MACNICA

伊藤忠商事CSIRTが海外拠点にも展開するスレットハンティングサービス

POINT

- 既存のセキュリティ製品をすり抜けることを前提にした高度な標的型攻撃を、AI技術を用いた独自のセンサーとアナリストによる分析で検出
- 2万台の端末を調査し、情報収集から検知、対応までの診断ライフサイクルを確立
- IT管理者がいない海外拠点の端末の安全性を可視化

インシデントの予防にフォーカスした伊藤忠商事のITCCERT

近年のサイバー攻撃は、犯罪目的の産業化によって技術や手法が高度化・巧妙化し、企業や組織を標的とした攻撃は経営上の大きなリスクになっている。

また、ランサムウェアやビジネスメール詐欺のように金銭を目的とした攻撃は、多くの企業にとって身近な脅威である。

そのため、最近では、コンピュータセキュリティにかかるインシデントに対処するための組織であるCSIRT（Computer Security Incident Response Team）を設置する動きが活発化しつつある。

伊藤忠商事株式会社（以下、伊藤忠商事）がCSIRTを発足したのは2012年のことだ。同社のCSIRTは「ITCCERT」と呼ばれている。“R”には、準備（Readiness）・対応（Response）・復旧（Recovery）の3つの要素を含むという。

「ITCCERTは全社のネットワークを管理・運用するIT企画部の中に仮想的に作られた組織です。ITCCERTはサイバーセキュリティ運用に特化し、インシデントの防止、対応、分析、再発防止などを中心に実施します。また、300社以上存在する伊藤忠グループ企業からも支援要請があれば直接の支援を行います」と語るのは、伊藤忠商事IT企画部 技術統括室ITCCERT上席サイバーセキュリティ分析官の佐藤 元彦氏だ。

伊藤忠商事ではカンパニー制をとり、各カンパニーでも情報システム部門が個別に設置されているが、サイバーセキュリティインシデントが発生した際はITCCERTが中心となって対応を実施する。

また、ITCCERTではネットワークの通信や社外から送信されてくるEメールなどを常時監視している。自社で蓄積したナレッジを基に独自の検知ルールを設定することで、既存のセキュリティ製品では検知できない特徴を把握し、万が一同様の攻撃が発生した時に検知できるルールを常に生み出している。

独自のインテリジェンス活動で得られたマルウェアの通信先やハッシュなどの情報は伊藤忠商事を守るために使われ、同社のセキュリティ事案の発生を未然に防止している。

「ITCCERTはインシデントのプリベンション（予防）にフォーカスしており、インシデントを起こさないことが重要と考え日々活動しています」と佐藤氏は強調する。

伊藤忠グループのスレットハンティングサービス

一方、伊藤忠グループや海外拠点は、伊藤忠商事本社のネットワークとは異なるネットワークを使っているため、これらの防御効果が直接の効果を発揮しない。

そのため、ITCCERTでは、グループ会社や海外拠点に向けた特別なサイバーセキュリティプログラム「“I”シリーズ」を展開している。

その内容はURLフィルタリングサービス、ビジネスメール詐欺対策ツール、サイバーセキュリティに特化したリスクアセスメント、実業務ですぐに役立つワークショップなど多岐に渡る。

そのメニューの1つ、「“I” Discovery」は、端末に潜伏するマルウェアを検査するエンドポイントセキュリティで、2017年10月のサービス開始から2万台以上の端末に対し脅威検査した実績を持つ。その中核技術には、台湾のTeam T5が

USER PROFILE

ITOCHU

伊藤忠商事株式会社

1858年（安政5年）に、近江商人だった初代伊藤忠兵衛が麻布（まふ）の行商で創業。その後大阪で呉服太物商を営み事業の礎を築いた。現在は日本を含む世界65ヶ国に約130の拠点を持つ大手総合商社として、繊維、機械、金属、エネルギー、化学品、食料、住生活、情報、保険、物流、建設、金融の各分野において国内、輸出入および三国間取引を行うほか、国内外における事業投資など、幅広いビジネスを展開する。

https://www.itochu.co.jp

伊藤忠商事株式会社
IT企画部
技術統括室
ITCCERT
上席サイバーセキュリティ分析官
佐藤 元彦 氏

システムインテグレータ企業で官公庁や大手民間企業に対するセキュリティコンサルティングや、情報セキュリティ監査・情報システム監査、インシデントレスポンスを経験。その後、伊藤忠商事株式会社のCSIRTチームであるITCCERTに所属し、同社／グループ全体のサイバーセキュリティ施策の立案・遂行・運用業務に努める。また同時に、国立大学法人千葉大学運営基盤機構 情報環境部門で准教授も兼任し、学内のCSIRTチームであるC-csirtの運用や、制度・仕組み作り、実務支援、トリアージ支援、情報提供なども行っている。

