WHITE PAPER

2021 年のサイバー脅威予測

FortiGuard Labs による年次予測

はじめに

毎年この時期には、テクノロジー環境のトレンドに注目することで我々が近い将来直面することになるセキュリティの問題を予測しています。セキュリティ脅威のトレンド予測は、科学より芸術に近いようにも思えますが、実際には脅威がどのようにして開発され、サイバー犯罪者がどのテクノロジーに（利用と悪用という両面で）注目しているかを十分に理解した上で、進化するビジネスのトレンドや戦略を加味することで、今後の方向性を予測するものです。

ただし、そのためには何年もかけてサイバー犯罪者の活動や行動を特定して評価し、法執行機関による犯罪者の追跡と逮捕に積極的に協力して、不正行為を阻止する戦略を構築する必要もあります。FortiGuard Labs のサイバーセキュリティ脅威の研究者は、20 年間にわたりそのような努力を続けてきました。細かい点での変化はおそらくあるものの、経験というレンズを通して見れば、攻撃パターンや犯罪行為、目的に大きな変化はありません。これらの予測可能な行動とテクノロジーのトレンドをマッピングすることで、組織がどのような備えによって接続されたリソースを将来のサイバー攻撃から保護する必要があるのか、重要かつ実用的なインテリジェンスを得ることができます。具体的には、データや知的財産の盗難、進化するランサムウェアの手口、デバイスを感染させる方法、ソーシャルエンジニアリング、その他の新たに生み出されるデジタル脅威などが含まれます。

サイバー犯罪者は多くのリソースを投入し、リモートワーカーやクラウドなどの新しいネットワークエッジ環境を標的にし、悪用するようになっています。

この年次予測レポートでは、数年前からランサムウェアの進化やデジタルビジネスの拡大に伴うリスク、さらにはコンバージドテクノロジー（中でも特にスマートビル、都市、重要インフラストラクチャなどのスマートシステムの一部であるテクノロジー）を標的にする攻撃などの多くの問題を取り上げてきました。また、形を変えて進化するマルウェア、スウォームベースの攻撃[1]、人工知能（AI）や機械学習（ML：Machine Learning）の武器化についても紹介してきました。これらの一部はすでに現実のものになっており、実現への道を着実に進んでいるものもあります。組織がこれらの脅威に先行するには、2 つのこと、すなわち 1 つ目には進行中のトレンドを把握すること、2 つ目には新たな脅威から自らを保護するための準備を今から始めておくことが必要です。

エッジの台頭

この数年間でネットワークは大きな変化を遂げました。つまり、従来のネットワーク境界が LAN（ローカルエリアネットワーク）、WAN（広域ネットワーク）、マルチクラウド、データセンター、リモートワーカー、IoT（モノのインターネット）、モバイルデバイスなどの複数のエッジ環境に置き換えられましたが、それぞれに固有のリスクと脆弱性が存在します。サイバー犯罪者にとっての最大の旨味の 1 つは、これらすべてのエッジが相互接続されている一方で、アプリケーションやワークフローが複数の環境に関係していたり、複数の環境間を移動したりすることが多いため、多くの組織が一元的な可視性と統一された制御よりもパフォーマンスや俊敏性を優先してしまっている点にあります。

サイバー犯罪者は、コアネットワークだけでなくリモートワーカーやクラウドなどの新しいネットワークエッジ環境を標的にし、悪用する攻撃に多くのリソースを投入するようになっています。新しいテクノロジーやコンバージングシステムを始めとするこれらの新しい環境の保護は、想像以上の困難を伴います。たとえば、リモートワークへの移行は、ネットワークにリモート接続するエンドユーザーやデバイスが増えるだけではありません。リモートワークを始めたばかりのユーザーや脆弱なデバイスを標的とする攻撃の急増は想定内でしたが、接続されたホームネットワークを標的とする新たな攻撃も確認されるようになりました。それらの攻撃の多くは、家庭用のルーターやエンターテインメントシステムなどの古い脆弱なデバイスを集中的に悪用しようとするものです。その一方で、一般家庭の環境に接続された、複数のデバイスやシステムを連携させるスマートシステムを標的にする新たな攻撃も始まっています。

