共同企画 | 第40回医療情報学連合大会（第21回日本医療情報学会学術大会） | 共同企画
共同企画3
急速に広がるオンライン診療・遠隔医療におけるサイバーセキュリティを考える
2020年11月19日(木) 14:00 〜 16:20 B会場 (コングレスセンター3階・31会議室)

[2-B-2-05] COVID-19の攻撃事例から考えるセキュリティ情報共有の重要性

*林 薫[1] （1. パロアルトネットワークス株式会社）
*Kaoru Hayashi[1] （1. パロアルトネットワークス株式会社）

キーワード：Threat Intelligence, Collaboration, Threat Hunting, Security Operation

新型コロナウイルス感染症（ COVID-19）が世界規模で流行するなか、多くの人々が現状に向き合い、生活の変化を強いられています。それは犯罪者としても同じ事で、彼らは世界中が注目するこのパンデミックに便乗することを選択してサイバー攻撃を開始しています。そのため、 COVID-19をテーマにしたフィッシングやマルウェアの配布、ドメインの悪用による詐欺行為などが世界中で行われています。また、感染症の対応に追われる医療機関を狙った攻撃の増加も確認しています。

攻撃者の視点から見た場合、サイバー攻撃に必要なツールや手法は容易に入手できものばかりであり必要なコストはゼロに近づいています。そのため、年間約1億以上の新しいマルウェアを確認するようになっています。また以前は単独で活動していた攻撃側は組織化することで攻撃を高度化し、成功率を高めています。このようにサイバー攻撃の数や質が変化してきた現在、攻撃が発生してから対応するといったリアクティブな対応では後手に回ってしまいます。プロアクティブに対応するためには、脅威インテリジェンスと呼ばれる情報を活用することが重要となってきます。

Gartnerによる脅威インテリジェンスの定義は「すでに存在する、もしくは今後現れる脅威や危険要素への対応にかかわる意思決定の材料となる、背景、構造、痕跡、影響、実行可能な助言を含む、証拠に基づく知識」となっています。ここで説明されている痕跡(IoC)や影響、そしてそれらに対処するために実行可能な対策について平時から準備する必要があります。こうした情報を活用する際には手作業ではなく、可能な限り自動化を行うことでかかる作業量や人員の増大を抑制することが重要です。さらに脅威情報を組織の枠を超えて同じ業界等で共有することで繰り返されるサイバー攻撃に効果的に対処することができるようになります。

COVID-19 の攻撃事例から考えるセキュリティ情報共有の重要性

林 薫
パロアルトネットワークス株式会社

Importance of Threat Intelligence Sharing in the COVID-19 era

Kaoru Hayashi
Palo Alto Networks

Threats and risks continue to grow, and corporate infrastructure continues to evolve. Organizations have been required to take stronger security in line with the current situation, but the number of organizations that can significantly increase budget and personnel is limited. Therefore, it is necessary to use and share information about attacks called threat intelligence. Threat intelligence is evidence-based knowledge that includes the context, mechanisms, indicators, implications, and actionable advice that can be used to make decisions. By gathering and analyzing information about the threats you face, you can create and share threat intelligence with particular group, such as ISAC. That means you can fight attackers with other organizations. In addition, security measures can be proactively implemented, and zero trust architecture can be introduced by leveraging threat intelligence. In particular, threat intelligence can be utilized in security operations, IoC(Indicator of Compromise) can be automated and detect threats, and other information can be used with EDR/XDR to find attackers lurking in the organization by threat hunting.

Keywords: Threat Intelligence, Collaboration, Threat Hunting, Security Operation

1. 緒論

新型コロナウイルス感染症（COVID-19）が世界規模で流行するなか、多くの人々が現状に向き合い、生活の変化を強いられている。それは世界中のサイバー犯罪者としても同じ事で、彼らはこのパンデミックに便乗したサイバー攻撃の活動を早い段階から開始しており、彼らが取得した COVID-19 をテーマにしたリスクの高いドメインはすでに四万を超えている。[1] また、COVID-19 やその関連情報といったフィッシングメールは世界中で観測されているが、その対象には感染症への対応で重要な役割を果たす政府医療機関、地方自治体、医療センターを持つ大学、研究機関などの組織も多く含まれている。[2]

ここで述べたようなサイバー攻撃の増加は COVID-19 を契機とした一時的なものではなく、過去10年以上継続している傾向であることはデータにより確認できる。例えばドイツの AV-TEST によれば、2011 年には延べ 6500 万のマルウェアが確認されていたが、2019 年にはその数は 10 億を超えており、増加傾向の歯止めがかかる兆候はみられない。[3]

企業は利便性やイノベーションのためインフラの改革に投資を行っている。これまでのオンプレミスやデータセンターに加え、クラウド利用や IoT の活用、在宅勤務をはじめとするモバイルユーザの増加などである。しかし企業インフラが複雑化することでガバナンスの低下やリスクの顕在化も生み出すこととなった。

