特別対談　辻 伸弘氏 × キヤノンマーケティングジャパン

「セキュリティ製品を入れておけば大丈夫」な時代は終わった

―企業と個人がそれぞれ気をつけるべきポイントとは

脅威動向が激しく変動し続けている近年、あらためて事後対策への注目度が高まっている。そこで今回、国内企業に求められる事後対策のあり方について探るべく、セキュリティリサーチャーとして活躍する辻氏と、国内で法人向けESETセキュリティソフトウェア シリーズの提供を行うキヤノンマーケティングジャパンの西村氏によるオンライン対談を企画した。そこでは、現在の企業における事後対策における課題と、その解決の糸口となるソリューションなどについて意見が交わされた。

世界的に拡大する標的型ランサムウェアの脅威

西村氏：最近のセキュリティ動向のなかで辻さんが特に気になっていることは何でしょうか。

辻氏：2015年頃 からランサムウェアを観察し続けているのですが、そのなかでも最近主流になってきている「標的型ランサムウェア」の動向に特に注目していますね。従来のランサムウェアというのは「窃取したり暗号化したりした情報を返して欲しいのであればいくら払え」といった条件を攻撃者から突きつけられるというのが一般的でしたが、最近の標的型ランサムウェアでは、これに加えて「条件に応じなければ盗んだ情報を公開するぞ」といった脅迫も行われます。

もっとも、企業が標的型ランサムウェアの被害にあったとしても、そのインシデントの詳細が公開されることは、いろいろな理由からほとんどありません。それでも同じような被害に遭わないようにするためには、公開してもらわないことには十分な対策が打てませんよね。なので、被害者側ではなく、攻撃者側を観察し続けることで、標的型ランサムウェアの実態が見えてくるのではないかと、以前に引き続いて観察を続けています。窃取した情報についても、攻撃者は公開していますからね。

西村氏：具体的にどんな方法で観察しているのですか。

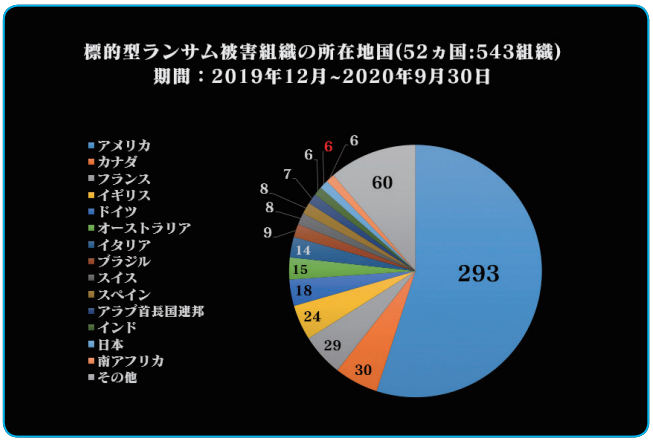
辻氏：2019年末頃から、Maze、DoppelPaymer、Nefilim、CL0Pなど主要な7種類のランサムウェアの動向を毎日観察して記録を取るようにしています。 観察方法としては、自動更新のチェックプログラムをつくって、定期的に アクセスして、攻撃動向について何か更新があれば自分に通知するようにしています。また私自身も1日に1回は直接見るようにしています。更新された攻撃情報などは地図上にポイントするとともに、データをExcelに蓄積しています。