AI ベースのバーチャルアシスタントを始めとする対話型のスマートデバイスは、ユーザーに関する大量の情報を収集して保存します。これらのデバイスを攻撃すれば、ソーシャルエンジニアリングを使った攻撃を高い確率で成功させる貴重な情報が手に入ることもあります。そして、これらのデバイスが生活の多くの要素を制御するようになると、そのシステムへの攻撃が成功することでセキュリティシステムをオフにしたり、カメラを無効にしたり、スマート家電を乗っ取って身代金を要求するといった行為へと発展する危険性があります。

しかしながら、それはほんの始まりに過ぎません。エンドユーザーとその自宅のリソースは、詳細情報を悪用する目的で攻撃される可能性がありますが、より高度な攻撃者はこれを次の段階に進む足掛かりとして使用します。リモートワーカーの自宅のネットワークを起点とする企業のネットワークに対する攻撃は、特にその企業の利用トレンドを確実に把握されてしまった場合、疑いを持たれることなく慎重に連携しながら進行する可能性があります。保存された接続データにアクセス可能なインテリジェントなマルウェアは、自らの行動を隠すことが容易になります。それだけではありません。高度なマルウェアが新しい EAT（Edge Access Trojans：エッジにアクセスするトロイの木馬）を使用してデータをスニッフィングし、ローカルネットワークから音声要求を傍受してシステムを侵害したり、コマンドをインジェクションしたりする可能性もあります。Go のようなプログラミング言語を使用して EAT の脅威にクロスプラットフォームの機能が追加されると、基盤の OS に関係なくデバイスからデバイスへと移動できるため、EAT がさらに危険なものになります。

高度なマルウェアが新しい EAT（Edge Access Trojans：エッジにアクセスするトロイの木馬）を使用してデータをスニッフィングし、ローカルネットワークから音声要求を傍受してシステムを侵害したり、コマンドをインジェクションしたりする可能性もあります。Go のようなプログラミング言語を使用して EAT の脅威にクロスプラットフォームの機能が追加されると、基盤の OS に関係なくデバイスからデバイスへと移動できるため、EAT がさらに危険なものになります。

大規模の組織の豊富なセキュリティリソースとの競争という点で、サイバー犯罪者は不利な立場にあります。サイバー犯罪を成功させるには、簡単に入手可能なリソースを攻撃者が活用する必要がありますが、特に 5G やそれ以降のテクノロジーの普及によって、これらのエッジデバイスも ML に活用されるようになるでしょう。エッジデバイスの処理能力を乗っ取ることができれば、サイバー犯罪者が大量のデータを密かに処理し、エッジデバイスがいつどのように使用されるか把握可能となり、エッジデバイスを攻撃すれば、従来のモノリシックシステムよりもはるかに効果的にクリプトマイニングを実行できます。感染した PC ノードの処理リソースが乗っ取られると、CPU の使用率が高くなってエンドユーザーのワークステーションにそのまま反映されるため、多くの場合はすぐに特定されてしまいますが、二次的なデバイスであれば、感染させても気付かれる可能性は極めて低くなると考えられます。したがって、エッジデバイスやエッジネットワークの数が拡大して企業ネットワークにおいて重要な役割を果たすようになる中では、これらのデバイスの他のヘルス指標の可視性がさらに重要になります。ところが多くの組織では、エッジコンピューティング戦略を導入するまでにその基盤となるデバイスがすでに侵害されてしまっているのです。

5G 対応デバイスを攻撃して悪用することは、高度な脅威の新たな機会をもたらすことにもなります。ここ数回の本レポートでは、スウォームベースの攻撃の開発と展開が進んでいる現状を解説してきました。スウォーム（群）攻撃は、何千ものデバイスを乗っ取り、専門スキル別にサブグループに分けて悪用します。ネットワークやデバイスを統合システムとして標的にし、リアルタイムで情報を共有することで**攻撃の進行中に**能力が強化され、結果として攻撃の有効性も向上します。スウォームテクノロジーには、個々のスウォームボットに処理能力を提供し、スウォームの異なるメンバー間で効率的に情報を共有するための大量の処理能力が必要です。これによって脆弱性を迅速に発見して共有し、関連付けることが可能となり、攻撃手法をさらに発展させて一層効果的に脆弱性を悪用できるようになります。また、これらのネットワークの処理能力を活用することで AI ベースのシステムを実現し、協調型の攻撃を通じて短時間で攻撃および検知回避の効率と効果を高めることもできます。