防衛する側の組織はこうした現在の状況に即したより強固なセキュリティ対策が必要となってきたが、予算や人員の大幅な増加が可能な組織は限られている。こうした拡大するサイバー攻撃と変化する環境がもたらすリスクから組織を防御するため、脅威インテリジェンスと呼ばれる攻撃に関する情報の利用と共有が必要となっている。本稿では脅威インテリジェンスの定義、必要性、利用方法、生成と共有について述べる。

2. 脅威インテリジェンスの定義と必要性

ガートナーによると脅威インテリジェンスとは、“すでに存在する、もしくは今後現れる脅威や危険要素への対応にかかわる意思決定の材料となる、背景、手順、痕跡、影響、実行可能な助言を含む、証拠に基づく知識” [4]（筆者訳）とある。単なる事実の羅列ではデータでしかないが、インテリジェンスは脅威や攻撃に関する情報を収集し分析した上で5つの要素から構成され、意思決定に利用できる形にしたものである必要がある。

次に脅威インテリジェンスが必要な理由を3点述べる。

2.1 他組織との協力

サイバーセキュリティを「攻撃からの防御」という観点で考えた場合、防御の主体は自組織になる。しかし攻撃を行う攻撃者は不特定多数であり、攻撃が起きるタイミングも場所も不明なため防御側が圧倒的に不利である。これを打破するには、単独で闘うのではなく他組織と協力することが効果的である。協力する方法はいくつかあるが、脅威インテリジェンスの共有を行うことで不明の攻撃者に対して他組織と共闘することができるようになる。具体的にはグループ会社やサプライチェーン、ISAC のように業界内で専門組織を設立するケースなどである。

脅威インテリジェンスにはオープンソースと呼ばれる無料で公開されているものや、ベンダーによって販売されている有償フィードもあり、これらも必要に応じて利用することで外部専門家の知見を活用することが可能である。

2.2 プロアクティブな対応

多くの脅威インテリジェンスはすでに発生した攻撃について分析したものであるため、これを利用することは「攻撃から防御を知る」ことができるようになる。先に述べた脅威インテリジェンスを構成する五つの要素のうち、手順や痕跡を手がかりに自組織を調査することで同様の攻撃を受けていないか確認することができる。また、助言なども利用し自組織の対応能力の再検討を行った上でセキュリティ体制を改善することも可能になる。その際、背景や影響などから優先度を決定することができる。攻撃を実際に受ける前や被害に気づく前に脅威インテリジェンスを利用してプロアクティブな対応することが可能になる。

2.3 ゼロトラストの導入

前章で述べたように、脅威は拡大を続け、企業のインフラ

は肥大化を続けているため、多くの組織はこれまでのセキュリティ対策ではリスクの低減が思うように進まなくなっている現実に直面している。そのため、大きなセキュリティ戦略の変革の必要性からゼロトラストという考え方がセキュリティの中で広まってきている。従来、信頼できないインターネットから信頼できる内部ネットワークを境界で防御するという境界型セキュリティが大勢を占めていたが、境界を超えて侵入された事例が後を絶たないことや、内部犯によるインシデントの発生など、組織内部のネットワークであっても信頼できないという考えが浸透するようになってきた。そのため、場所を問わず「アクセス毎に必ず検証する」というゼロトラストの導入を検討する組織が増えてきている。

米国では各省庁の最高情報セキュリティ責任者の連絡機関である CIO 協議会が米国国立標準研究所（NIST）に対してゼロトラスト に関する標準化の定義と開発要請をしている。これを受け 2020 年 8 月に発行した NIST Special Publication 800-207 Zero Trust Architecture では、”ゼロトラストがサイバーセキュリティにおけるパラダイムの変革”（筆者訳）であると述べられている。[5)]

ゼロトラストではリソースへのアクセスを検証する際、様々な情報ソースを利用して許可すべきかどうか判断するが、その情報ソースの一つに脅威インテリジェンスが含まれている。

3. 脅威インテリジェンスの利用法

組織の防衛には、セキュリティ態勢の構築と、セキュリティ運用という2つの観点がある。その双方に脅威インテリジェンスは貢献する。

セキュリティ態勢の構築とは防衛能力の準備のことであり、セキュリティ戦略方針の策定、セキュリティ組織の構築や人の配置、ポリシーやプロセスの決定、セキュリティ製品の導入と設定などによって作られる。前章で述べた通り、すでに発生している攻撃から防御を知ることで自組織の能力の改善を行うことができる。また脅威インテリジェンスを組み込んだゼロトラストネットワークを導入することでデータ侵害を防ぐためのより強固な体制を築ける。

セキュリティ運用とは実際に準備された環境を使って防衛をおこなっていくことであるが、ここでも脅威インテリジェンスが有効に活用できる。特に脅威インテリジェンスの要素である痕跡は IoC (Indicator of Compromise)とも呼ばれ、ドメイン名や IP アドレス、ファイルハッシュなど機械処理が容易なデータ形式であり、セキュリティ製品等と組み合わせて検出と防御の自動化が行える。

