2020 年 3 月 26 日

フォーティネットジャパン株式会社

米国時間 2020 年 2 月 26 日に発表されたプレスリリースの抄訳です。

グローバルな脅威トレンドから明らかになった サイバー犯罪者の政治的意図と経済的目的

～FortiGuard Labs のフォーティネット脅威レポートが、国家間を行き交うスパムのトラフィックフローや大統領選挙妨害ビジネスの現状に関する新たな視点を公開～

幅広い適用領域で（Broad）システム連携し（Integrated）自動化された（Automated）サイバーセキュリティソリューションの世界的リーダーであるフォーティネット（Fortinet®、NASDAQ: FTNT）は本日、最新のグローバル脅威レポートの研究結果を発表しました。

- 2019 年第 4 四半期の研究調査からは、サイバー犯罪者がデジタルインフラストラクチャ全体であらゆる攻撃の機会を狙っているだけでなく、さらなる成果の達成のためにグローバル経済や政治の状況を最大限に活かそうとしていることが明らかになっています。
- グローバルなトレンドは、脅威の検知率と検知件数が地域で異なる可能性を示していますが、攻撃の巧妙化と自動化のレベルは地域を問わず一貫しています。さらに、脅威がかつてないほど急速に拡大しているため、サイバーセキュリティ対策に優先して取り組むことが世界中で急務となっています。
- このレポートの詳細と重要なポイントについては、フォーティネットセキュリティブログをご参照ください。また、本レポート（日本語）の全文は、こちらでご覧いただけます。

本レポートのハイライト

1）あまりチャーミングではない子猫（Charming Kitten）の問題：調査によると、2019 年第 4 四半期は複数の地域で Charming Kitten に関連する相当量の活動が確認されました。Charming Kitten とは、イランとつながりのある APT（高度な継続的脅威）集団です。2014 年頃から活動を続けているこの集団は、現在まで数多くのサイバースパイ活動に関与しています。

最近では、米国の大統領選挙に関連した特定のメールアカウントに対する一連の攻撃との関係が指摘されており、Charming Kitten が選挙妨害ビジネスにまで手を伸ばしていることを示唆しています。さらに、Charming Kitten が標的を欺いて機密情報を提供させる 4 つの新しい戦術を採用していることも確認されています。

2）悪化する IoT デバイスのセキュリティリスク：IoT デバイスは、依然として脆弱性のあるソフトウェアの問題に直面しており、これらの脅威が無線 IP カメラなどの思いも寄らないデバイスにまで影響を及ぼす可能性があります。この状況が悪化するのは、さまざまなブランド名で（時には異なるベンダーによって）販売されている商用デバイスにコンポーネントやソフトウェアが組み込まれている場合です。そうしたコンポーネントやサービスの多くは、さまざまな共通のソースに含まれる事前作成されたコードの断片を使用してプログラミングされています。これらの共通コンポーネントや過去に開発された古いコードはエクスプロイトに対して脆弱な場合があります。これが、幅広いデバイスで同じ脆弱性が繰り返し出現する理由です。デバイスへのパッチ適用が容易ではないことに加え、その規模の大きさが問題をますます深刻にしており、サプライチェーンのセキュリティの難しさが浮き彫りになっています。パッチに対する認識不足やパッチの提供不足、一部の IoT デバイスにおける脆弱性の検知率、そしてデバイスを「奴隷化」しようとする IoT ボットネットの試みが要因となり、これらのエクスプロイトはこの第 4 四半期に IPS による検知件数が第 3 位を記録しました。

3）新参の脅威を支援する古参の脅威：常に新しい脅威の一歩先を行かなければならない組織は、古いエクスプロイトや脆弱性に有効期限などないことを忘れがちです。そして、攻撃者は古い脅威であってもそれらが機能する限り使用し続けます。その分かりやすい例が EternalBlue です。このマルウェアは、一般的な脆弱性や重大な脆弱性を悪用するように時間をかけて改良されてきました。EternalBlue は、WannaCry および NotPetya ランサムウェア攻撃をはじめとする数多くの攻撃で使用されています。また、昨年 5 月 BlueKeep のパッチが公開されました。BlueKeep は、悪用されると「ワーム」の特性を発揮することがあり、WannaCry や NotPetya と同じ速度と規模で拡散する可能性があります。そして 2019 年第 3 四半期には、脆弱性「BlueKeep」を悪用する機能を追加した EternalBlue ダウンローダートロイの木馬の新バージョンが登場しました。現在実環境に出回っているバージョンは完成版ではないため、幸いにもロード前に標的のデバイスがクラッシュします。しかし、これまでのマルウェアの開発サイクルを踏まえれば、強い決意を持ったサイバー犯罪者が近い将来にこのマルウェアパッケージの機能を改良して、深刻な被害をもたらすバージョンを完成させることになると考えらえれます。また、BlueKeep のパッチが 2019 年 5 月に公開されているにもかかわらず、極めて多くの組織が脆弱

