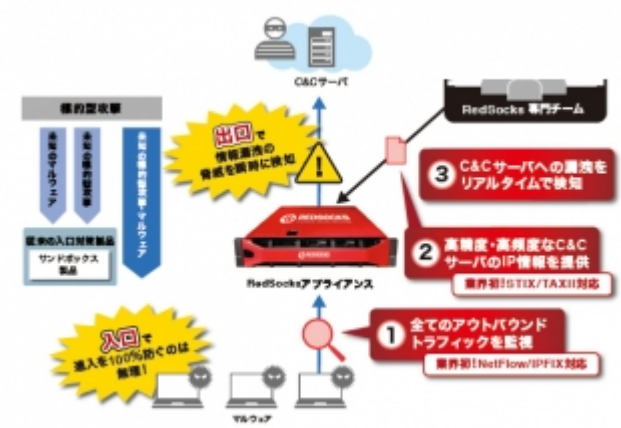
次世代標的型攻撃対策のオランダRedSocks社と国内初のディストリビューター契約を締結



NetFlow /
IPFIXで全アウトバウンド・トラフィックを監視してリアルタイムに検知可能な「RedSocks Malware Threat Defender」を販売開始

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、標的型攻撃・マルウェア対策研究の先進国であるオランダに本社を構えるRedSocks（レッドソックス）社と日本で初めてディストリビューター契約を締結し、次世代標的型攻撃対策製品「RedSocks Malware Threat Defender」（以下、RedSocks MTD）を、本日7月16日
より販売開始します。

RedSocks社のハードウェアアプライアンス「RedSocks
MTD」製品は、全てのアウトバウンド・トラフィック（企業や組織からインターネットへの通信）を監視し、標的型攻撃による情報漏洩の危機となる通信を、リアルタイムに、検知・通知可能な製品です。
また、サイバー攻撃に関する情報共有や交換のため策定された技術仕様STIX /
TAXII(※注1)にも近々対応予定で、同じく対応する他社ファイアウォール製品などと連携し、リアルタイムに、検知と同時に、自動遮断までするソリューションも実現予定です。

ネットワールドは、今回の発表に先立ち、高精度・高鮮度な情報によるリアルタイムの検知、完全なプライバシー保護、低負荷の仕組みなどのRedSocks社ならびにRedSocks
MTD製品の優位性にご賛同いただいた、国内の複数社のお客様において既にPOC
（概念実証）を開始しておりますが、今後さらに多くのお客様へのご販売、ISP /
MSP事業者様、セキュリティ企業様でのサービスでの利用を積極的に展開してまいります。

◆ 次世代の標的型攻撃対策とは

従来のシグネチャベースのセキュリティ対策では、標的型攻撃や未知のマルウェアを検知するの

が難しいことは周知の事実です。さらに、多くの標的型攻撃対策製品で利用されている「サンドボックス」（仮想マシンベースのマルウェアを実行し解析するシステム）で実行されていることも認識し、すり抜ける高度なマルウェアも登場しています。
今後も巧妙化し続ける攻撃やマルウェアに対し、未知のマルウェアの侵入や感染を100％防御することは難しくなっており、侵入や感染はあることを前提として、如何に早く、標的型攻撃による情報漏洩や詐取の危機を発見し、被害拡大を最小限にできるかが対策の鍵となります。
国土の4分の1が海抜
0m以下のオランダは、サイバー攻撃により万一ポンプ停止が起こると、経済に大打撃を受けることや、首都アムステルダムがインターネット国際回路集積都市（ハブ）でもあることから、標的型攻撃・マルウェア対策研究が非常に進んだ国でもあります。そのようなオランダで、2012年に創立したRedSocks社には、「Cuckoo
Sandbox」の開発者や、サイバー攻撃に関する情報共有のため策定された技術仕様であるTAXIIの策定メンバーなど著名人が多く集結し、マルウェアが今後どんなに進化しても対応可能な次世代の標的型対策の開発と検知精度の向上に取り組んできました。「RedSocks
MTD」は、インターネットへの出口（アウトバウンド）でリアルタイムに、情報が詐取される通信を正確に発見することをコンセプトに開発されたユニークな製品です。

