急増する高度で巧妙なサイバー攻撃
―事例に学ぶ、未知の脅威への対応策

いま多くの日本企業が、ゼロデイ攻撃をはじめとした未知の攻撃がもたらす脅威にさらされている。こうした攻撃が厄介なのは、従来のマルウェア対策だけでは十分に防ぎきれない点にある。では、効果的な対策はないのだろうか――ある企業の事例を追いながら、少ない人的リソースとコストでも、未知の脅威から自社を守るのに十分な効果が得られる具体的な対策を紹介したい。

未知の脅威がもたらすリスクを知り、重い腰を上げたA社

ここで紹介するA社は、産業機器を製造する国内大手メーカーであり、高品質なその製品は海外市場においても高いシェアを誇っている。社員は海外法人も含めると5,000人近くにもなり、多数のグループ会社も有している。

そんなA社だけに、多くの国内企業と同様に海外からと思われる不正アクセスが頻繁に検出されていた。約4年前からこうした傾向が見られたものの、なかなか具体的な対策を立てるまでには至らなかった。というのも、本社情報システム部門のスタッフは15人程いるものの、そのうち情報セキュリティ担当者は3人程度であり、日々の業務に追われていたのである。また、限られたセキュリティ予算のなかで、不正アクセス対策にコストを割くのもハードルが高かった。

しかしながら、昨年に情報セキュリティ担当者の1人が企業向けのセキュリティセミナーを受講したのをきっかけに、事態は急速に進展することとなった。セミナーでは、従来のマルウェア対策だけでは侵入時に危険か否か即断ができないこと、ゼロデイ攻撃をはじめとした未知のサイバー攻撃による被害が昨今多発していること、同じく近年急増している標的型サイバー攻撃ではエンドポイントを狙うマルウェアも攻撃対象に合わせて、カスタマイズされるため検知が難しくなっていることなど、最新の脅威動向が取り上げられていたのである。セキュリティ担当者がセミナーの内容をCISO(Chief Information Security Officer)に報告したところ、同社が展開するB2Bビジネスにおいて重要な取引先情報や、製品品質を支える数々のノウハウなどが機密情報の漏えいにつながりかねない最優先に対処すべき重大リスクだと判断され、早急な対策へと舵が切られたのだった。

検討後わずか数週間で、ゼロデイ攻撃に対する即時防御が可能な体制に

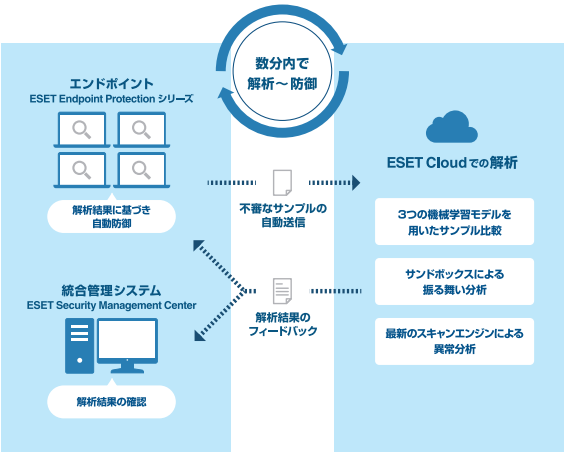
A社としては深刻な課題であった未知の脅威対策だが、結果的に想像していたよりも短期間かつ容易に、効果的な解決策を打つことができたのだった。なぜなら同社では、具体的な対策の検討を開始してからわずか数週間後に、キヤノンマーケティングジャパン(キヤノンMJ)が法人向けに提供するESETセキュリティ ソフトウェア シリーズの新製品である「ESET Dynamic Threat Defense(以下、EDTD)」の導入に成功したからである。

EDTDは、ベースとなる法人向けエンドポイントセキュリティソリューション保護製品「ESET Endpoint Protection(EEP)シリーズ」と連携することで、未知の高度なマルウェアに対する検出力・防御力を高める次世代アンチウイルスソフト(NGAV)のクラウドサービスである。エンドポイント側で

脅威の防御

クラウド型ゼロデイ攻撃対策　ESET Dynamic Threat Defense

未知の高度な攻撃をクラウドテクノロジーで自動解析・自動防御



- NGAV的なクラウドサービス
- 100%白黒判定ができない不審なサンプルをクラウドで自動送信し、多段階に解析
- 解析は数分で完了、悪質な場合は全端末にフィードバックされ自動ブロック
- サンプルの解析結果をレポートとして可視化
- エージェントレス

