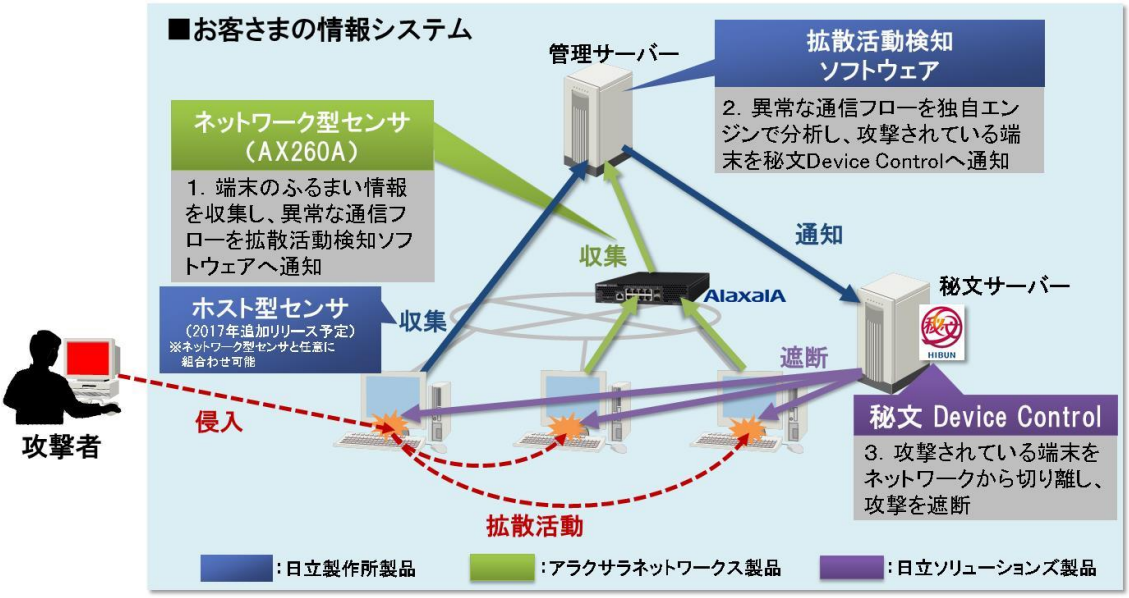
2016 年 6 月 6 日
株式会社日立製作所

情報システム内における標的型サイバー攻撃の拡散を検知するソリューションを販売開始



本ソリューションの概要イメージ

株式会社日立製作所(執行役社長兼 CEO:東原 敏昭／以下、日立)は、このたび、情報システム内における標的型サイバー攻撃の拡散を検知するソリューション（以下、本ソリューション）を 6 月 30 日から販売開始します。なお、販売開始に先立ち、6 月 7 日に開催する「日立セキュリティセミナー」にて、本ソリューションに関する講演および展示を行います。

本ソリューションは、情報システムへ侵入したマルウェアの標的型サイバー攻撃を自動で検知する、新たなサイバー攻撃対策ソリューションです。本ソリューションは、攻撃者のマルウェア*1 が起こす「不審なふるまい」と端末やサーバー装置を渡り歩く「拡散活動」という標的型サイバー攻撃の特徴を捉えるエンジンを備えることで、高い攻撃検知能力を実現しています。これにより、標的型サイバー攻撃対策の専門家がいない場合においても、侵入したマルウェアの標的型サイバー攻撃を検知し、攻撃者から大切な情報資産を守ることができます。

近年、社会問題となっている標的型サイバー攻撃による被害は増加の一途をたどっており、2015 年度における標的型サイバー攻撃の報告件数は 3,828 件にのぼり、前年度に比べ 2.2 倍（過去最多）となっています*2。こうした標的型サイバー攻撃に対処するためには、さまざまな検知手法のサイバー攻撃対策製品を組み合わせることで、多層的に情報システムを守ることが有効です。サイバー攻撃対策はマルウェアのシステムへの侵入を防ぐ入口対策、侵入した後に情報を探して端末やサー

