2014 年 6 月 5 日
株式会社日立製作所

マルウェアの挙動を多種多様な環境で解析できる マルウェア解析システムの試作に成功

標的型攻撃にも利用されるマルウェアを自組織内で解析可能に

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、このたび、標的型攻撃等のサイバー攻撃に悪用されるマルウェアの挙動を自動的に解析するマルウェア解析システムの試作に成功しました。本システムでは、外部に委託をすることなく自組織内で、OS やソフトウェアのバージョン等の異なる複数の実行環境下で、マルウェアの挙動解析を自動的に行えることに加えて、環境依存型のマルウェア*1 の挙動把握やマルウェアが影響を受ける環境の特定を容易に行うことが可能です。また、これまで高度な専門知識を有したマルウェア解析者が手作業で行ってきた一連の解析作業(動的解析、観測、挙動解析、レポート)を自動で行うことで、解析全体にかかる時間を 75%短縮*2します。

近年、特定の企業をターゲットとしてサイバー攻撃を行う標的型攻撃は、高度化、国家の機密保持、企業防衛の観点においても社会的な問題となっています。また、標的型攻撃に利用されるコンピュータウイルス、ワーム、スパイウェアなどの悪意あるソフトウェア(マルウェア)の組織への侵入を許してしまうケースが増えているため、マルウェアの挙動を解明して被害拡大防止策を講じる必要があります。

このような背景から、日立は、マルウェアを多種類の動的解析環境(OS やソフトウェアのバージョンが異なる被感染環境)で同時に実行させることにより、環境によって挙動が異なるマルウェアを自動的に解析するシステムを開発しました。今回試作したマルウェア解析システムに用いた主な技術は以下の通りです。

(1)多種動的解析環境の構築

環境によって挙動の異なるマルウェアを解析するため、複数種類の解析エンジン*3 や、動的解析環境を用いてマルウェア解析システムを構築しました。なお、動的解析環境の構築にあたっては、従来から培ってきたマルウェア解析ノウハウに基づいてマルウェアの攻撃傾向を分析し、攻撃を受けやすい環境を選定、構築しました。

(2)マルウェア特徴情報の抽出

マルウェア解析を業務として行っている専門家のマルウェア解析ノウハウ(暗黙知)を形式知化して挙動を解析するとともに、解析結果からマルウェア特有の挙動を抽出する技術を開発しました。本技術は、マルウェアが解析を逃れるために備えている隠匿機能や不審なネットワーク接続等のマルウェア特有の不正行動を抽出するもので、この技術を用いることで、容易にマルウェアの脅威を明ら

かにすることができます。

(3)外部のマルウェア解析サービスと連携

文書ファイル等の機密情報に寄生するマルウェアについては、マルウェアの解析作業を外部に委託しづらいという課題もありましたが、マルウェアが寄生する機密情報そのものを外部に提供することなく、外部のマルウェア解析サービスと連携することで、機密保護しながら解析の精度を高める技術を開発しました。

試作した本システムは、総務省実証事業「サイバー攻撃解析・防御モデル実践演習の実証実験の請負」におけるマルウェア解析の実証の成果を活用*4しています。

なお、本システムは、2014 年 6 月 11 日に東京コンベンションホールにて開催される「日立セキュリティソリューションセミナー」にて参考展示する予定です。今後は、株式会社日立アドバンストシステムズにより、2014 年度中の製品化に向けた開発を進めていきます。

*1 環境依存型のマルウェア:特定の OS や仮想環境でのみ動作するようにプログラムされたマルウェア。
*2 解析全体にかかる時間を 75%短縮:従来のマルウェア解析者の手作業による解析時間(1 時間)を 15 分に短縮。
*3 解析エンジン:マルウェアの挙動を解析する製品。
*4 マルウェア解析の実証の成果を活用:実証においては、OS やソフトウェアのバージョン等が異なる解析環境を 80 種類程度構築し、マルウェアの挙動を解析した結果、環境によって挙動が変化するマルウェアの存在を確認。

■照会先

株式会社日立製作所 研究開発本部 技術統括センタ [担当:吉田]
〒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