なシステムを未だ更新していません。EternalBlue と BlueKeep に対する攻撃者の関心が持続し、進化していることから、どちらの脅威についてもシステムへの適切なパッチの適用とセキュリティの確保が不可欠であることをあらためて意識しなければなりません。

4）トレンドで浮き彫りになった、国家間を行き交うスパムのトラフィックフローの現状：これまでと同様、スパムは組織と個人が共に対処しなければならない大きな課題です。この第 4 四半期のレポートでは、国家間のスパムトラフィックの流量、さらにスパムの送信量と受信量の比率を示すデータを組み合わせることで、長く継続しているこの問題を視覚化し、新たな視点を提供します。スパムの大半は、経済的トレンドと政治的トレンドに左右されているようです。たとえば、米国にとって最も量が多い「スパムの取引相手」は、ポーランド、ロシア、ドイツ、日本、ブラジルなどの国々です。また、送信されたスパムの量を地域別に見てみると、東ヨーロッパが世界最大のスパムの生産国であることが分かります。それ以外でアウトバウンドのボリュームが多いスパムの大半は、アジアの各地域を送出元とするものです。ヨーロッパのその他各地域が、スパムの流量がマイナス（送信量よりも受信量のほうが多い）の地域の上位を占めており、アメリカ大陸とアフリカがそれに続きます。

5）サイバー犯罪者を追跡して次の展開を予想する：ある地域で検知された IPS トリガーを見ると、標的になっているリソースを確認できるだけでなく、今後サイバー犯罪者が注目する可能性のあるものが示唆されることがあります。これは、一定数の攻撃が成功した、あるいは単に一部の地域に特定の種類のテクノロジー多数導入されたという要因に基づいています。しかしながら、そうではない場合もあります。たとえば、shodan.io によれば、ThinkPHP の大部分は中国で導入されており、インストール数は米国の 10 倍近くに達します。各地域の企業がほぼ同じ割合でソフトウェアにパッチを適用していると仮定した場合、ボットネットがエクスプロイトを展開する前に ThinkPHP の脆弱なインスタンスを探っているだけなのであれば、APAC 地域で検知されるトリガー数ははるかに多くなるはずです。ところが、最近のエクスプロイトによって APAC 全域で検知された IPS トリガーは、北米と比べてわずか 6%しか多くありません。つまり、これらのボットネットが、発見したすべての ThinkPHP インスタンスにエクスプロイトを展開しているだけであることを意味します。さらに、マルウェアの検知数を同様に見てみると、組織を標的とする脅威の大半は VBA（Visual Basic for Applications）マクロであることがわかります。これは、VBA マクロが今なお効果的な標的で、攻撃者にメリットをもたらすためだと考えられます。一般に、機能していないものの検知数が多い状態は長くは続きません。何かが大量に検知されている場合、誰かがその攻撃の被害者になっているといえます。

幅広い適用領域で（Broad）システム連携し（Integrated）自動化された（Automated）セキュリティの必要性

アプリケーションが急増し、数多くの接続デバイスによって境界が拡張されるに伴って、管理と保護を必要とする数十億の新たなエッジが誕生しています。さらに組織は、拡大を続けるデジタルインフラストラクチャを標的とする攻撃が、人工知能や機械学習の活用などによって高度化しているという問題にも直面しています。分散ネットワークを効果的に保護するには、セキュリティの境界のみに限定した保護から、自社の新しいネットワークエッジ、ユーザー、システム、デバイス、および重要なアプリケーションに分散されているデータの保護へと移行する必要があります。デジタルイノベーションによって急速に進化する今日のネットワークを保護できるのは、デバイス、ユーザー、モバイルエンドポイント、マルチクラウド環境、SaaS インフラストラクチャを含む攻撃対象領域全体で、包括的な可視化と保護を実現するように設計されたサイバーセキュリティプラットフォームだけです。

