セキュリティ対策をすり抜ける攻撃！

隠れた脅威を見つけ出すスレットハンティングとは?

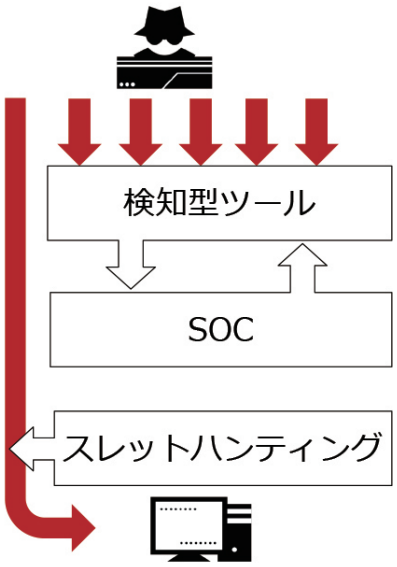
昨今、サイバー攻撃が高度化･巧妙化するなか、基本的なセキュリティ製品を導入している企業であっても、マルウェアに侵害される事例が頻繁に報道されている。このように、セキュリティ製品任せでは脅威から身を守ることができなくなっている現状を受けて、新たな対策のアプローチとして提唱されているのが「スレットハンティング」である。

スレットハンティングとは、その名のとおり、スレット（脅威）をハンティング（狩る）するものであり、アンチウイルスやファイアウォールなど既存のセキュリティを回避して侵入してくる脅威を可視化するための分析手法のことを言う。既存のセキュリティとは役割が異なることから、どちらか片方だけ導入すればよいというものではない点に注意が必要だ。たとえるならば、既存のセキュリティは建物の扉の鍵に該当し、これに対してスレットハンティングは屋内に配備された警備員に該当すると言えるだろう。施錠された扉で資産を保護したうえで、それらを破ってまでも侵入してくる不審者を警戒することで、よりセキュリティを盤石なものとするのである。

国内でもいち早く「スレットハンティングサービス」の提供を開始したのが、幅広いセキュリティ製品・サービスを展開するキヤノンマーケティングジャパン（以下キヤノンMJ）である。そこで本稿では、同社においてスレットハンティングサービスの商品企画を担当する、キヤノンマーケティングジャパン株式会社 セキュリティソリューション商品企画部 衣川瑠美子氏に、スレットハンティングを企業が実施する必要性や、スレットハンティングを実現するキヤノンMJのソリューションについて話を聞いた。

キヤノンマーケティングジャパン株式会社
セキュリティソリューション商品企画部
衣川瑠美子氏

既存セキュリティとの違い



IPSやUTMのようなツールの目的は
自動的に脅威を検知・駆除・遮断すること

SOCの目的はセキュリティツールが出す
大量のアラートから真の脅威を識別し対応すること

スレットハンティングの目的は
アラートが上がらない隠れた脅威を発見すること

技術面、法制面の双方から高まるスレットハンティングの必要性

――いまどうして「スレットハンティング」の必要性が高まっているのでしょうか。

衣川氏：大きくわけて、技術的な要素と法的な要素という2つの背景があると考えています。

まず、技術的な要素として挙げられるのが、サイバー攻撃が高度化・広範化している点です。これまでは「うちには関係ない話」「スパイ映画の世界でしょ」といった企業も多かったのではないかと想像します。しかしながら、いまや日常生活を含めたあらゆる行動がデジタル化し、多くの人が攻撃者との接点を持ってしまっています。また、攻撃手法が高度化していることにより企業を狙ったサイバー攻撃を従来の検知技術で見つけることが困難になっています。

実際にキヤノンMJグループが提供しているスレットハンティングの現場でも、UTM、メールセキュリティ、端末アンチウイルス、Webセキュリティのすべての防御壁をすり抜けて侵入を許してしまったという通信を検知していますし、大手自動車メーカーや電機メーカーの被害事例から同様のことが生じていると推測しています。攻撃者は攻撃対象が防御していることを織り込み済みで、検知されないようにOS標準機能を使用した攻撃を展開したり、端末に保存せずにメモリ上でロードして検知の目をかいくぐったり、といった手段を使ってくるのです。これらの最新の具体的な攻撃手法や実際の検知方法の詳細については、当社グループの上級アナリストが解説するウェビナー動画※を公開していますのでぜひご確認ください。

そしてもう1つの背景となる法的な要素としては、2020年6月に公布され2022年の施行が予定されている個人情報保護法の改正が挙げられます。今回の改正によって、事業者の責務として、個人情報漏えい時には本人への通知と個人情報保護委員会への報告義務が新たに追加されました。また、罰則が強化され、個人情報保護委員会への命令違反や虚偽報告を行った場合に法人に適用される罰金の最高額が1億円以下と高額になりました。