これをすべて実現するには、AI を次世代へと進化させる必要があり、ML を利用したローカルの学習ノードの活用も重要です。またこれらのノードには、分析や行動の機能だけでなく、発見した情報を相互にやり取りしたり更新したりする能力も必要になります。こうした AI の進歩は、すでに始まっています。我々は、エッジデバイスを標的として攻撃するサイバー攻撃者を手助けする、オープンソースのツールキットが増加するものと予測しています。これらのツールを利用することで、サイバー犯罪者は侵害されたデバイスのアドホックネットワークを簡単に作成して管理し、大量の処理能力を瞬時に手に入れられるようになります。結果として、より効率的に攻撃を仕掛け、セキュリティシステムを突破し、対策を回避できるようになることが考えられます。資金力のあるサイバー犯罪組織であれば、高度な AI を追加して防御側の戦略を検知し、防御策に打ち勝つこともできるようになるでしょう。さらには、侵害されたエッジデバイスのネットワークが、サービスとして販売される例も増加することが予想されます。このような不正エッジネットワークを悪用すれば、情報の処理や標的に関する情報の収集、さらには防御を突破するためにできるだけ多くの攻撃ベクトルを同時に標的にする協調型攻撃の実行も可能になると予測されます。

我々は昨年、5G の登場が実用的なスウォームベース攻撃が開発される最初の転機となる可能性があると予測しました。また、情報とアプリケーションの共有や処理を高速実行できるアドホックネットワークをローカルに構築することで、これが可能になるとも予測しましたが、現在はその予測がさらに現実に近づいているようです。たとえば米国では、基本的な 5G カバレッジ（建物を貫通し、長距離をカバーするのに有効な 600 MHz 周波数帯）を、5,000 都市の 2 億人以上が利用できるようになっています。また、はるかに高速なミリ波の 5G の展開も 6 つの都市を皮切りに始まっており、さらに多くの都市でも展開が予定されています。MIMO（Massive Multiple-Input Multiple-Output）テクノロジーなどの新たな進歩によって、モバイル化が高度に進んだ環境の無線端末に対しても優れたサービスを安定して提供できるようになりました。そして今、5G 対応の新しいスマートフォンへの 5G mmWave アンテナの搭載が開始していることで、その動きがさらに加速しています。

サイバー犯罪者が、このことが持つ意味やエクスプロイトの機会を見逃すはずがありません。5G とエッジコンピューティングの武器化によって、侵害されたデバイス各々が悪意のあるコードの攻撃経路となるだけでなく、デバイス群が連携して 5G の速度で標的を攻撃することもできます。接続されたバーチャルアシスタントや同等のスマートデバイスから提供されるインテリジェンスが追加されれば、速度、インテリジェンス、各国語対応といった特性によって、従来型のセキュリティテクノロジーを難なく突破できる可能性もあります。

5G とエッジコンピューティングの武器化によって、侵害されたデバイス各々が悪意のあるコードの攻撃経路となるだけでなく、デバイス群が連携して 5G の速度で標的を攻撃することもできます。

攻撃のリスク：AI ベースで攻撃を予測する（あるいはセキュリティシステムを突破する）プレイブックの急増

AI とプレイブックの融合で攻撃を予測

AI への投資は、タスクの自動化だけでなく攻撃発生の前後に自動化システムによる攻撃の調査と検知も可能にします。中でも最も興味深いサイバーセキュリティ戦術の 1 つが、攻撃やサイバー犯罪組織の行動を詳細に記述したプレイブックの開発と使用です。

今日、AI や ML のシステムがネットワークで大きな役割を果たすようになり、そういったプレイブックの構築と導入の実現へと大きく近づいています。MITRE ATT&CK フレームワークなど、行動や方法論の文書化と標準化のための様々なスキームを採用した基礎的なプレイブックが、FortiGuard Labs をはじめとするいくつかの脅威研究機関によってすでに作成されています。脅威インテリジェンス機関が提供するこれらの脅威の「フィンガープリント」や TTP（戦術、技術、手順）を AI システムにフィードすることで、攻撃パターンを検知し、攻撃シーケンスの次のステップを予測してシャットダウンすることで攻撃を中断させることができます。