開発したハンティングツール「ThreatSonar」が活用されている。

ハンティングに必要不可欠な情報を収集するフォレンジック技術

ThreatSonarは端末の実行中プロセスや削除されたファイルに関する情報、メモリ上のデータなどコンピュータ・フォレンジックに必要な情報を素早く収集する。収集した情報を独自のエンジンで解析することで不審ファイルの精緻な抽出が可能だ。AIが補助する独自のビヘイビアモデルで不審な挙動を検出するため、シグネチャベースのアンチウイルスで検知できないような徹底した調査が可能だという。収集した情報は専門知識を持つITCCERTのスタッフが分析することにより、既存のウイルス対策ソフトでは検知できないマルウェアが潜伏している場合も検出可能になった。また、検出結果をITCCERTと各グループ会社の情報システム部門が共同で結果を分析することで、早期に適正な対応が判断できるようになっている。

既存のエンドポイントセキュリティでは検知できない脅威を発見

さまざまなエンドポイントセキュリティの手法がある中で、ThreatSonarを選んだ理由について、佐藤氏は、基本技術がアンチウイルスではない点と、セキュリティレベルを大きく向上できるソフトウェアとしての優秀性を挙げる。

伊藤忠グループの子会社は300社を超え、従業員数は約10万人に上る。さらに、商社という側面から合弁会社の設立や資本業務提携も活発である。そのため、伊藤忠グループでは特定のエンドポイントセキュリティ製品の導入を強制しておらず、各社の要件に基づいて最適な製品が導入されている。各社に共通しているのは、アンチウイルス製品を導入している点ぐらいだ。

「次世代アンチウイルス製品もアンチウイルスの延長線上です。アンチウイルスベンダーは技術の得手不得手があり、全ての脅威を網羅的に排除するのは難しい。そのため、各社が利用している既存のアンチウイルスを活用しながら、独自の機能ですり抜けた脅威を検出できるセキュリティ製品としてThreatSonarはとても魅力的でした」

“I” Discoveryの提供を開始したところ、50社以上のグループ企業がサービスの利用に手をあげた。ワンショットのスキャンを行った企業は申込企業の半数を超え、定期実行を行う企業も出始めた。“I” Discoveryの定期実行を行う企業の情報システム部門は、既存のセキュリティ製品で検出できない未知の攻撃や、検知を回避するような攻撃によって自社端末が侵害されていないことを確認できる点に満足しているという。

グループ会社への展開は導入の容易さが決め手

「ThreatSonarはインストールの必要はありません。軽量なスキャナーを配布して実行するだけなので、ユーザ側に知識や運用のスキルを求めず、全てバックグラウンドでサイレントに動作します。

また、動作中の通信量は軽微なためネットワークへの負担が少なく、OSやアプリケーションなどとの競合や環境依存などの問題が起きないのもメリットです」（佐藤氏）

リソースの限られた海外拠点でも監視体制を構築

“I” Discoveryを実施することにより、長年正規のプロセスに隠れていたバンキングマルウェアが見つかった事例も報告されているという。また、アクティブなマルウェアだけではなく、潜伏状態のマルウェアや、ユーザによってインストールされたリスクを含んだソフトウェアを検出するのは心強いと佐藤氏は評価する。

なお、“I” Discoveryは海外拠点のユーザも利用している。海外拠点によってはIT管理者が不在、さらには駐在員が1名しかいないケースもある。また、海外拠点で使用している端末はWindowsのOSバージョンや言語も様々だ。そのような環境でも容易に展開でき、運用面でも問題が起きないのがThreatSonarのメリットのひとつだ。

最後に、ITCCERTでは今後、“I” Discoveryにカスタムシグニチャの適用を検討しており、伊藤忠グループのセキュリティの更なる強化に取り組んでいくと佐藤氏は語ってくれた。

Mpression Cyber Security Service™ スレットハンティングサービスのご紹介

MPRESSION Cyber Security Service

マクニカネットワークスでは、ThreatSonarのスキャン結果の分析、スレットハンティングをお客様に代わって弊社のセキュリティアナリストが実施する「スレットハンティングサービス」をご提供しています。また、弊社が蓄積する脅威インテリジェンスに基づいて作成するカスタムシグネチャを反映することで、日本を狙う標的型攻撃の検知率の向上を図っています。

スレットハンティングサービスは、「ワンショット」での利用と「年間」利用の2つのメニューをご用意しております。

https://www.macnica.co.jp/

MACNICA

株式会社マクニカ　ネットワークス カンパニー

〒222-8563 横浜市港北区新横浜1-5-5
TEL.045-476-2010 FAX.045-476-2060
西日本オフィス
〒530-0005 大阪市北区中之島2-3-33 大阪三井物産ビル14階
TEL.06-6227-6916 FAX.06-6227-6917