バーを渡り歩く拡散活動への対策を行う内部対策、守りたい情報資産にアクセスされても実被害につながることを防ぐ出口対策の 3 つの対策から構成されます。
これまでは、主に入口・出口対策の製品開発が行われておりましたが、同時にそれらのセキュリティを回避する標的型サイバー攻撃が日々開発されていました。また、日々巧妙化する標的型サイバー攻撃を高い精度で検知し続けるためには、専門家による継続的なサイバー攻撃対策製品の運用ポリシーの見直しや製品のチューニングが求められるため、運用上大きな負担となっていました。

そこで日立は、システムの多層防御を強化する内部対策製品に着目し、専門家の継続的なメンテナンス作業を必要とせず、情報システム内に侵入したマルウェアの標的型サイバー攻撃を自動的に検知する拡散活動検知ソフトウェアを開発・提供することにしました。

具体的には、本ソリューションのソフトウェアを管理サーバーにインストールすることで、端末におけるマルウェアの拡散活動を検知します。本ソリューションのソフトウェアがインストールされると、「機械学習型エンジン」により、各端末の正常なふるまいを学習し、自動的にそのふるまいから逸脱する異常な端末を検出します。その後、「攻撃拡散分析エンジン」により、その異常なふるまいをする端末と通信する他の端末の動きを全体的に分析し、異常なふるまいが連動していないか確認します。
本ソリューションは、正常なふるまいを自動学習することにより、逸脱する異常な端末を判定するため、最新のマルウェア情報の入力や専門家によるチューニングなどを必要とせず、日々巧妙化する標的型サイバー攻撃への対応を可能にします。

なお、本ソリューションはアラクサラネットワークス株式会社(代表取締役社長　南川　育穂／以下、アラクサラネットワークス)が販売する、ホワイトリスト機能*3 を搭載した小型アプライアンス「AX260A」と連携します。「AX260A」は情報システム内の通信情報を収集し、異常な通信を拡散活動検知ソフトウェアへ通知するセンサーの役割を果たします。これにより、情報システム内の端末やサーバーに新たなソフトウェアなどをインストールしなくても標的型サイバー攻撃を検知できます。

また、本ソリューションは株式会社日立ソリューションズ（代表取締役　取締役社長：柴原　節男／以下、日立ソリューションズ）が販売する情報漏えい防止ソフトウェア「秘文 Device Control」とも連携します。「秘文 Device Control」は、拡散活動検知ソフトウェアの攻撃検知情報を元に端末をネットワークから切り離す、対処の役割を果たします。これにより、攻撃者が重要情報を持ち出す前に攻撃を頓挫させ、お客さまの大切な情報資産を守ります。

今後は、本ソリューションに関連したサイバー攻撃対策サービスを順次開発、提供する予定です。

■本ソリューションの主な特長

1.「機械学習型エンジン」と「攻撃拡散分析エンジン」により、情報システム内の拡散活動を検知

(1)　高い精度での攻撃検知率を実現

本ソリューションの「機械学習型エンジン」と「攻撃拡散分析エンジン」は、攻撃者が起こす異常なふるまいと拡散活動から標的型サイバー攻撃を自動で検知します。この 2 つのエンジン*4は、お客さまが情報システムを通常利用する際の通信情報などを自動的に学習して、攻撃を検知するための手がかりとします。これにより、最新のマルウェア情報を用いずに、巧妙な攻撃手法を用いた標的型サイバー攻撃などに対しても、高い精度での攻撃検知率を実現しています。*5

