サイバー攻撃全盛期、未知の脅威を追跡するスレットハンティングアプローチ

サイバー攻撃による国内企業の被害は、企業規模を問わず依然として増え続けている。どこもセキュリティ対策には投資をしてきているはずだが、大手企業であっても被害は後を絶たず、より踏み込んだ対策が求められている。具体的にどのような対策が功を奏するのか、キヤノンマーケティングジャパングループのセキュリティアナリスト2人から話を聞いた。

ケース 1
緊急アラートが起こらないことに悩むセキュリティ現場の事例

従業員1,000人を超える製造業。製造業では個人情報だけでなく開発や製造にまつわるデータも機密事項であり、そうした情報が漏洩すると社会的な信用を失墜し企業の存続にも影響を与えかねない。そのため同社ではSOC（Security Operation Center）を運用しており、セキュリティ機器が検知した脅威アラートの調査を行っている。
しかしながら、同社ではSIEMに取り込む大量のログから有意義な情報をほとんど得られず、社内ネットワークに脅威が本当に存在しないのか不安を覚えているという。同社では幸いなことにまだ情報流出という事態には見舞われていないが、同業他社がDXの一環としてECサイトを立ち上げたところ、サイバー攻撃を受けてしまい情報を漏洩したというニュースを耳にしている。そのため上層部からの定期的なセキュリティの報告要請がある一方で、日々のアラートに確信が持てない現場担当者には常に不安が付きまとう状況が続いているのだ。

依然として変わらない感染原因、進化するマルウェア

キヤノンITソリューションズ 上級セキュリティアナリスト（CISSP、GCIH）、山田和政氏は次のように解説する。


キヤノンITソリューションズ株式会社
上級セキュリティアナリスト（CISSP、GCIH）
山田和政氏

「当社のお客さまから自社組織がマルウェアに感染していないかどうか調べてほしいという依頼が多く、感染しているケースでは原因を調査し説明をさせていただくのですが、傾向として特に新しい動きはないといえます。むしろ感染の入り口は王道パターンであるe-Mail経由のマルウェア感染と公開サーバの脆弱性を狙った攻撃という2つの方法が続いていて、一方でマルウェアは高度化しておりセキュリティ機器による検知を回避できるものになっているという状況です」（山田氏）

また山田氏は次のように述べている。

「よく狙われる企業の公開サーバの代表的なものとしては、CMSで作られたメンテナンスされていないコーポレートサイトと、最近盛んなリモートワークで使われるVPNルーターが挙げられます。それぞれ脆弱性を突いて、そこを足がかりに組織内へと侵入するのですが、業種業態を問わず攻撃を受けているという印象がありますね。脆弱性の観点では、今回の同業他社が攻撃を受けてしまったケースでも、公表されている情報から判明していることは、ECサイトの脆弱性が狙われたということです」（山田氏）


キヤノンITソリューションズ株式会社
セキュリティアナリスト
新山怜史氏

山田氏と同じチームに所属するセキュリティアナリストの新山怜史氏は、今回の事例もふまえ、攻撃を受けてしまったケースの特徴を次のように解説する。

「インシデント発生したケースを時系列に調べてみると、攻撃を受けてから検知するまでにかなり時間が経ってしまっていて、既に情報が流出していたというケースが多いです。顧客やパートナーなど外部からの指摘を受けて攻撃が発覚するというパターンもあり、さらに悪いことには、攻撃の全貌や被害状況を把握できずにステークホルダーに報告ができないというケースもあります。こうした攻撃の多くは正常な通信を装うことから、現在主流の境界型セキュリティだけでは検知するのに限界があるといえるでしょう。被害を防ぐには、パッチを最速で当て続けるか、さらに閾値を緩くして大量のアラートを発生させてそれらを選別するかになりますが、どちらも現場の担当者の負担は相当なものです」（新山氏）