セキュリティを強化しても監視の目を逃れ侵入する攻撃者を追跡するために、脅威インテリジェンスの中の手順と呼ばれる情報を利用する。これは攻撃者が攻撃を実行する際の TTP、すなわち戦術 (Tactics)、テクニック (Technique)、手続き (Procedure)と呼ばれる情報で、攻撃者のふるまいに関する分析情報である。攻撃者やマルウェアのふるまいを端末上で記録し検出するソフトウェアとして EDR (Endpoint Detection and Response) と呼ばれる製品や、端末上のふるまいに加えネットワーク上でのふるまいやネットワークトラフィックの分析情報と突合して検出精度を高めた XDR (Extended Detection and Response) という製品がある。こうした EDR や XDR と脅威インテリジェンスを利用することで組織に潜む高度な技術を持った攻撃者を検出することが可能になる。

4. 脅威インテリジェンスの生成と共有

外部の脅威インテリジェンスを収集しセキュリティ向上のために利用するだけでなく、自組織で観測した情報の収集と分析から脅威インテリジェンスを生成し活用することは自らが直面する課題を理解し、適切な対策を立てるためにも重要である。これは経営層が必要とする中長期的なセキュリティ戦略や投資計画に利用できるため、技術面だけでなく、マネージメントの観点からの分析が必要な場合がある。こうした脅威インテリジェンスの生成には、民間だけでなく軍や法執行機関に広く採用され確立されたインテリジェンスサイクルを利用する（図1）。[6)]

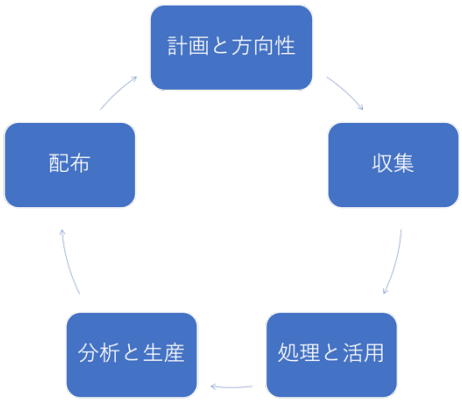

図 1　インテリジェンスサイクル

脅威インテリジェンスの生成はまず計画と方向性の段階でプライオリティとミッションを設定し、必要なデータと能力を定義する。データはすでに利用している SIEM、ファイアウォール、EDR や XDR といったセキュリティ製品からの情報を利用し、外部ソースのデータを利用し情報を豊かにしていく。こうして収集した情報を可能な限り自動化したワークフローで処理・活用する。分析のフェーズではノイズを除去し重要なものを明確化したインテリジェンスを生成する。その際、誰がこのインテリジェンスを利用するのか、適切な時期に配布できるかといったことに注意する。

生成された脅威インテリジェンスはグループ会社や ISAC など必要に応じて外部と共有する。現代の攻撃は単発で終わるものだけでなく、サプライチェーンや業界を横断的に攻撃してくるケースもあるため、グループ企業や業界が共有された脅威インテリジェンスで対策できる状態になれば、自組織のリスクも低減できる。共有する際の注意点として、信頼関係がある相手であるか、一定程度のフリーライダーを許容できるか、共有したインテリジェンスが適切に処理される形であるか、を検討する必要がある。

5. 結論

企業がとりまく脅威と環境は急速に変化しており、特に攻撃が巧妙かつ激化しているため、限られた人員と予算で対応するにはなんらかのパラダイムシフトが必要となる。十分な自動化をともなった脅威インテリジェンスの活用と共有は、現在まで投資してきたセキュリティ資産と人を活用し、プロアクティブな対応へ移行することで早期に攻撃を発見し組織のデータ侵害リスクを低減することが可能となる。

参考文献

1) Janos S, Zhanhao C, Oleksii S, Netanel R, Adrian M. 新型コロナウイルス感染症につけこむサイバー攻撃者たち：関心の高いドメイン名登録で収益化. パロアルトネットワークス株式会社, 2020. [https://unit42.paloaltonetworks.jp/how-cybercriminals-prey-on-the-covid-19-pandemic/ (cited 2020-Aug-28)].

2) Peter R. 脅威攻撃グループ SilverTerrier による新型コロナウイルスをテーマにしたビジネスメール詐欺の手口. パロアルトネットワークス株式会社, 2020. [https://unit42.paloaltonetworks.jp/silverterrier-covid-19-themed-business-email-compromise/ (cited 2020-Aug-28)].
3) AV-TEST ORG. Malware Statistics & Trends Report. AV-TEST GmbH, 2020. [https://www.av-test.org/en/statistics/malware/ (cited 2020-Aug-27)].
4) Rob M. Definition: Threat Intelligence. Gartner, 2020. [https://www.gartner.com/en/documents/2487216/definition-threat-intelligence (cited 2020-Aug-27)].
5) Scott R, Oliver B, Stu M, Sean C. Zero Trust Architecture. National Institute of Standards and Technology, 2020. [https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf].
6) マーク・M・ローエンタール. インテリジェンス 機密から政策へ 慶應義塾大学出版会, 2011; 81-104