◆「RedSocks Malware Threat Defender （RedSocks MTD）」について

◇ 検知の仕組み

「RedSocks
MTD」アプライアンスを、インターネットへの出口であるファイアウォールやルーターなどのミラーポートに接続し、NetFlow / IPFIX
(※注2)により、全てのアウトバウンドのパケットの中から必要なフロー情報（送信先のIPアドレスやURL、デバイスの送信元IPアドレス、MACアドレス、ポート番号、プロトコル）を抽出して保有します。
この情報を、RedSocks社が擁するエキスパートチーム「The Malware Intelligent
Team」(以下、MIT)」から、30分に1回の高頻度で送られてくる信頼性の高いC&Cサーバ(※注3)の情報と照合（マッチング）して、マルウェアによるC&Cサーバへの通信をリアルタイムに検知して、管理者に即時に通知 します。
感染した端末の特定、マルウェアの種類、送信先のIPアドレスやURLの早期把握が可能で、社内のコンピュータセキュリティインシデント対応チームCSIRT（シーサート）やSOC（セキュリティ・オペレーションセンター）サービスの早期対応と、情報漏洩の被害拡大の最小限化に有効です。

◇ 特長

（1）高精度な情報、高頻度の更新
24時間365日稼動のRedSocks社のエキスパートチームMITは、ラボ内で、膨大なリストの精査と、膨大な数の未知のマルウェアを、サンドボックスだけでなく、ベアメタル（物理環境）でも綿密な検証をしています。こうして抽出した、世界中のC&CサーバのIPアドレス /
URLや攻撃者に関する高精度な最新リストや情報が、お客様のサイトに設置された「RedSocks
MTD」アプライアンスに30分に1回の高頻度で送られます。
ちなみに、RedSocks社のMITは、昨今の標的型攻撃で話題の「Emdivi」と呼ばれるマルウェアやその亜種で使われた /
使われている、海外はもちろん日本国内に設置されたC&CサーバのIPおよびURL情報も数多く発見しています。

この情報には、マルウェアが自体の通信を偽装するために利用する、インターネット上の公開プロキシサーバや、マルウェアがIP
情報を得るために利用するインターネット上で公開されているIP
チェックサイトの情報なども含まれ、情報漏洩や詐取の動きをより早い段階で検知することも可能です。
現在は、30分に1回の頻度でRedSocks社のMITから最新情報が送られて、「RedSocks
MTD」での検知力、リアルタイム性を最大化していますが、年内には20分に1回とさらに早くなる予定です。

（2）低負荷で高速に検知
アウトバウンド・トラフィックの情報はミラーポートから受け取るので、「RedSocks
MTD」アプライアンス内を通信が経由するわけではなく、また、NetFlow / IPFIX
により必要なフロー情報だけを抽出する仕組みのため、使用する帯域は1%程度で、通常の通信への負荷や影響は一切ありません。また、既存のネットワーク環境の設定を変更する必要もありません。
さらに、「RedSocks
MTD」アプライアンス内では、IPアドレスやURLの照合（マッチング）だけで、通信を解析する必要がないため、高速なリアルタイム検知が可能です。マッチングの他に、ヒューリスティック検知（挙動検知）も行っていますが、これらの検知手法のCPU負荷は少なく、通信のフロー数の制限もありません。複雑なサイジング等も不要で、同じ1種類のハードウェアアプライアンスで、大規模から中小規模のお客様、ならびにサービスプロバイダー様のニーズにも対応可能です。

（3）完全プライバシー保護
「RedSocks
MTD」アプライアンスは、サンドボックスを搭載するタイプの製品と異なり、RedSocks社のMITから情報を受け取るだけで、お客様の機密情報を含む検体や情報を外部（メーカー等）へ提供する必要は一切ありません。また、NetFlow /
IPFIX対応により、パケットの中身を一切見ないので、プライバシーや機密情報を出したくないというご要望の強い日本のお客様にも安心してご利用いただけます。

（4）100 %オランダ製
RedSocks社は100%オランダの企業であり、米国家安全保障局（NSA）
がバックドアを製品に設置しているといった疑念も一切ありません。「RedSocks
MTD」の仕様では、お客様の機密情報を含む検体や情報を外部
（メーカー等）に出す必要は一切ありませんが、米パトリオット法（米国愛国法）の下、捜査令状によりお客様のプライバシー情報が捜査対象として提出されるといったリスクも無く、安心してご利用いただけます。

