2014 年 6 月 17 日

キヤノン電子、クルウィット社「SiteVisor」との機能連携ソリューションをリリース

～ サイバー攻撃をリアルタイムに可視化、マルウェア感染の検知から感染経路の特定、駆除まで、事後対策を自動化 ～

キヤノン電子株式会社（本社：東京都港区芝公園 3-5-10、代表取締役社長：酒巻久、以下「キヤノン電子」）は、標的型攻撃から企業の情報資産を守る Windows 用セキュリティソフト「SML セキュリティスイート with SiteVisor」をリリース致します。

キヤノン電子ではセキュリティソフトウェア「SML(Security Management with Logging)」を開発・販売し、企業内部からの情報漏えいだけでなく、サイバー攻撃から企業の情報資産を守る製品・サービスをお客様にご提供して参りました。この度、SML と株式会社クルウィット（本社：東京都三鷹市下連雀 3-34-8、代表取締役社長：国峯 泰裕）の「SiteVisor」を機能連携させ、マルウェアによる不正なダークネット※1 通信をリアルタイムに可視化することでマルウェア感染を検知し、かつマルウェアプログラム自体の検出、及びマルウェアの感染経路を特定する機能を備えた、マルウェア監視・感染事後対策ソリューションの提供を開始致します。

※1 ダークネット：インターネット上で到達可能かつ未使用の IP アドレス空間。

■ 背景

サイバー攻撃の猛威は拡大の一途をたどっており、巧妙化する攻撃手法から企業資産を守るには、新しい防御手段が必要となってきています。キヤノン電子では、2013 年に「SML セキュリティスイート」をリリースし、ホワイトリスト方式のプログラム・通信制御機能や外部アンチウィルスソフトと連携したマルウェア感染経路特定機能を提供して参りました。また、株式会社クルウィットでは、独立行政法人情報通信研究機構（NICT）が研究開発した対サイバー攻撃アラートシステム"DAEDALUS" を商用化した「SiteVisor」を販売し、従来とは全く考え方の異なる、新しい視点でマルウェアを検知、可視化するシステムを提供して参りました。

この度、「SML セキュリティスイート with SiteVisor」では SML と SiteVisor を機能連携させる事で、より広範囲のマルウェアの感染活動を検知し、企業内部のダークネットの発信元を特定、更に発信元の侵入経路を特定するという、新しい価値をお客様にご提供致します。

■ 機能連携の仕組み

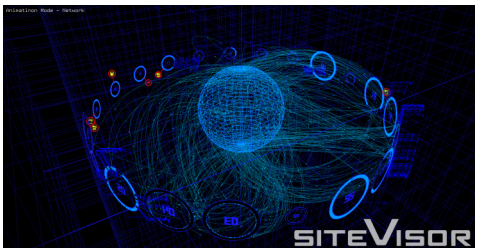
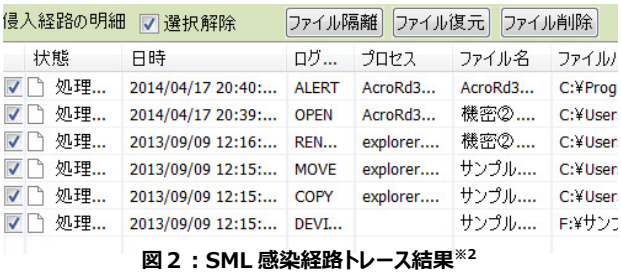


図 1 ：SiteVisor 可視化システム画面

組織内に設置した SiteVisor のダークネットセンサが不正な通信を検知すると、検知情報を SML 管理サーバへリアルタイムに通知します。SML 管理サーバではコンピュータ端末のシステム情報、操作履歴などが集中管理されており、これらの情報を元に不正通信の発信元である端末を特定します。