この情報が AI 学習システムに追加され、訓練された ML システムによって強化されれば、ネットワークは実際に攻撃が進行するのを待つことなく効果的に脅威にレスポンスできるようになります。ネットワークのエッジや、時にはネットワークの外に偵察センサーとして置かれたリモート学習ノードによって、高度でプロアクティブな保護が提供され、脅威を検知しサイバー犯罪者やマルウェアの動きを予測して事前に対策を講じることができるようになるでしょう。また、他のノードと連携し、これまでに手に入れることができなかった攻撃コードの成果物、コンパイラの振る舞い、シンボル、APT（高度な持続的脅威）グループに特有のスタイルなどの攻撃プロファイルを同時に検知することで、攻撃のすべての手段を遮断することもできます。

サイバー犯罪者の攻撃パターンや悪意のある振る舞いの詳細、すなわち TTP をプレイブックに反映させることで、脅威へのレスポンスを強化し、攻撃シミュレーションを生成してサイバーセキュリティのプロフェッショナルのスキルを強化できます。このような防御側チームのトレーニングによって、ネットワークのロックダウンと並行してセキュリティチームのメンバーのスキル向上を図ることができます。また組織においても、リアルタイムのサイバーリスクのグラフィック表示である現在活動中の脅威のヒートマップに注目することで、インテリジェントシステムでネットワークトラフィックやターゲットをプロアクティブに難読化し、予測される攻撃経路に魅力的なおとりを正確に仕掛けてサイバー犯罪者を誘い込むことができます。将来的には、あらゆるカウンターインテリジェンスを未然に防ぎ、優れた制御状態を維持できるようになります。

サイバーセキュリティ開発のこの分野では、大規模組織の豊富なセキュリティリソースとの競争という点で、サイバー犯罪者は不利な立場にあります。一般的にこの分野において防衛側が有利であるのは、大規模の実装に必要な予算も専用リソースもあるためです。サイバー犯罪者には、AI の十分な活用を可能にする、一般的には自らの手元にない大量のデータとコンピューティングリソースだけでなく、AI のトレーニングに何年間も投資して期待どおりの結果を出せるようにする必要もあります。ほとんどの犯罪組織にとって、これには膨大なコストが必要であるため、最も高度なサイバー攻撃であっても極めて初歩的な ML や AI のソリューションしか活用できないと考えられます。しかしながら、そのようなプレイブックの自らの攻撃への活用に必要なリソースをすでに持ち合わせているサイバー犯罪者も存在します。彼らの手にかかれば、プレイブックを利用して攻撃を修正し検知を回避したり、同じプレイブックを利用しているために防御側の手の内を先読みして対策を無効化したりできる可能性もあります。

そして、これは一時的な問題ではありません。侵害された（主にエッジ）デバイスの広大なネットワークを活用することで、巧みなサイバー犯罪者が企業ネットワークに肩を並べるほどの処理能力を手に入れることができる可能性もあります。そして、その壁を乗り越えれば、手に入れたリソースがダークネットでサービスとして売り出されるのは時間の問題だと思われます。すなわち、AI ベースのシステムや高度なセキュリティプレイブックの採用や開発が遅れている組織は、これらの戦術の犠牲になる可能性が高くなるということです。

身代金モデル：ダークネットでの交渉、サイバー保険

ランサムウェアは進化を続け、引き続き今日の組織が直面する最も危険で有害な脅威となっています。たとえば、ランサムウェアの開発者が昨年新たに実装したある戦略は、身代金を支払うことなく感染システムを自力で復旧させるという多くの組織の判断を打ち砕くものでした。今日のサイバー犯罪者は、データやシステムを暗号化するだけでなく、そのデータを公開サーバーに投稿するようになりました。そして、身代金を要求するだけでなく、要求を無視すれば重要な知的財産や機密情報を公開すると脅迫します。場合によっては、企業やその重役を辱める可能性のある機密情報を手に入れることで、さらに悪質な行動に出る可能性もあります。恐喝、中傷、名誉毀損はいずれも、デジタルの世界に場所を移した取引の道具です。性的な画像や情報を公開すると脅迫するセクストーションに法執行機関が注目するようになり、家庭のカメラが攻撃されて録画された映像が投稿される例[2]が、すでにいくつも報道されています。

ランサムウェアは進化を続け、引き続き今日の組織が直面する最も危険で有害な脅威となっています。

このような手口が一つの犯罪組織の専売特許であり続けることはありません。皮肉なことに、最近ではダークネットに身代金交渉をビジネスモデルとして手掛ける組織まで登場するようになりました。これには、身代金の減額やランサムウェアの活動期間の短縮という短期的なメリットがあるかもしれませんが、犯罪行為を正当化し、利益を手に入れる機会をサイバー犯罪者に常に与えてしてしまうという、思いとどまるべき理由もあります。