SBテクノロジー株式会社
プリンシパルセキュリティリサーチャー
辻 伸弘氏

キヤノンマーケティングジャパン株式会社
サイバーセキュリティ技術開発センター
サイバーセキュリティ技術検証課
西村 亮氏

標的型ランサム被害組織Map

辻氏：こうした観察の結果、2019年12月から2020年9月30日までの期間における標的型ランサムウェア攻撃で被害を受けた組織の数は543組織にものぼっています。そしてポイントした地図を見ることで、たとえばCLOPであれば被害がヨーロッパに集中しており、とりわけドイツの組織の被害が多いことがわかります。あと全体的な被害を受けた組織の所在地域・国については293組織と圧倒的にアメリカが多くて、日本の組織の被害は6件となっています。業種別では、全体で見るとわりとバラついているのですが、最近目立っているのが、建設・土木業界の組織の被害でしょうか。あと、不動産や弁護士の被害も多い印象を受けるのですが、扱っている情報の重要性と、その割にはセキュリティ対策が進んでいないといったことが背景としてあるのかもしれませんね。



標的型ランサム被害組織の所在地国

西村氏：標的型ランサムウェアによって機密情報などが窃取されてしまった場合、攻撃者に金銭を支払ってでも取り戻すべきかどうかの判断基準についてどう考えますか。

辻氏：そこは非常に難しい問題で、正直、答えはないでしょうね。経営判断としか言いようがありません。実際、公開はされていないものの支払っているケースも多いですし。ただ、被害にあったときに、誰の判断で、いくらなら払うのかなど、事前に自社なりの判断基準を準備しておくことは必要だと思います。

私の知っているものだと、よく似た標的型ランサムウェア攻撃を受けた2つの組織で、片や攻撃者に金銭を支払い、片や支払わなかったという判断に分かれたケースがあります。支払ったのはある病院で、木曜の夜にランサムウェアの感染を認識してから、週末中に攻撃者に対し日本円にして400万円ぐらいを支払ったことで、月曜からは通常運営に戻っています。一方の支払わなかったアメリカのある自治体では、日本円にして少なくとも10億円を対策と復旧にかけました。この2つの組織の行動、どちらが良いのかは第三者から判断するのは難しいでしょうね。

「流行りだから」でセキュリティ製品を導入したのでは無意味

西村氏：脅威が増大傾向にある標的型ランサムウェアの被害に遭わないために、個々人が気をつけるべきポイントは何だと考えますか。

辻氏：標的型ランサムウェアに関しては、個人個人でできる対策というのは限定的かもしれません。侵入経路はいくつかありますが、個人で気をつけられるポイントとしてはメールという経路が挙げられますので 、添付ファイルをむやみに開かない、リンクのURLを安易に踏まないなど、基本的なところは引き続き注意すべきでしょう。そのなかでは、“コロナ禍”で再び攻撃が活発になっているEmotetのように、情報の窃取に加え、更にほかのウイルスへの感染のためにバックドアのように振る舞うマルウェアがランサムウェアの感染を招いたりするので、気をつけないといけないでしょう。

西村氏：辻さんのお話を聞いていて、やはりこれまでのように「アンチウイルスがあれば大丈夫」といった時代は終わりを告げ、何か被害が生じたとしても、いち早く通常の状態に戻せるようにするという対策がこれからの主流になってきていると、あらためて実感しました。もちろん、一人ひとりのユーザーが気をつけるべき点は気をつけつつ、企業側でも対策を施していたとしても、サイバー攻撃による被害を完全に防ぐことはできないので、もし被害に遭ってしまったら、どれだけ早い段階で元に戻せるかにフォーカスすることが重要でしょうね。

辻氏：その通りだと思います。Emotetにしても、どうすればEmotetによる被害を防げるかという限定的な話になりがちですが、実際の攻撃にはいくつものフェーズがあるので、それを踏まえたうえで、どこで検知し、どこで止めるのか、そのためにはどのようなセキュリティ製品が必要なのかといった、全体の流れのなかから対策を考える必要があるでしょうね。