◆ 「RedSocks Malware Threat Defender」の販売について

◇ 販売 / 出荷開始：2015年7月16日
◇ 販売経路：ネットワールド販売パートナー様経由
◇ 参考定価（帯域幅により、金額が異なります）

150Mbpsまでの場合：
アプライアンス + 初年度サブスクリプション： 4,230,000円（税別）
次年度サブスクリプション： 1,395,000円（税別）

※250Mbps、1Gbps、10Gbpsにつきましてはお問い合わせ下さい。
※別途、ヘルプデスクやハードウェア保守メニューもご用意しております。

[※注釈]……
（1）STIX / TAXII
STIX（Structured Threat Information eXpression）： 脅威情報構造化記述形式
サイバー攻撃活動に関連する項目を記述するため標準化された技術仕様。
http://stix.mitre.org/
TAXII（Trusted Automated eXchange of Indicator Information）： 検知指標情報自動交換手順
サイバー攻撃活動に関連する脅威情報を交換するため標準化された技術仕様。
http://taxii.mitre.org/
（2） NetFlow / IPFIX
NetFlowは、シスコシステムズによって開発された、IPトラフィック情報を収集するためのネットワーク・プロトコルで、トラフィック監視のデファクトスタンダードとなり、様々なプラットフォームで使用されている。IPFIX（Internet Protocol Flow Information Export)は、NetFlow v9をベースに、標準化組織であるIETFが標準化したもの。
（3）C&Cサーバ
C&C（コマンド＆コントロール）
サーバとは、外部から侵入して乗っ取ったコンピュータを利用したサイバー攻撃で、踏み台のコンピュータを制御したり命令を出したりする役割を担うサーバコンピュータのこと。サイバー攻撃では、同時に多数のコンピュータから攻撃させたり、攻撃元を割り出しにくくするなどの目的で、しばしば無関係な第三者のコンピュータをウイルスに感染させるなどして乗っ取り、攻撃に利用することがある。その際、侵入したコンピュータを操作したり、攻撃の指示を出したりするメッセージを発信するコンピュータのことをC&Cサーバという。（出典：IT用語辞典 e-Words）

……
◆今回の発表に関してエンドースをいただいております。

◇ グローバルセキュリティエキスパート株式会社 取締役常務 辻 誠 様
標的型メール訓練サービス、マルウェア感染調査や緊急対応サービスをはじめとする新しい脅威に対抗するサービス／ソリューションをご提案するサイバーセキュリティサービスラインナップを持つGSXは、ネットワールド社による「RedSocksMalware Threat Defender」の製品リリースを心より歓迎申し上げます。昨今、益々標的型攻撃への対策が急務となっている企業にとって、リアルタイム性を持った情報漏洩危機を検知できる”次世代型”（非サンドボックス型）標的型攻撃対策製品が有効なサイバーセキュリティソリューションとなることを期待するとともに、ネットワールド社のセキュリティビジネスをご支援します。

◇ オリゾンシステムズ株式会社 取締役社長 水口 俊一 様
この度は「RedSocks Malware Threat Defender」製品の発売おめでとうございます。同じくネットワークセキュリティソリューションに携わっております弊社としても、かような製品環境が整うことは大変に喜ばしいことと存じます。また、RedSocks MTDは弊社主力製品でございますFlowMon（ネットワークトラフィック可視化、監視、振る舞い検知）と同じく、NetFlow/IPFIXデータ技術をベースにした製品であり、FlowMonのProbe機能との連携に大きな効力を生む製品となっております。
昨今のデータ流出事故の多くは、マルウェアと呼ばれる悪意あるウィルスソフトが原因となっております。Advanced Cyber

Threatと呼ばれ、より進化したこれらの攻撃手法は従来のセキュリティ基準では防ぎきれていません。RedSocks
MTDのリリースにより本分野でのパートがさらに強化され、弊社製品ともどもソリューション提案においても有力な製品のひとつになると考えております。大いに期待しております。
……

Generated by ぷれりりプレスリリース
https://www.prerele.com