しかしながら、現実としてランサムウェアは今後もエスカレートし続ける可能性が高く、その影響はネットワークでのハイパーコンバージェンスの定着に伴ってますます大きくなると予想されます。ネットワーク、デバイス、アプリケーション、ワークフローが相互に交差することでより高度なサービスが提供されるため、ネットワークのどこかで故障すると重要なプロセスに影響する可能性があります。また、システムの重要インフラストラクチャシステムへのコンバージェンスが進むにつれて、リスクにさらされるデータやデバイスも増加します。パワーグリッドや医療システム、交通管理インフラストラクチャなどのクリティカルなリソースが標的になれば、人命に関わります。多くの患者がいる ICU を標的にするランサムウェア攻撃が遅かれ早かれ起こる可能性が高く、ランサムウェアはその後にさらに発展し、犯罪行為とテロリズムの境界を越えることになるでしょう。事実、最近の例[3]ではランサムウェア攻撃によって病院の IT 予約システムが新しい患者を受け付けられなくなり、救急車で運ばれてきた患者の他院への移送を余儀なくされ、不幸にも移送中に患者が死亡したことも報告されています。重要なインフラストラクチャを標的に同様の攻撃が仕掛けられ、原子力発電所の安全制御システムを無効化したり、ダムのゲートを開放したりする可能性もあります。

本レポートで取り上げた他の脅威と同様、サイバー犯罪者がランサムウェアの脅威をエスカレートさせ続けることができるかどうかは、エッジシステムやその他のシステムを活用し、悪用できるかどうかにかかっています。脆弱なデバイスを利用して新しいエッジネットワークが構築された場合、サイバー犯罪者は複雑なシステムに存在する脆弱性を検知して AI を活用したマルウェアを開発し、複数の攻撃ベクトルを標的にするなどの方法で高度な攻撃を実行できます。より大きなネットワークに匹敵する処理能力を手に入れることができれば、複数の攻撃要素を同時に調整する必要があるスウォームベースの攻撃などを仕掛けることもできます。

スウォームインテリジェンス（群知能）

2019 年にお伝えしたとおり、ML と AI の活用によってスウォームインテリジェンス[4]が進化を続けています。Gerardo Beni 氏[5]と Jing Wang 氏が 1989 年に初めて紹介したスウォームインテリジェンスとは、分散され[6]、自らを組織化する能力を持つ[7]システムによる集団行動[8]のことであり、自然発生的なものも、人工的なものもあります。蟻、蜂、白蟻、鳥の群れ、バクテリアなどの生物学的システムから着想を得たスウォームインテリジェンスは、車両の経路選択やジョブショップスケジューリング（JSS）、「ナップザック」問題などの複雑な問題を最適化する計算ツールとして活用されています。スウォームインテリジェンスの最大の悪用例は、IP ネットワークのルーティングへの蟻のコロニーアルゴリズムの応用です。

スウォームインテリジェンスの開発は、新しい医薬品や治療法の開発、複雑な輸送環境の調整、軍や航空宇宙産業が運用する大規模システムにおける、様々な問題解決の自動化分野で大きな意味を持ちます。

これまでに何回もお話したように、スウォームインテリジェンスが悪用され、企業がセキュリティ戦略を更新しない場合は、攻撃者にとって戦局を優位にするものとなる可能性もあります。サイバー犯罪者がボットベースのスウォームを使用することで、ネットワーク防御を瞬く間に突破して重要なデータを効率的に見つけて持ち出し、フォレンジック情報が削除されたり、攻撃されたりする恐れがあります。

複数のペイロードを使ってリアルタイムで偵察し、攻撃に最適なツールを選択するマルウェアはすでに見つかっていますが、命令を受け取ることで収集したデータに基づいて攻撃を変えたり、それらの情報をコマンド & コントロールセンターと共有したりすることもできるでしょう。新しい HEH ネット[9]の場合は、感染したピアを独自の P2P（ピアツーピア）プロトコルを使って追跡し、攻撃者が任意のシェルコマンドを実行できるようにしています。このボットネットは Go 言語で書かれているため、クロスプラットフォームで動作します。さらに、自己破壊コマンドをトリガーすることで感染デバイスからすべてのデータを削除するワイパー機能も備えていますが、これは我々が 2017 年に予測していたもの[10]です。