個人情報を取り扱う企業にとっては、その扱いについていま一度セキュリティを強化するとともに、有事の際にはすぐに状況を把握できる環境を整えることが重要になってきます。

――いわゆる「EDR」との違いはどこにあるのでしょうか。

衣川氏：端末から得られる情報をもとに検知を行うのがEDRで、そのデータソースは一般的にはクライアント端末に設定したエージェントになります。実際にはプロセスの挙動などのイベントを解析するのですが、そうすると、プロセスに起こった変化を検知するので、タイミングとしては侵害が発生したあとの検知となります。また、EDRだけではカバーしきれない脅威の存在や、エージェントを入れることができず、対応ができないといった現実もあります。

それに対して、当社グループのスレットハンティングはネットワークを分析対象としています。EDRは現時点で受けている攻撃に深くフォーカスするのに対し、ネットワーク分析では時系列に沿って一連の流れを広範囲で見て、脅威のきっかけを捉えます。

クライアント端末の挙動に対する検知に強いEDRと、エージェントレスで感染前の検知が可能なNDR（Network Detection and Response）領域であるスレットハンティングは、検知においてそれぞれ異なる強みを持っているという点から“双璧”と言えるかもしれません。

特許技術による際立った高速性が脅威の早期発見・早期対応を可能に

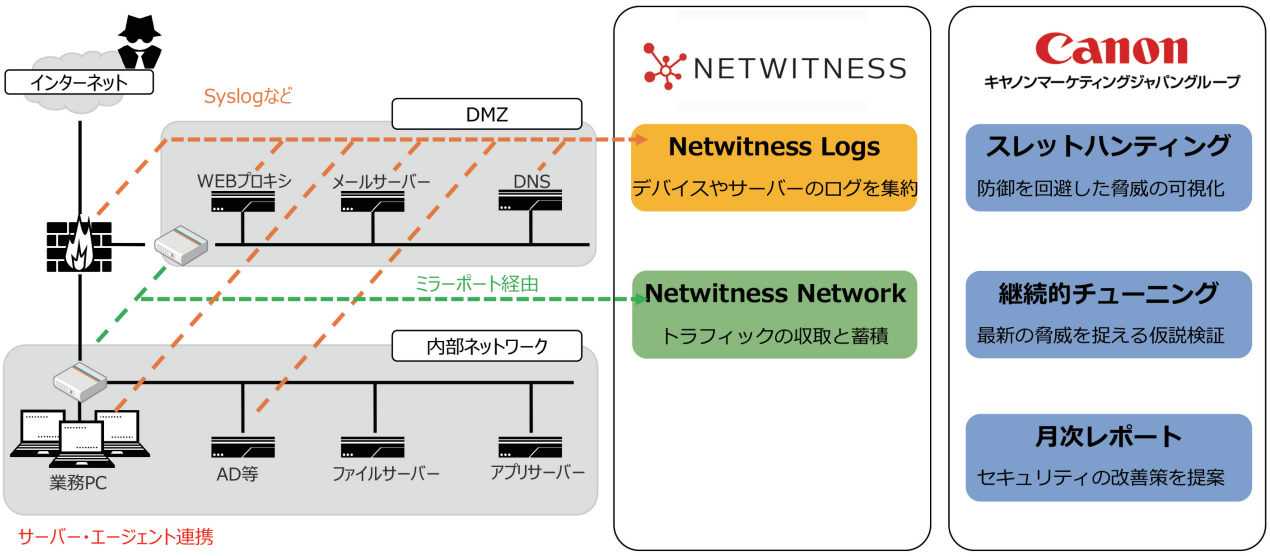
――では、ここまで挙げられたような課題について、キヤノンMJグループが提供するソリューションはどのようにして解決できるのでしょうか。

衣川氏：当社グループが提供するスレットハンティングサービスの軸となるのが、RSA社のネットワーク脅威可視化ソリューション「RSA NetWitness Network」です。NetWitness NetworkはNDRやフォレンジックの機能を兼ね備える商品です。ミラーリングしたスイッチポートからキャプチャしたパケットを保存し、豊富な検索項目を生成することでアナリストがハンティングするうえで有効な情報を提供します。

NetWitness Networkの優位点の1つが高速検索性です。通常、ネットワーク内の膨大なパケットを集めて保存し、過去の通信から調査対象のパケットを見つけようとすると、かなりの時間を要してしまうものです。これではインシデントが発生しても、その原因にたどり着けない、社外に公表すべき事実にたどり着けない、といったことが起こってしまいます。そこでNetWitness Networkでは、ネットワークセッション（ペイロード）を解析しなければ得られない情報をRSA特許の技術によりメタデータとして作成してインデックス化することで、長期間かつPBクラスの大容量のデータであっても速やかな検索を可能としているのです。こうしたNetWitness Networkならではの高速性は、脅威の早期発見・早期対応を可能にします。

