BlackBerry | CYLANCE

脅威リサーチャーという仕事：前編

セキュリティ最前線で戦うプロフェッショナル

サイバー攻撃が急増する中、マルウェア情報を事前定義するシグネチャ方式のセキュリティ対策では手遅れになるケースが増えています。そこで人工知能（AI）を用いて未知のマルウェアを発見する新たなテクノロジーが登場してきており BlackBerry Cylance はこの分野で先行しています。BlackBerry Cylance の日本法人には、日々登場する新たな脅威をリアルタイムで検出し、世の中に情報を提供したり、対策をアドバイスしたりするプロフェッショナル「脅威リサーチャー」が在籍しています。

最重要インフラとも言えるインターネットの安全を守る脅威リサーチャーという仕事はどのようなものなのでしょうか。セキュリティの最前線で戦う 3 人の脅威リサーチャーに話を聞きました。

BlackBerry Cylance脅威解析チーム
・BlackBerry Cylanceアジア太平洋地域マネージャー　本城 信輔 氏（中央）
・BlackBerry Cylance上級研究員　糟谷 正樹 氏（右）
・BlackBerry Cylance上級主任研究員　長谷川(市田) 達也 氏（左）

脅威リサーチャーの仕事とは

脅威リサーチャーと聞いて、耳慣れないと感じる人も多いと思います。アジア太平洋地域マネージャーを務める本城信輔氏は「世の中に日々発見されるマルウェアをはじめとしたセキュリティの脅威をいち早く発見し、解析する仕事です」と話します。

2018 年 7 月から 8 月にかけて、「PandaBanker」と呼ばれる、情報搾取型のマルウェアを感染させることを狙ったメールがばらまかれたとの新聞報道がありました。11 のクレジットカード会社や銀行系のカード会社など、多数の顧客を持つ企業が標的として狙われました。PandaBanker は、請求書の送付などを装ったメールを経由してパソコンに送り込まれた別のマルウェアが、外部のサーバと通信することで感染します。ブラウザが細工され、標的となる企業のサイトへの接続を検知すると、正規サイト上にカード情報の再登録などを求める偽の画面が表示され、だまされて入力するとその情報が盗まれてしまいます。

クレジットカードの情報が盗まれれば、すぐにでも金銭的な被害が出てもおかしくありません。そうした脅威を世界中で何者かが常につくり出そうとしており、それを未然に、もしくは発生後、迅速に防ぐという大役を担っているのが脅威リサーチャーなのです。

上級研究員を務める糟谷正樹氏は、このバンキング型のトロイの木馬である PandaBanker による脅威が迫っていることを発見しました。新聞社の取材に、メールの添付ファイルを安易に開かないことや本来は不要な部分でクレジットカード番号を求められたら別の端末で接続して確かめるなどの対応をするべきとコメントしています。

糟谷氏によると、脅威リサーチャーの基本的な業務は、検知した脅威ファイルの分類と解析です。そのファイルがマルウェアなのか分析を行い、どの様な悪意のある動きをするのかを見極めます。

「最重要なものは、日本だけでなく世界の担当者が交代で処理する」と糟谷氏。北米、欧州、アジア太平洋地域にいるリサーチャーのうち、日中時間帯の者が対応する「フォローザサン」（太陽に従う）の考え方で、24 時間 365 日の監視体制を敷いています。特に緊急性が高く、アウトブレークの可能性があるマルウェアに関しては米国やヨーロッパのチームと共同で解決に当たります。

BlackBerry Cylance
上級研究員
糟谷 正樹 氏

解析対象になるファイルは「1 日数件、多い時は 10 件ほど。すぐ解析できるものや、いったん簡単な報告をした上でじっくり解析に取り組むものなど様々ありますが、どちらかというと私はマルウェア解析の深堀りを得意とします」（糟谷氏）。マルウェアが作成され即日ばらまかれるケースもあるため、世の中に出回っていない本当に未知のものが見つかることも珍しくありません。基本業務はお客様のための解析ですが、深堀りした脅威をまとめ

て、世の中に脅威情報を発信することも行います。

もう 1 人のリサーチャー、長谷川氏も同様にマルウェアの解析を手掛けている。ただし、糟谷氏のように 1 つの課題を深掘りするというよりは、サイバー犯罪者たちの攻撃をおびき寄せる「おとり」であるハニーポットを仕掛け、幅広く攻撃者の侵入を監視し、動向を調査したり、ハニーポットにかかったマルウェアの挙動を分析したりして、トレンドの先読みを得意とする。

「ハニーポットでの“取れ高”や、世の中から活きた検体を入手できているかを重視しています。誰も持っていないフレッシュな検体を取り、最終的にブログや講演の場などを通じて世の中に周知することで日本のセキュリティ向上に貢献できていると考えると、大きな達成感が得られます」（長谷川氏）