(2)　誤検知を抑えインシデント対処コストを低減

正常なユーザのふるまいとの差異を攻撃検知の根拠とすると、正常なユーザが普段と違う操作をした際も攻撃として検知してしまい、誤検知の対応に追われるという課題があります。この課題に対して、本ソリューションは拡散活動検知ソフトウェアの「攻撃拡散分析エンジン」によって複数端末の挙動を俯瞰して監視し、情報システム内部で標的型サイバー攻撃の拡散活動を行う際に見られる、複数端末での異常なふるまいの連鎖を分析することで、高い攻撃検知率を保ちつつ、誤検知率を単純なふるまい検知型製品の 1/10 に低減しています。*6

(3)　専門知識を必要としない運用を実現

本ソリューションは、拡散活動検知ソフトウェアの「機械学習型エンジン」と「攻撃拡散分析エンジン」による自動学習の成果に基づいて 標的型サイバー攻撃を検知するため、サイバー攻撃対策製品に必要な、複雑なパラメータ調整やルール設定を必要としない運用を実現しています。

2. 2 つの製品と連携してソリューションを提供

(1)　アラクサラネットワークス「AX260A」との連携による検知率向上

本ソリューションは、アラクサラネットワークス株式会社(代表取締役社長　南川　育穂／以下、アラクサラネットワークス)が販売する、ホワイトリスト機能を搭載した小型アプライアンス「AX260A」と連携します。「AX260A」は、ホワイトリストに登録されていない異常な通信フローを検出して拡散活動検知ソフトウェアへ送信するセンサーとしての役割を持ちます。これにより、情報システム内の端末にエージェントソフトウェアなどをインストールしなくても、標的型サイバー攻撃を検知できます。

(2)　日立ソリューションズ「秘文 Device Control」との連携による迅速な対処の実現

本ソリューションは、株式会社日立ソリューションズ（代表取締役 取締役社長: 柴原　節男／以下、日立ソリューションズ）が販売する情報漏えい防止ソフトウェア「秘文 Device Control」と連携します。「秘文 Device Control」は、拡散活動検知ソフトウェアからの検知情報を受信すると、攻撃の起点となっている端末をネットワークから切り離します。これにより、攻撃者が重要情報を持ち出す前に攻撃を頓挫させ、お客さまの大切な情報資産を守ります。

*1 マルウェア: 悪意をもったソフトウェア

*2 出典:警察庁発表資料「平成 27 年におけるサイバー空間をめぐる脅威の情勢について」
https://www.npa.go.jp/pressrelease/2016/03/20160317_01.html

*3 ホワイトリスト機能:ネットワーク上でやりとりされる通信を学習し、許可リストを自動で生成する機能。許可リスト生成後、運用状態に切り替えて、ネットワークにおけるすべての通信を監視。許可リストにない不正な通信をシャットアウトすることで、さまざまな攻撃からネットワークを効果的に保護することが可能。

*4:特許出願中　特願 P2014-195244「ウイルス検知システム及び方法」、特願 P2015-087821「サイバー攻撃分析装置及びサイバー攻撃分析方法」

*5*6:当社実証実験により、検知率 90%以上の成果を確認しています。

■提供開始時期

本製品の提供開始時期は、2016 年 6 月 30 日となります。

■日立セキュリティセミナーでの展示について

6 月 7 日(火)に東京コンベンションホール《 東京スクエアガーデン 5F 》において日立グループが提供するセキュリティ製品やサービスに関するセミナー「日立セキュリティセミナー」にて、本ソリューションに関する講演および展示を行います。

・セミナーサイト http://www.hitachi.co.jp/sss/

■関連情報

・「AX260A」に関するアラクサラネットワークスの Web サイト
http://www.alaxala.com/jp/news/press/2016/20160426.html

・「秘文 Device Control」に関する日立ソリューションズの Web サイト
http://www.hitachi-solutions.co.jp/hibun/sp/

■お客様お問い合わせ先

株式会社日立製作所 ディフェンスビジネスユニット
サイバーセキュリティソリューションに関するお問い合わせフォーム:
https://www8.hitachi.co.jp/inquiry/hitachi-ds/cybersecurity/form.jsp

以 上