クラウド型ゼロデイ攻撃対策製品「ESET Dynamic Threat Defense(EDTD)」

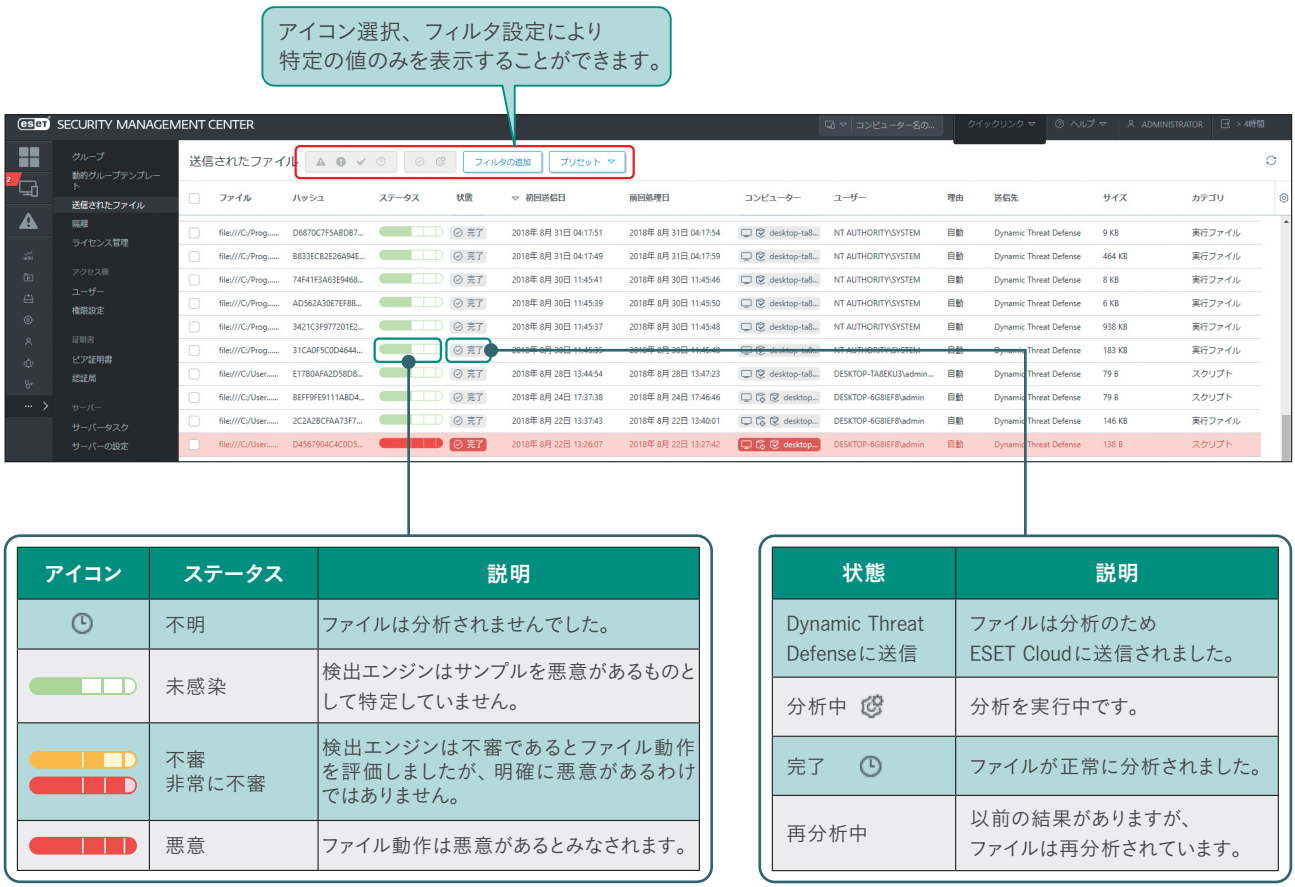
完全には判断できなかったファイルをクラウド側で高度かつスピーディな解析で検知を可能とするのがEDTDの最大の特徴だ。加えて、解析結果をレポートで可視化するため、効果的な対策につなげやすいといったメリットもある。

EDTDは、法人向けエンドポイント保護製品 EEPと連携して動作するが、A社では数年前よりこの製品を全社的に導入しており、多層防御による高い検知率や軽快な動作を高く評価していた。そしてEDTDは、EEPで用いるESET Security Management Center(ESMC：管理サーバー)の設定画面でライセンスを有効にするだけで導入が完了するため、容易かつコストも最小限に抑えることが可能だ。A社でもこの操作だけで、そのあとは自動的にEDTDと連携して処理が実行されるようになり、未知や亜種のマルウェアも検知できる体制を整えたのだった。