また、セッションの再現が可能であることも、課題解決を可能にするほかに類を見ないNetWitness Networkの優れたポイントと言えるでしょう。パケットデータだけでは人間の目にわからないことも、セッション、つまりどのような通信が行われたか

スレットハンティングサービス



を再現できるのです。具体的には、流出したテキスト・メールビュー・Webビュー・ファイル抽出などさまざまな形式で再現が可能です。たとえばメールであれば、本文のみならず別ファイルに偽装されたマルウェアの添付ファイルまでも含めてすべて再現できるので、あとから確実に内容を追跡できます。

このほかにも、NetWitness Networkはスレットハンティング・ツールとしてさまざまな優れた特徴を有しており、前述したスレットハンティングのニーズが高まっている背景にある技術的な要素と法的な要素のいずれの課題も解決することが可能です。

脅威分析までをキヤノンMJグループがトータルサポート

――NetWitness Networkはどのような課題を持った企業におすすめできるでしょうか。

衣川氏：たとえば、CSIRTを構築してはいるものの、日ごろの脆弱性管理や社内教育などの日常業務に追われていたり、そもそも人手不足に陥っていて複雑な詳細分析をスピーディに行うことができなかったりといった企業には、特にうってつけのソリューションです。

また、SIEM内のログ情報でアラートがあがらないことに不安を覚えている企業や、経営層や株主といったステークホルダーへのコミュニケーションのために攻撃の影響範囲をすぐに把握したい企業、標的型の攻撃を受けた場合に既存システムで検知できるか不安な企業なども、導入効果が高いと言えるでしょう。

――キヤノンMJグループがNetWitness Networkを扱うことの強みはどこにあるのでしょうか。

当社グループでは、パケット解析アナリストを擁しており、スレットハンティングサービスを展開しております。こういったサービスを展開している企業はまだ少なく、これが最大の強みであると自負しています。せっかくツールを持っていても、使いこなせなければ意味がありません。キヤノンMJグループに解析運用をアウトソースしていただくことで、ネットワーク内にひそむ脅威を見つけ出し、原因を特定し、改善するまでをトータルでお手伝いさせていただくことが可能です。

――最後に、スレットハンティングの実施を検討している企業に一言お願いします。

衣川氏：既存の環境に影響を与えない導入のしやすさもNetWitness Networkの特徴なので、まずはPoCの実施をおすすめします。PoCで現状を可視化することで、実は社内に不安なパケットが流れていた、という気づきにもつながるはずです。

冒頭にお話したように、もはやサイバー攻撃は身近な問題であり、ひとたび被害にあえば事業継続を脅かすようなリスクにつながります。既存のセキュリティ対策を行っていたにもか

かわらず、侵入され、情報が漏えいしてしまい、さらには原因究明が迷宮入りしてしまってどこまで被害影響があるかがわからない――といったような事態を防止するためにも、ぜひ、キヤノンMJグループにお声がけください。

――より強固なセキュリティ対策を実現できそうですね、ありがとうございました。

※ ウェビナー動画
https://cweb.canon.jp/it-sec/solution/netwitness/lp/webinar20201223/

参考 サイバーセキュリティ情報局
「脅威を見つけ出すスレットハンティングとは？」
https://eset-info.canon-its.jp/malware_info/special/detail/201007.html

ネットワーク脅威可視化“RSA Netwitness Network”

NETWITNESS

既存のセキュリティツールをすり抜けて組織内に侵入した脅威を発見します。
大容量、かつ高負荷となる解析処理をすることを前提にした設計により高速検索を実現しており、ネットワークパケットの解析効率を大幅に向上させます。

スレットハンティングサービス

キヤノンマーケティングジャパングループのパケット解析専門のアナリストがお客様のパケットを解析します。
既存の対策に、セキュリティアナリストによる高度な解析を組み合わせることで、セキュリティ機器をすり抜けて侵入してきた攻撃を水際で捉えることができます。

詳細情報はこちら ▶ https://cweb.canon.jp/it-sec/solution/netwitness/

製品に関する情報はこちらでご確認いただけます。

Home Page セキュリティソリューション ホームページ
canon.jp/it-sec

●お求めは信用のある当社で

開発元：RSA Security LLC
Canon キヤノンマーケティングジャパン株式会社
〒108-8011 東京都港区港南2-16-6 CANON S TOWER

2021年5月現在
MRNW2105CMJ-PDF