端末を特定すると、端末の操作履歴（ログ）が分析され、不正な通信を発生させていたプログラムが特定されます。更に、元凶となっているプログラムが、いつ、どこから、どのように侵入してきたか経路をバックトレースし、感染源を特定し、かつ、検出された不正プログラムが社内ネットワークの他の端末に拡散していないかフォーワードトレースし、感染状況を即時に把握する事ができます。また、これらの分析結果はレポートにより一覧で確認する事ができます。


侵入経路の明細　選択解除　ファイル隔離　ファイル復元　ファイル削除

状態	日時	ログ...	プロセス	ファイル名	ファイル/
処理...	2014/04/17 20:40:...	ALERT	AcroRd3...	AcroRd3...	C:¥Prog
処理...	2014/04/17 20:39:...	OPEN	AcroRd3...	機密②....	C:¥User
処理...	2013/09/09 12:16:...	REN...	explorer....	機密②....	C:¥User
処理...	2013/09/09 12:15:...	MOVE	explorer....	サンプル....	C:¥User
処理...	2013/09/09 12:15:...	COPY	explorer....	サンプル....	C:¥User
処理...	2013/09/09 12:15:...	DEVI...		サンプル....	F:¥サン

図 2 ：SML 感染経路トレース結果※2

※2 ：画面は開発中のものです。予告なく変更となる場合があります

■ SML セキュリティスイートについて

「SML セキュリティスイート」は操作ログ記録、デバイス制御、PC 利用時間制御など内部漏洩防止機能に加え、「ホワイトリスト方式のコンピュータ制御機能」により許可されたアプリケーションや通信操作だけを可能にし、未知のマルウェアや許可されていないアプリケーションの実行を標準で禁止します。ホワイトリスト機能の特長として、システム更新やセキュリティパッチ適用など必要な構成変化を自動で判別しホワイトリストを生成する「ホワイトリスト自動生成機能」を備えており、システム管理者様の運用コストを大きく低減致します。

【主な機能一覧】

- Windows PC の操作ログ記録
- アプリケーションの起動制限（ブラックリスト方式、ホワイトリスト方式）
- アウトバウンドの通信制限（ホワイトリスト方式）
- ウェブの閲覧制限（ブラックリスト方式、ホワイトリスト方式）
- USB メモリなどのデバイス使用制限
- PC の利用時間制限

■ SiteVisor について

SiteVisor は、独立行政法人情報通信研究機構 （NICT）が研究開発した、対サイバー攻撃アラートシステム “DAEDALUS”（ダイダロス）を株式会社クルウィットが技術移転を受け、商用化したサービスです。インターネット上で到達可能かつ未使用の IP アドレス空間「ダークネット」を観測し、マルウェアの不正な活動状況をリアルタイムに可視化し、セキュリティリスクを把握します。

【サービス一覧】

- SiteVisor External (外部監視モデル ※ダークネットセンサ及び可視化の提供はありません)
- SiteVisor DMZ (内部/外部監視モデル)
- SiteVisor Private (内部監視モデル)
- SiteVisor Ultimate (全方位監視モデル)

【株式会社クルウィットについて】

株式会社クルウィットでは、世界中の人々を繋ぐ『インターネットサービス事業』と「安心・安全・安定・信頼」を担保する『情報セキュリティ事業』をお客様にご提供致します。

会社名 ： 株式会社クルウィット（clwit, Inc.）
所在地 ： 〒181-0013 東京都三鷹市下連雀 3-34-8 三鷹ハイデンス 509 号
代表者 ： 代表取締役 国峯 泰裕
設立 ： 2000 年 10 月6 日
資本金 ： 10,000,000 円
事業内容： インターネットサービス事業、情報セキュリティ事業
URL ： http://www.clwit.co.jp/

▼本件に関するお問い合せ先
キヤノン電子株式会社 LM 事業部 LM 営業課 担当：池田 祐一
TEL ： 03-6910-4125
FAX ： 03-5472-7671
Mail ： 「セキュリティ：ログマネジメント」よりご記入ください。
→お問い合せフォーム（お問い合せ個人情報取り扱い要旨）