未知の脅威も自動防御＆高い検知率で運用負荷を軽減

A社がEDTDの運用を開始して約1年、EEPとEDTDの連携により世界中で大流行した新種のマルウェアも、サプライチェーン攻撃とおぼしき怪しいファイルも検知したことで被害を免れることができた。当初の懸念事項であった運用負荷も、EDTDであれば未知の脅威に対する自動防御も可能であるため、人的リソースを割くことなく、容易に運用することができたという。加えて、EDTDの誤検知の少なさも運用負荷の軽減に大きく貢献している。

実はA社では、EDTDの導入を検討する際に他社製のNGAV製品も試用していた。しかし、その製品は安全なファイルまでもマルウェアと判断してしまう過検知が著しく、セキュリティ担当者が検知後の判断作業に追われてしまうといった状況に陥ってしまった。そうした無駄な労力もEDTDであればほとんど生じないことが、この1年の運用であらためて実感できたのだった。なお、ESET社では従来から一貫して「誤検知ゼロ」を目標に掲げており、第三者テスト機関であるAV-Comparativesからも「最も誤検知率が低いベンダー」と評価されているほどだ。これに加えて、検出結果の脅威度判定に応じて検知レベルを3段階で設定可能なため、A社にとって最適な検知レベルを設定することがで



アイコン	ステータス	説明
	不明	ファイルは分析されませんでした。
	未感染	検出エンジンはサンプルを悪意があるものとして特定していません。
	不審 非常に不審	検出エンジンは不審であるとファイル動作を評価しましたが、明確に悪意があるわけではありません。
	悪意	ファイル動作は悪意があるとみなされます。

状態	説明
Dynamic Threat Defenseに送信	ファイルは分析のため ESET Cloudに送信されました。
分析中	分析を実行中です。
完了	ファイルが正常に分析されました。
再分析中	以前の結果がありますが、 ファイルは再分析されています。

日本語環境にも対応しており、一覧で確認することができる

きた。さらに、PC担当の情報システムスタッフが感心した動作の軽快さも、EDTDのみならずEEPを含めたESET製品の強みとなっている。

シームレスな事後対策も可能に

EEPとEDTDを連携させることで、サンドボックス上での高度な振る舞い検知を軸に未知や亜種のマルウェアであっても検知・防御ができるようになり、エンドポイントセキュリティの底上げを実現したA社。同社は現在、4段階で表されるEDTDのサンドボックスでの検出結果レポートを解析した上で次なる対策を検討するなど、情報セキュリティ対策のPDCAサイクルも整えることができた。

そんなA社では、今後のロードマップとしてサイバー攻撃による被害を受けた際の事後対策を的確に行うEDR(End point Detection and Response) 製品「ESET Enterprise Inspector(EEI)」の導入を検討中だ。EDRもまたEEPと連携することで、事後の対処策をシームレスに統合することを実現できるセキュリティソリューションである。EEPとEDTDによってエンドポイントでの防御を強化した地盤固めが、EEIの導入で将来的にもA社の活躍を支えることだろう。

送信されたファイルの一覧および分析情報をレポートで確認

クラウド型ゼロデイ攻撃対策製品

ESET DYNAMIC THREAT DEFENSE

イーセット ダイナミック スレット ディフェンス

製品の詳細情報はこちら

▶https://eset-info.canon-its.jp/business/edtd/

ESET Endpoint Protectionシリーズの検出力・防御力をさらに高めるクラウドサービスです。ゼロデイ攻撃に用いられるような未知の高度なマルウェアに対する検出・防御の即時性を高め、ESET Endpoint Protectionシリーズのユーザーは、端末への新規プログラムインストールをする必要がなく、手軽に多層防御機能を強化することができます。

EDR (Endpoint Detection and Response)

ESET ENTERPRISE INSPECTOR

イーセット エンタープライズ インスペクター

製品の詳細情報はこちら

▶https://eset-info.canon-its.jp/business/eei/

ESET Enterprise Inspectorは、エンドポイントレベルでのマルウェア対策を30年にわたり手がけてきたESET社の経験を基に開発されたEDR製品です。組織内の端末から収集したさまざまなアクティビティをもとに、端末上の疑わしい動きを検出・分析・調査し、組織内に潜む脅威をいち早く割り出し、封じ込めることができます。

製品に関する情報はこちらでご確認いただけます。

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：ESET, spol. s r.o.

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

2020年9月現在
MEDT2009500MUR-654