※本リリースは、株式会社日立ソリューションズ、トレンドマイクロ株式会社から配信しております。
重複して配信される場合がございますが、あらかじめご了承下さい。

2016年7月26日
株式会社日立ソリューションズ
トレンドマイクロ株式会社

トレンドマイクロと日立ソリューションズがマルウェア感染拡大防止ソリューションで連携

入口・出口と内部ネットワーク監視でマルウェアを早期に検知し、感染端末の通信を自動遮断

株式会社日立ソリューションズ(本社:東京都品川区、取締役社長:柴原 節男／以下、日立ソリューションズ)は、トレンドマイクロ株式会社(本社:東京都渋谷区、代表取締役社長 兼 CEO:エバ・チェン／以下、トレンドマイクロ)と連携し、マルウェアの感染拡大を防止するソリューションを8月31日から提供開始します。

本ソリューションでは、トレンドマイクロの「Deep Discovery Inspector(以下、DDI)」を活用した入口・出口監視と内部ネットワークの監視でマルウェア感染端末を早期に検知し、日立ソリューションズの「秘文 Device Control」により感染端末の通信を自動遮断します。

これにより、企業は、マルウェア感染拡大を防止するとともに、システム管理者は、通信遮断後も感染端末を遠隔操作して、状況確認や遮断解除などを行えるため、運用負荷を軽減できます。

■背景

昨今、標的型攻撃が巧妙化する中、マルウェア感染を想定した多層防御が求められており、ネットワークの入口・出口監視に加え、侵入したマルウェアを早期に発見して被害拡大を防止する内部ネットワーク監視が重要となっています。また、システム管理者は標的型攻撃の事後対応として、マルウェアの駆除以外に、被害状況の調査・報告や再侵入防止などさまざまな作業が必要であり、その運用負荷も課題となっています。

■ソリューションの概要

1. ネットワークの入口・出口監視と内部ネットワーク監視により、侵入したマルウェアを早期に検知

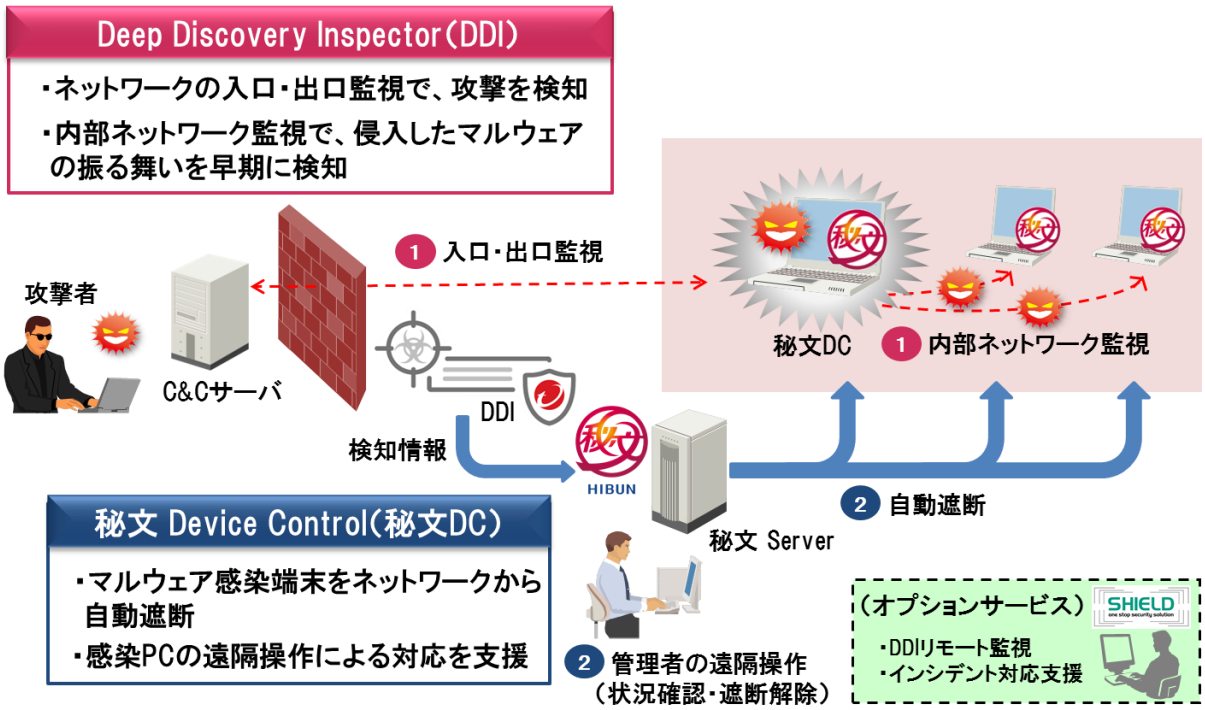
本ソリューションでは、ネットワークの入口・出口に加え、内部ネットワークを監視することで、マルウェアの早期検知を実現します。入口・出口監視では、サンドボックス※1のみならず、パターンやルールに基づいた通信の振舞いから、標的型攻撃やゼロデイ攻撃、マルウェアによるC&Cサーバー※2への通信などを検出します。さらに、内部ネットワーク監視では、他の端末への拡散、データベースや各種サーバーへの不正な通信を検知し、感染した端末を特定することができます。

