がある端末群の数が一定以上になると、拡散活動が行われていると判断します。

本技術は、端末の不審動作や関係を元に各端末が受けた攻撃内容や攻撃経路を分析できるため、攻撃の全容解明や対策立案などにも役立てることができます。

今回開発した技術の性能を測定するため、過去に発生した攻撃事例やセキュリティベンダの報告、学術論文などを元に代表的な標的型攻撃を模擬した攻撃シナリオを策定し、実証実験を社内で実施しました。その結果、一般的に想定される標的型攻撃の検知率97%を達成し、誤検知が発生する頻度を従来のホワイトリスト型対策の10分の1に削減したことを確認しました。本技術は、高い検知率と低い誤検知頻度の双方を実現するものであり、運用コストが低く効果的な標的型攻撃対策に大きく寄与します。

標的型攻撃対策技術の重要性は、情報系ネットワークに留まらず、製造プラントの制御ネットワークやIoTなどにも拡大しています。日立は、本技術を社会インフラシステムに活用し、安全・安心な社会の実現に貢献していきます。

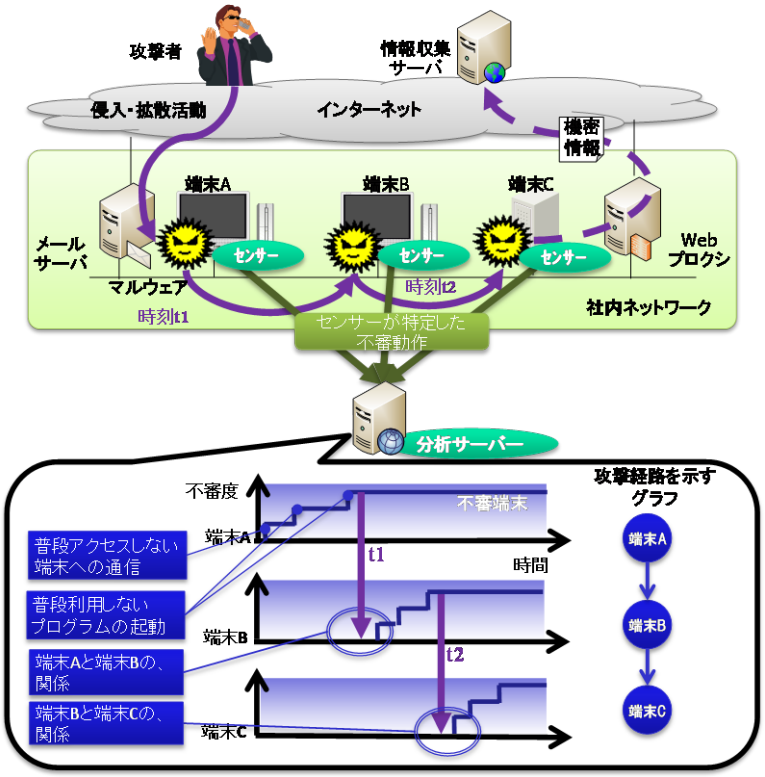
なお、本成果は、10月21日から長崎県で開催される「コンピュータセキュリティシンポジウム2015（CSS2015）」にて発表する予定です。

*1 官公庁や企業、社会インフラなど特定組織のネットワークを執拗に狙い、情報漏えいや情報システムの破壊を行う攻撃。通常、マルウェア付きメールなどで特定の端末にコンピュータウイルスなどを感染させたのち、他の端末へも侵入を広げて被害を拡大させていく

*2 端末内で明確に悪意がある動作をほとんど行わず、アンチウイルスソフトウェアによる検知が難しいマルウェア

*3 ウイルス対策ベンダなどのセキュリティ組織に知られていないプログラムの欠陥・不具合

*4 サービスの脆弱性を悪用して端末の制御を奪う攻撃



今回開発した技術が標的型攻撃を検知するまでのプロセス

■照会先

株式会社日立製作所 研究開発グループ 技術統括センタ 情報企画部 [担当:湯本]
〒244-0817 神奈川県横浜市戸塚区吉田町 292 番地
電話:050-3135-3409(直通)

以上