こうした攻撃パターンでは、発覚までに時間がかかるケースが多く、長いと1カ月近くもかかってしまうという。セキュリティ機

器の検知を回避する攻撃も見つけ出せるアプローチが必要であるといえる。

境界型セキュリティの限界がセキュリティ現場の疲弊を招く

ケースIで紹介した製造業のようにセキュリティ対策に注力している企業でも、決して楽観視できない状況が続いているのはなぜなのだろうか。

「攻撃側も、検知型のセキュリティ対策はされているものと認識したうえで検知を回避する攻撃をしかけてきます。たとえば、ファイル名とデータ構造を偽装し画像ファイルに見せかけたマルウェアなどが挙げられます。従来のセキュリティ機器では無害な画像データとして認識するのでマルウェアを検知せずに通信が許可されてしまいます。結果としてアラートが上がってこないために侵入されていることに気づけません。また、たとえば最近増えている機械学習(AI)型のセキュリティ対策製品は、閾値を下げて大量にアラートを発生させても機械学習により防御してくれるので、一見すると運用の手間が省け良い製品に思えます。しかし我々が実際に何社か製品を検証したところ、残念ながら完全に機械学習だけに頼り切って大丈夫とはいえない評価となりました。アラートの真偽を判定するのは現実的に難しく、機械学習の判断に委ねているとただ現場のセキュリティ担当者が数多くのアラートに振り回される要因になってしまいます」(山田氏)

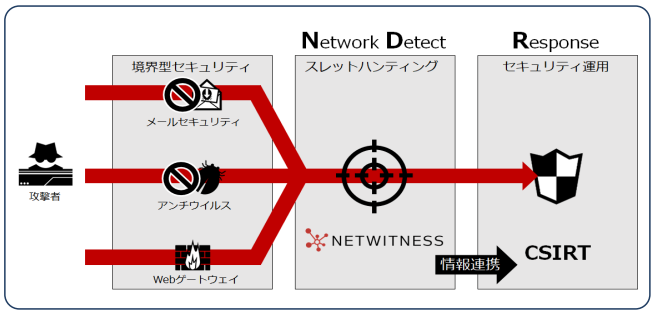
また、公開サーバの運用に関しても、検知型セキュリティツールで防げない脅威が存在する。たとえば昨今ニュースとなったVPN装置やSaaSの脆弱性を突いた攻撃や、アンチウイルスを回避して感染するようなマルウェアも珍しくなく、100%防御することは難しい。

「今回の事例では同業他社がサイバー侵害を実際に受けてしまっていますが、この例のようにECサイトなどを運営している場合、脆弱性の管理が問題になります。脆弱性を突いて侵入を許してしまうケースが増えており、検知型のセキュリティツールで防げない脅威にどう向き合うかということは課題であると思います」(山田氏)

「また、ECサイトを新たに立ち上げる場合、サイト担当者とセキュリティ管理者の間にはセキュリティリスクに対する認識が異なっていることがあります。その差を埋めるための専門知識をサイト担当者にわかりやすく伝えるには時間がかかるし、一方でサイトを公開するまでの時間も限られています。結果として、ある程度妥協した状態でサイトを公開せざるを得ないという現場もあるのではないかと推察されます」(新山氏)

見えない攻撃を見つけ出す「スレットハンティング」のアプローチとは?

こういった防ぎきれないサイバー攻撃の実態を受けて、いま注目されているのがNDRというアプローチである。キヤノンマーケティングジャパンではNDRのソリューションとして「スレットハンティングサービス」を業界内でいち早く提供している。このスレットハンティングサービスを実現するのが、NetWitness, an RSA Businessの脅威検出製品であるNetWitnessPlatformの製品群の一つであるNetWitness Networkである。同社のスレットハンティングサービスはネットワーク内を流れるパケットを解析し攻撃に関連する通信を見つけ出すアプローチであり、そこに脅威が存在するかもしれないという仮説を立てながら解析することで、通常見逃されがちな脅威を発見するものである。