※1 保護された領域内でプログラムを動作させ実際の振る舞いを見ることで不正プログラムを検知する仕組み

※2 コマンド&コントロールサーバーの略で、マルウェアに攻撃の指令を出したり、窃取データを収集するサーバー

2. マルウェア感染端末をネットワークから自動遮断することでマルウェアの感染拡大を防止

DDIで検知した感染端末の情報を基に、「秘文 Device Control」が感染端末側で通信を自動遮断します。さらに、画面にメッセージを表示して、マルウェアに感染したことや、遮断した後の対応手順などを端末利用者に通知します。また、システム管理者は、通信を遮断した後も感染端末を遠隔操作して、状況確認や遮断解除などを行うことができます。



■構成する製品

「Deep Discovery Inspector」、「秘文 Server」、「秘文 Device Control」

※別途 Syslog サーバー製品が必要です。

■オプションサービス(日立システムズ提供)

・DDI リモート監視(SHIELD セキュリティデバイス監視サービス)

日立システムズの「SHIELD SOC(Security Operation Center)」から、お客様サイトの DDI を 24 時間 365 日、監視・運用するアウトソーシングサービスです。

・セキュリティインシデント対応支援(SHIELD クラウド CSIRT サービス)

セキュリティに精通したアナリストが、発生したセキュリティインシデントの内容を分析し、情報提供することで、インシデント発生後のシステム管理者の対応判断を支援します。

「SHIELD」:https://www.hitachi-systems.com/solution/t01/shield/

■提供価格

個別見積

■トレンドマイクロの「Deep Discovery Inspector」について

標的型攻撃やゼロデイ攻撃を、ネットワーク上の振舞いから見つけ出し、早期に対処し被害の深刻化を抑止するための対策製品です。攻撃の初期段階から内部の拡散、外部への通信に至るあらゆる段階において、不正なファイルや通信の検知に加え、管理ツールを悪用した攻撃までの早期発見、早期対処を支援します。

「Deep Discovery Inspector」:http://www.go-tm.jp/ddi

■日立ソリューションズの「秘文 Device Control」について

PC につながるさまざまなデバイスの利用を禁止することで、データの不正コピーを防止します。また、接続先ネットワークを制限することで、安全なネットワーク利用環境でのみ、PC を使用させることができます。企業から機密情報を「出さない」情報漏洩対策を実現します。

「秘文」シリーズは、これまでに 7,600 社、790 万ライセンス（2016 年 3 月末時点）の導入実績があり、持出制御ソフトウェアで国内シェア No.1※3 の製品です。

「秘文 Device Control」：http://www.hitachi-solutions.co.jp/hibun/sp/product/dc/

※3　出典：「2015 ネットワークセキュリティビジネス調査総覧」株式会社富士キメラ総研（2014 年度金額ベース）
端末管理・セキュリティツール分野（持出制御ソフトウェア、暗号化ソフトウェア）にて国内シェア No.1

■商品・サービスに関するお問い合わせ先

日立ソリューションズ ホームページ：https://www.hitachi-solutions.co.jp/inquiry/　Tel：0120-571-488

■報道機関からのお問い合わせ先

株式会社日立ソリューションズ
担当部署:　経営企画本部 広報・宣伝部
担当者:　竹谷、安藤
Tel：03-5479-5013　Fax：03-5780-6455　E-mail：koho@hitachi-solutions.com

日立ソリューションズ グループは、お客様の業務ライフサイクルにわたり、豊富なソリューションを全体最適の視点で組み合わせ、ワンストップで提供する「ハイブリッドインテグレーション」を実現します。

※　TREND MICRO、 Deep Discovery Inspector、および、Deep Discovery は、トレンドマイクロ株式会社の登録商標です。
※　秘文、ハイブリッドインテグレーションは、株式会社日立ソリューションズの登録商標です。
※　SHIELDは、株式会社日立システムズの登録商標です。
※　その他記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

このニュースリリース記載の情報(製品価格、製品仕様、サービスの内容、発売日、お問い合わせ先、URL等)は、発表日現在の情報です。予告なしに変更され、検索日と情報が異なる可能性もありますので、あらかじめご了承ください。
