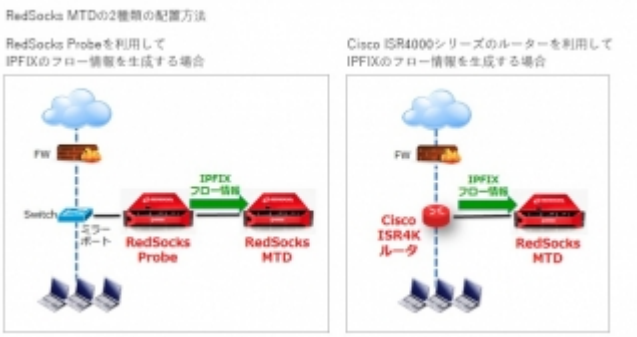
次世代の出口対策製品「RedSocks MTD」の新版をリリース



端末視点のアラート解析画面を追加し、長期間に遡ってフローデータ確認が可能に

RedSocks本社の製品責任者が来日し、導入後の運用やアラート解析方法を
レクチャーする「RedSocks実践セミナー」を9月29日 に開催

ITインフラのソリューション・ディストリビューターである株式会社ネットワールド（本社：東京都千代田区、代表取締役社長 森田
晶一）はRedSocks社（本社：オランダ）の標的型攻撃の出口対策製品の最新版「RedSocks Malicious Threat Detection （以下、RedSocks MTD）3.5」を発表し、本日9月13日
より提供開始します。

サンドボックス技術を利用しても、入口や内部での未知のマルウェアの侵入や感染の検知、出口でのC&Cサーバーなど悪意あるサイトへの通信の検知は限定的で、100%防ぐことは難しい時代です。
「RedSocks
MTD」は、全てのインターネットへの通信から、RedSocks社の高度なブラックリストとヒューリスティック検知により、リアルタイムに悪意あるサイトへの通信の検知が可能です。「RedSocks MTD」は、通常のWebレピュテーションでは検知が難しい、日々ランダムに通信先のドメイン名を生成し変更される「Domain Generation
Algorithm（DGA）」を利用したマルウェアのC&Cサーバーへの通信の検知や、サンドボックスでは検知が難しい、インターネット上に公開されている公開プロキシーサーバーや国内も含め世界中のハッキングされたサイトへの通信の検知も可能です。

最新版の「RedSocks MTD 3.5」では、従来からの特長はそのままに、新しくアラート解析（Alert Analysis）画面や脅威の多い端末を特定する機能が追加され、各種UIを追加・強化しています。また、日本市場からの要望であったCisco ISR4000シリーズのルーターにも対応しています。

ネットワールドでは、「RedSocks MTD」の導入検討が増えており、導入後の運用やSOC（Security Operation
Center：セキュリティオペレーションセンター）へのご質問の増加を受けて、RedSocks本社から製品・開発の責任者（Product Manager）を招き、最新版「RedSocks MTD
3.5」をベースに、「RedSocks MTD」で検知したアラートからの解析方法を中心に、

9月29日（木） に「RedSocks 実践セミナー」を開催いたします。

◆ 最新版「RedSocks MTD 3.5」の新しい機能・特長

1. より長期に、過去に遡ってのフローデータ解析：
「RedSocks MTD」で検知したアラートの内、Thread level 1（脅威レベル1）のアラートは赤くハイライト表示され、メールにより通知されます。RedSocks社の高度なブラックリストによりURLマッチングした通信については、ホスト名とURLも表示されます。
「RedSocks MTD」のアラート発生時に、旧バージョン「RedSocks MTD 3.4」では、アラート発生前15分間のフローデータをGUIで確認したり、CSVで出力し、解析が可能でした。新版の「RedSocks MTD 3.5」では、さらに長期間（約3か月程度）遡って、フローデータの確認が可能になりました。
また、新たに設けられたData Protection Officer（DPO）権限の管理者は、任意の期間を設定して、フローデータの出力や解析も可能です。出力したフローデータには、TCPフラグの情報も含まれています。

2. 端末視点のアラート解析画面の追加：
新版の3.5では、新たにアラート解析（Alert Analysis）画面が追加されました。ソース元のIPアドレスごとに、過去発生したアラートのThread level（脅威レベル）やアラート数、アラートの詳細が確認できます。クライアント端末視点で脅威が可視化できるため、該当の端末へのピンポイントでの対策の実施により、セキュリティ強化やコンプライアンス強化に役立ちます。

3. 脅威の多い端末ランキングの追加：
アラート解析（Alert Analysis）画面では、脅威の検出が多い順にソースIPがリスト表示されます。また、IPアドレス（IPv4）またはMacアドレスごとに登録できるエイリアス名（別名）を利用し、判読性を高めることが可能です。

4. Cisco ISR4000シリーズのルーターへの対応：
「RedSocks MTD」は、「リアルタイム検知」、「端末の制限無し（端末のOSは問わない）」、「完全プライバシー保護（データや検体を外部に出す必要は一切無し）」を実現するため、インターネットへの全通信のIPFIXのフローデータを監視、解析する仕組みです。
インターネットの出口に配置されたスイッチやルーターのミラーポートから、キャプチャーしたパケットをIPFIXのフローデータに変換するために「RedSocks Probe」が必要です。最新版の「RedSocks MTD 3.5」では、Cisco ISR4000シリーズのルーターに対応しました。これにより、「RedSocks Probe」無しで、直接Cisco ISR4000シリーズが生成するIPFIXフローデータを「RedSocks MTD」が認識し、監視、解析できるようになりました。

Cisco ISR4000シリーズのルーターはインラインに配備するため、ネットワールドでは、「RedSocks MTD」でThread level 1（脅威レベル1）のアラートを検知した際に、コマンドを実行し、自動遮断するプログラムを開

発し、自動遮断までできるソリューションの提供を予定しています。

◆「RedSocks 実践セミナー」開催概要

◇主 催： 株式会社ネットワールド / 協 賛： RedSocks社
◇日 程： 2016年9月29日（木） 14：30～17：30（受付開始 14：15）
◇会 場： 株式会社ネットワールド 8階 会議室
◇定 員： 20名
◇対 象： SOCパートナー様、パートナー様のネットワーク＆セキュリティエンジニア
◇アジェンダ：1. RedSocks 会社紹介、ラボ紹介、製品紹介
2. RedSocks 導入方法、管理方法
3. RedSocks Security Analytics （解析方法）
4. Q&A 30分程度
※3. がメインのセッションで、1.5～2時間程度を予定しております。
※全セッションに逐次通訳が付きます。

◇申 込：メールにてお申込。メールアドレス＜ redsocks-info@networld.co.jp ＞宛に、RedSocksセミナー申込希望として以下をご連絡下さい。
（必要情報：会社名・部署・お名前・メールアドレス）