継続的に仮説検証を続けることで脅威の早期発見に繋げることができるうえ、侵入した脅威を現在進行形で見つけることすらあるという。山田氏は次のように説明する。

「仮説に基づいた検証はスレットハンティングの本質です。たとえばUTMやファイアウォールで守っていたとしても、もしかしたら攻撃者に侵入されているかもしれないと仮説を立てて、検討を巡らせるというものです。そのうえで、どういった経路で侵入されているのかを考えていきます。最近はVPN装置の脆弱性を踏み台として侵入するパターンが増えていますが、そうであればVPN端末のIPアドレスから怪しいパケットが発生しているのではないかという仮説を立てて“網を張る”のです。そうすると、実際に攻撃を発見したり、見つからなくてもあちこちに網を張ることで予防につなげたりすることができるのです」(山田氏)

ケース2 スレットハンティングでマルウェア感染を事前に防いだ好事例

卸売業を営むある大手企業では、ネットワークの可視化と証跡保存のためにNetWitness, an RSA BusinessのNetWitness Networkを導入し、山田氏のチームがスレットハンティングサービスを提供している。

そんな中、ビジネスメールを装った標的型攻撃メールが発端で一台の端末がマルウェアに感染し、この端末を踏み台として段階的にマルウェアを拡散する通信パターンを発見したという。ネットワーク内のパケットをスレットハンティングで解析していくと、マルウェアをダウンロードするだけでなくデータを送信している痕跡が見られたことから、情報漏洩も発生している可能性が疑われた。

そこでさらにNetWitness Networkで取得したパケットをもとに、同製品が生成するメタデータにより高速解析を実施し外部

に送信される通信を深く調べたところ、マルウェアがファイルを暗号化して外部に通信していた痕跡を発見。より深く分析するためNetWitness Networkのセッション再現機能により外部に送信されたファイルを復元した。当該ファイルは暗号化されていたが、キャプチャしていた通信データを利用して復号し、漏洩したデータ内容を突き止めることにも成功。幸いにして初期段階で発見したことから、重要なデータが漏洩する前に対処することができたのである。

スレットハンティングサービスで9割以上の脅威を削減

この事例は、山田氏らのチームが実際にスレットハンティングの手法を元に、ネットワークパケットの解析を行い、マルウェア感染による被害を最小限に抑えたというものだ。実際のデータはお見せできないが、現場から回収されたマルウェアを検証環境で動作させ、マルウェアが外部に送信したデータをキャプチャしたのが次の画像である。Webブラウザで送受信されたデータ、ドキュメント作成中の入力データ、クリップボードの中身、メール操作履歴などがマルウェアによってテキスト化され、外部に送信されていることが確認できる。

```
12-05-2021 17:25:38
USER: FORENSICS
URL: https://syndication.twitter.com/i/jot
REF:
LANG: ja-JP
AGENT: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
COOKIE: guest_id=v1%3A148057333537796640; pid="v3:1480644914387403334035285"; _ga=GA1.2.9670917
POST: dnt=0&tfw_redirect=https%3A%2F%2Fplatform.twitter.com%2Fjot.html&l=%7B%22widget_origin%22


12-05-2021 17:29:21
C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
新規 Microsoft Excel ワークシート.xlsx - Excel

okyakusama
he
kyouryokumousiire

mainabi
heno
kokuti


12-05-2021 17:29:47
Clipboard

スケジュール確定


12-05-2021 17:30:32
C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
```

今回の事例では従業員がビジネス詐欺メールに添付されていたWordファイルを開封してしまったことによりマルウェアに感染した。そもそも、これらのインシデントからいえるのは、組織や人の心理的に弱い部分を狙った攻撃は原則的に防ぎにくく、それを認める必要があるということだ。

「社内ルールに則っていればインシデントは発生しないと思われがちですが、そうではなく誰かがマルウェアを開いてしまったことを前提に、そのあとのことを常に考えないといけないのです。社員の教育で対処できる部分もありますが、完全には防ぎきれないことを前提に対策を考えるべきでしょう」(山田氏)

第1の事例に出てきた同業他社は既存のセキュリティをすり抜けてマルウェアに感染し、第2の事例では巧妙に作られたメールを介してマルウェアに感染してしまっていた。最新のサイバー攻撃の現場では侵入されてしまうことを前提とした守りが必要であり、守りのカギとなるのは、早期発見し内部拡散を防ぐアプローチである。内部ネットワークに何が起こっているのか、感染端末からどのような通信が発信され、漏洩した情報はどのファイルなのか、自社の環境を襲うサイバー攻撃をいち早く発見し、被害が発生することをくいとめることが大切なのだ。