FortiGuard Labs のグローバルセキュリティストラテジスト、Derek Manky（デレク・マンキー）は、次のように述べています。

「サイバースキルギャップの深刻化、デジタル攻撃対象領域の拡大、そして疑いを持たない個人ユーザーに対するソーシャルエンジニアリングなどを駆使した不意打ちの成功などの要因で、サイバーセキュリティをめぐる攻防戦においては明らかに犯罪コミュニティが優位に立つ場面が多くなっています。巧妙化と自動化が進む脅威に対して組織が優位性を維持するためには、攻撃に使用されているものと同じテクノロジーと戦略をネットワーク保護に活かす必要があります。つまり、AI ドリブンの脅威インテリジェンスとプレイブックが備える能力とリソースを活用する統合プラットフォームを採用することで、デジタルインフラストラクチャ全体の保護と可視化が実現することを意味します」

レポートの概要

この最新のフォーティネット脅威レポートは、2019 年第 4 四半期にフォーティネットのさまざまなセンサーを駆使して世界中で観察された数十億件もの脅威イベントに基づく、FortiGuard Labs の脅威インテリジェンスを説明するものです。グローバルおよび地域別の視点に加えて、脅威動向の中心的かつ補足的な 3 つの側面であるエクスプロイト、マルウェア、ボットネットに関する調査を網羅しています。

FortiGuard Labs について

FortiGuard Labs は、グローバルな脅威インテリジェンスを提供するフォーティネットの調査研究組織です。悪意のあるサイバー攻撃からの保護に不可欠なグローバル脅威インテリジェンスおよびコンテキスト分析を提供することをミッションとしています。その実現のため、FortiGuard Labs は世界 31 ヵ国に 200 人を超える脅威研究者とアナリストを擁しており、業界で最も効果的で実績のある人工知能（AI）および機械学習（ML）システムの 1 つを利用しています。このプラットフォームは毎日約 100 億件のイベントを分析しており、フォーティネット製品向けに最新の実用的な脅威インテリジェンスを生成し、お客様に最新の脅威特定情報と保護対策を提供し続けています。さらに、セキュリティインテリジェンスに関する 200 件以上のパートナーシップやコラボレーションを通じて、統合脅威インテリジェンスエコシステムを維持する役割を担っています。業界をリードする研究者とアナリストのチーム、その優れた性能が実証されている革新的な AI / ML システム、そして広範なセキュリティインテリジェンスのエコシステムが一体化することによって、フォーティネットは最先端の脅威検知能力を活用し、お客様そしてパートナー各社を確実に保護します。詳細は、フォーティネットの Web サイト、ブログ、FortiGuard Labs の脅威インテリジェンスをご覧ください。

フォーティネットについて (www.fortinet.com)

フォーティネット（NASDAQ: FTNT）は、世界中の大手企業、サービスプロバイダ、そして政府機関を守っています。フォーティネットは、拡大するアタックサーフェス（攻撃対象領域）に対するシームレスな保護とインテリジェンスを提供し、外部との明確な境界が消滅したネットワークでの、増え続けるパフォーマンスの条件に応じるパワーで、現在もまた将来も、お客様に貢献します。ネットワーク上でも、アプリケーションやクラウド、またはモバイル環境であっても、妥協することなく、極めて重大なセキュリティ上の問題に対応するセキュリティを提供できるのはフォーティネットのセキュリティ ファブリックのアーキテクチャだけです。フォーティネットは世界で最も多くのセキュリティアプライアンスを出荷し、世界 440,000 以上のお客様がビジネスを守るためにフォーティネット に信頼を寄せています。フォーティネットのネットワークセキュリティエキスパート(NSE)インスティチュートは、テクノロジーカンパニーとしても、ラーニングカンパニーとしても業界で最も大きく広範なサイバーセキュリティのトレーニングプログラムを有しています。フォーティネットジャパンについては、www.fortinet.com/jp をご覧ください。