西村氏：まさしくセキュリティ製品の選定にも影響していますよね。 あまりにも多くの製品があるなかで、どうしても検討フェーズでは機能の比較に偏りがちですが、まずは人が気をつけるべきポイントを整理することが大事で、それだけでもセキュリティレベルを上げることができますからね。 実際、セキュリティレベルを高めたいから製品を導入したいというざっくりとした要望が多くあります。「EDR(Endpoint Detection and Response)ってよく知らないけど、流行ってるみたいだからうちでも導入したい」などです。ご存じのとおり、EDRというのは導入すれば終わりではなく、日々の運用監視が重要となってくるので、そこまでを踏まえて、本当に自分たちで使いこなせるのか、費用対効果はあるのかなど、しっかり考えなければいけ

ないはずです。

辻氏：どんなに優れたセキュリティ製品があっても、使いこなせなければ無用の長物ですからね。なので、その製品を使いこなすには、自分たちに足りないのは何か最初に明確にしないといけないでしょう。そもそも扱える人材が社内にいるのか、もしいないのであれば外部に委託するかなど、ですね。同じく最近流行りの脅威インテリジェンスにしても、そこから情報だけもらったとしても、その意味がわからないのであれば有効な対策に結び付けられないですから。EDRにしても、そこから上がってくるアラートの意味を理解できるのか、画面は見やすいか、などが大事なのかもしれません。

西村氏：そうですね。製品の機能も大切ですが、そもそもEDRとは何かという前提や、そこから提供される情報について理解して、組織に展開できる知識や能力があるかがまずはポイントとなってくると思います。

EPPと統合したEDR製品の強みとは

辻氏：ここからは西村さんにお聞きしたいのですが、これからEDRの導入を検討するとき、企業や組織に、最低限これだけはやっておいて欲しいということはなんですか。

西村氏：やはり、OSを最新状態に保ったり、適切なアクセスコントロールを施したりなど、製品に頼らずにできるセキュリティ対策をしっかりとしていることが最低限必要です。そこが……、な状態のまま、EDRに限らずほかのセキュリティ製品を入れても十分な効果は期待できません。EDRというのは、アンチウイルスのように入れてしまえばそれで安心という製品ではありませんから。

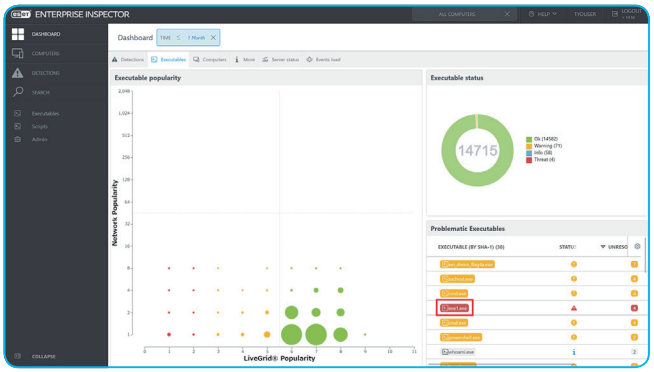
辻氏：最近はEDR万能説とAI万能説がはびこっていますよね。すべて任せてしまえばやってくれる……？そんなわけないのですが……。

西村氏：AIにしても、やはり人に依存するところがありますよね。トレーニングセットはどれを選択すべきか、どういったところにAIを活用すべきか、といった人による判断が肝になってきますから。

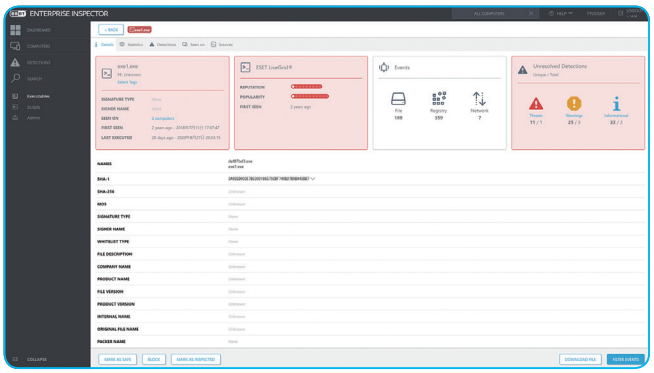
辻氏：そこで気になるのは……、やっぱり西村さんが扱っているEDR製品の特徴は？となりますよね。