BlackBerry Cylance
上級主任研究員
長谷川 達也 氏

人工知能を駆使したセキュリティソリューション

世界の重要インフラであるインターネットの安全性を守る重要な仕事を担う 3 人の脅威リサーチャー。3 人が所属するセキュリティ企業、BlackBerry Cylance はどんなソリューションを提供しているのでしょうか。

BlackBerry Cylance が提供する CylancePROTECT は、シグネチャやクラウド、レピュテーションルックアップを参照することなく、人工知能、アルゴリズム技術、機械学習を用いて、高い精度でゼロデイマルウェアの攻撃から防御することを強みとしています。従来のセキュリティ対策のほとんどはシグネチャ型と呼ばれるもので、事前に定義した脅威リストを基に検知対象のファイルとのマッチングをします。しかし、近年はゼロデイ攻撃が横行するなど、シグネチャ型の防御では間に合わなくなってきているのが現実です。一方で、AI を活用する BlackBerry Cylance のモデルは、「マルウェアらしさ」をテクノロジーが評価し、亜種や変異型のマルウェアも検出するというまったく異なる仕組みで、悪意のあるプログラムを高い確率で見つけられるのです。

シグネチャベースのセキュリティ企業にも長く在籍していた本城氏は「シグネチャベースの技術に寿命が来ている」と指摘します。従来型のアンチウイルスソリューションは、事後対応的なテクノロジーに依存しています。マルウェア作者が製品による検知テストと改変を繰り返すことによって、検知されないマルウェアを作り出すことは簡単です。シグネチャベースのセキュリティ企業は、検知できなかった検体に対してシグネチャを作るという事後対応に追われます。そのため、悪意のあるマルウェア作成者とそれを検知するセキュリティ企業のイタチゴッコのようなマルウェアの検出作業が続いてしまいます。

しかし、CylancePROTECT は AI(機械学習) を活用し、実行される前に脅威を予測、発見、防御するのです。これにより、マルウェア解析の深掘りやブログでの世の中への周知など、本来やるべき業務に時間を割けるようになったことが 1 つの大きな変化だと 3 人は口をそろえます。

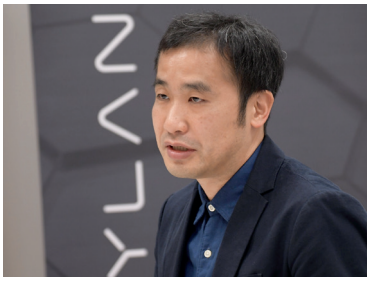
また、多くのセキュリティ企業が、フィリピンやロシアなど 1 カ所のみにアナリストを配置しているのに対して、BlackBerry Cylance は日本を含めて複数の拠点の脅威リサーチャーが連携して活躍していることも特徴的です。

脅威リサーチャーになり、スキルを向上させるには

社会的に大きな存在意義を持つ脅威リサーチャーですが、いったいどのような技術を持つ人が求められ、スキルを向上させているのでしょうか。

本城氏は「最初からマルウェアに関わっている人というのが少ないこともありますが、一般的な IT 技術者の知識をお持ちで、自分で調べて技術を習得するタイプの人であれば十分、脅威リサーチャーの道を目指せるでしょう」と話します。ネットワークや OS などを担当する技術者であればそのノウハウも役立ちます。「何より重要なのはパッションです」と本城氏。難しい解析になるほど燃えるといった好奇心を持ち続ける人に脅威リサーチャーを目指してほしいといいます。

具体的なスキルアップ手段としては、SANS Institute の体系的なトレーニングを受けるのも有力だと糟谷氏は語ります。政府や企業・団体間における研究、及びそれらに所属する人々の IT セキュリティ教育を目的として、1989 年に設立された組織です。



BlackBerry Cylance
アジア太平洋地域マネージャー
本城 信輔 氏

ここまで、セキュリティ業界で注目される脅威リサーチャーの仕事について、3 人のプロフェッショナルに話を聞きました。刻一刻と変わるセキュリティ環境とソリューションの動きをつぶさに追い、対策をすることで、世界中のユーザーを守るという非常に重要な仕事であることが分かります。次回は、3 人がどのようなバックグラウンドを持ち、第一線の脅威リサーチャーとして活躍しているのか、それぞれの経験を詳しく聞いていきます。

(取材・執筆 : 友永慎也)

Cylance Japan株式会社
〒100-6510 東京都千代田区丸の内1-5-1 新丸の内ビルディング10F
www.cylance.co.jp
03-6386-0061 (代表)

BlackBerry | CYLANCE

201908-WP001