それには内部の通信データを高速に解析できる仕組みとスレットハンティングのアプローチが有効である。Netwitness Networkなら、取得したパケット情報をもとにペイロードを解析しなければ得られない情報をメタデータとして生成できるため、解析効率を大幅に向上することが可能だ(NetWitness, an RSA Businessの特許技術)。また、今回の事例のようにセッションの再現が可能であることも他製品に類を見ない優位点である。メールやファイルデータをすべて復元できるので、証跡保存と迅速な被害状況の追跡に大いに役立つものである。加えて、セキュリティ現場の状況によっては解析に専門家の力を借りることも選択肢の一つである。専門のセキュリティアナリストがネットワークパケットの解析をサポートすることで、組織内に侵入した見えない脅威が発見できるようになる。

キヤノンITソリューションズは、山田氏や新山氏をはじめとしたパケット解析専門のセキュリティアナリストがNetwitness Networkを活用して、顧客のパケットを解析するスレットハンティングサービスを提供。既存の対策にセキュリティアナリストの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た攻撃を水際で捉えることができるのだ。また、解析サービスのみではなく、報告書としてセキュリティの改善提案が受けられることもキヤノンマーケティングジャパングループが提供するスレットハンティングサービスの長所である。

スレットハンティングで脅威を捕らえる詳細については、キヤノンマーケティングジャパンが公開しているウェビナー動画でも詳細が解説されているのでぜひご覧いただきたい。

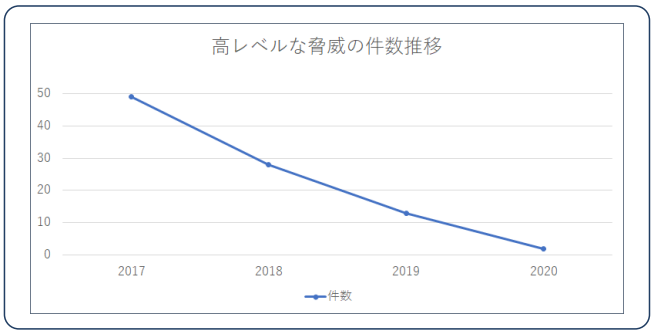
最後にスレットハンティングサービスの導入効果について触れたい。

この企業はセキュリティ対策への投資に積極的で、既にいくつかのセキュリティ機器が導入されていた。ただし、セキュリティ機器が具体的にどの程度の効果を上げているのか測る術がなく、問題が発生しないのは対策が上手くいっているからなのか、それともセキュリティ機器が機能していないからなのか、判断できない状態であった。

これに対して山田氏のチームが初年度のスレットハンティングを行った結果、実に年間49件もの重大なセキュリティ脅威が発見され、さらに脅威が侵入し易くなっている箇所も特定することができたという。

キヤノンマーケティングジャパングループは脅威を検出したあとのアドバイスも提供している。この企業ではアドバイスに基づいてセキュリティ対策を改善し続け、サービス導入から4年を経て重大な脅威の件数は49件から2件へと大幅に減少した。

スレットハンティングを通じて継続的にセキュリティ対策の効果が確認できたことにより、セキュリティ対策の現状を認識し、さらなる改善に向けて適切な投資をすることができたのである。



「白黒判定できないグレーな部分に隠れた脅威を発見できるのが、スレットハンティングサービスの強みです。発見された脅威に対して何をすればいいかわからなくても、我々から推奨策を提示できます。どうすればセキュリティ課題を解決できるのか、ぜひ一緒に考えさせていただき、最終的にお客さまの本来的な業務にリソースを集中できるようになることを目指しています。まずは遠慮なくご相談ください」と、山田氏は力強く締めくくった。

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

※ 製品紹介サイト：
https://cweb.canon.jp/it-sec/solution/netwitness/

ネットワーク脅威可視化 “RSA Netwitness Network”

NETWITNESS
An RSA Business

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6月現在
MRNW2105CMJ-PDF