西村氏：そうですよね（笑）。ではしっかり紹介させてください！我々が提供しているのは、ESETセキュリティ ソフトウェア シリーズのEDR製品「ESET Enterprise Inspector（以下、EEI）」で、その最大の特徴はアンチウイルスなどエンドポイントセキュリティの基本となるEPP（Endpoint Protection Platform）製品とシームレスに統合している点にあります。EEIは、ESET社の30年以上にわたるエンドポイントセキュリティ対策の知見をもとに開発されたEDR製品でして、エンドポイント内に潜む脅威の検出、封じ込め、侵害範囲の可視化を行い、迅速なインシデント対応を支援することができます。既存のEPPで取り扱っている高度なエンドポイントデータを用いてEDR機能を実現でき、ESETシリーズの多層防御に、もう1つ高度なレイヤーを簡単に追加できるのです。

具体的なお話をすると、EEIは、ESETのクラウドベースシステムと連携することで、ESET Augur（機械学習エンジン）、ESET LiveGrid（レピュテーション＆フィードバック）、それにESET社の研究者の高い知見という、ESET独自の複合技術を活用することができるようになっています。このうちESET LiveGridというのは、最新の分析結果をリアルタイムで提供するレピュテーションシステムと、疑わしいサンプルをESET社に送信し詳細な分析にかけるフィードバックシステムが組み合わせてあり、世界1億1千万台以上のセンサーから集積されたデータを分析することで、常に最新のデータをもとにしたトリアージを実現します。企業ネットワークとLiveGridの流行度を軸にして、社内とグローバルのギャップを可視化することができます。LiveGrid上の評判や流行度を確認することで、トリアージの判断材料として活用できるので、セキュリティチームの判断のミスを防ぐだけでなくトリアージ時間の節約にも貢献できるのが強みです。



実行ファイルの状態や種類を一覧表示したダッシュボード画面。ここでは「脅威」を示す赤いラベル（赤枠）の「exe1.exe」をクリックすることで、より詳細な情報を確認することができる（下図参照）



「exe1.exe」の詳細画面。ESET LiveGridでのスコアが低く、パネルが赤く表示されている。ほかにも証明書情報や製品情報が不明となっていることから、総合的に見て不審なファイルである可能性が高いことがわかる。

辻氏：EPPと統合されており、最新の情報がわかりやすく可視化されるというのは大きいですね。やはりサイバー攻撃の対策というのは、日頃の準備が8割だと思いますので、まずは自分たちのセキュリティレベルについて知り、把握したうえで、いろいろな意味で準備をしておくことが最も重要でしょう。

西村氏：まったく同感です。平時のときにこそ、何かあった際に自分たちに何ができるのかを考えおくべきでしょうね。たとえば、38℃の熱が出てしまった時のインパクトや対処法も、その人の平熱が何度であるかによって変わってくるはずです。セキュリティ製品についても、普段の自分たちの状態を把握したうえで、選べるようにすることが必要となってくるでしょう。我々としても、製品を提案する際には、そこを大切にしていかねばと、今回の辻さんとのお話からあらためて実感できました。今日はお付き合いいただき、ありがとうございました。

辻氏：こちらこそ、ありがとうございました。

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。

EDR運用監視サービス

製品の詳細情報はこちら

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

ESET Enterprise Inspectorを用いたEDR運用監視サービスです。24時間365日体制で専門のセキュリティエンジニアがESET Enterprise Inspectorのアラートを監視・分析。危険度に応じて速やかにお客さまへ通知します。侵害端末のネットワーク隔離や不正プロセスの強制停止など、インシデントレスポンスの初動対応も行い、セキュリティ侵害を抑制します。

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

2020年11月現在

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

MEDR2011500MUR-655