HEH やそれに類似する新たな脅威は、マルウェアの開発者が（たとえば C 言語を使用して）コンパイルしたネイティブのバイナリから Go のようなクロスプラットフォームのツールへの移行を進めていることを示す良い例です。

最終的に、このような攻撃は機能別にクラスタリングされた何千あるいは何百万もの専用のボットで構成されることになり、攻撃中にリアルタイムのインテリジェンスを相関付けることで高速かつ効率的に標的を攻撃し、攻撃レベルを上げてアクティブな防御システムも突破できるようになることが予測されます。

このような究極の攻撃システムに対する唯一の防御は、攻撃の一手一手の検知と予測、そして対策の実行が可能な AI を活用したテクノロジーです。未来のサイバー戦争はマイクロ秒単位で進行します。人間の主な役割は、セキュリティシステムに十分なインテリジェンスがフィードされていることを確認することであり、それによって進行中の攻撃に対抗するだけでなく、攻撃を予測して回避可能になります。

脅威の事実を知った後でセキュリティを実装する方法では、設計段階にあるテクノロジーにセキュリティを直接組み込む方法ほどの速さと有効性を実現することはできません。

未来の脅威

重要な教訓の一つは、脅威の事実を知った後でセキュリティを実装する方法では、設計段階にあるテクノロジーにセキュリティを直接組み込む方法ほどの速さと有効性を実現できないことです。最大の関心事の一つとしては、Starlink を始めとする高度な衛星ベースシステムを利用したデータやインターネットリンクの利用が拡大していることが挙げられます。衛星セキュリティシステムは主に遠く離れた場所に存在すること、カスタマイズされたハードウェアで動作し独自のオペレーティングシステムとアプリケーションを使用していることから、サイバー攻撃とは無縁と考えられていました。しかしながら、衛星ベースのネットワークが次々と登場する中で、衛星の基地局が攻撃され衛星ベースのネットワーク経由でマルウェアが拡散すれば、何百万人もの接続ユーザーを攻撃可能になる危険性があります。

計算処理能力の向上に伴い、これらの衛星ネットワーク経由でやり取りされる暗号化されたトラフィックは、いずれ有効な防御メカニズムではなくなってしまうでしょう。航空会社やクルーズ船、軍事システムでは、以前から衛星データが積極的に活用されてきましたが、企業の所有物あるいは重要インフラストラクチャに接続されているシステムのどちらであっても、複雑なシステムが衛星ベースのネットワークを利用するようになり、サイバー犯罪者がそれらのシステムを標的にするようになったとしたら、どのような影響があるでしょうか。これを足掛かりに、おそらくは DDoS（分散型サービス拒否）のような攻撃が OT を標的にして開始するものと予想されますが、衛星システムによる通信の普及に伴い、より高度な攻撃がすぐに後に続くことになるでしょう。

量子の脅威

最も将来性ある脅威予測は、量子コンピューティングに関連するものです。多くの人が、量子コンピューティングはその特性上攻撃耐性があると主張していますが、量子ベースのデバイスが暗号鍵やアルゴリズムの突破などの目的で使用されたとしたら、どうなるでしょうか。

量子コンピュータでは、これまでとは異なる方法で情報を表現し計算するため、今のコンピュータよりはるかに高速で動作します。それは、単なる**飛躍的な進化**ではなく、**革命**と呼ぶほどのものです。磁場での電子の動きを利用したキュービット（量子ビット）が発表されたことで、デバイスの処理能力の指数関数的な向上が可能になりました。量子コンピュータ以前のシステムではビットは 1 次元であり、ある状態または他の状態（オンまたはオフ）のいずれかです。量子力学は、最も簡単な言い方をすれば 2 次元であるため、量子ビット（キュービット）は重ね合わせ[11] 状態の両方を同時に表すことができます（オンとオフに加えて、オンでもオフでもない状態）。簡単に言えば、これまでのコンピュータは 2 つの状態しか表現できないビットを計算に使用するため、利用できる状態の数は直線的に（3 ビットであれば 6 つの状態 [2+2+2]、4 ビットであれば 8 つの状態というように）しか増えません。一方量子コンピュータでは、表現できる数が指数関数的に（3 つの量子ビットで 2 の 3 乗、すなわち 8 つの状態、4 つの量子ビットで 2 の 4 乗、すなわち 16 の状態というように）増加します。

それだけではありません。キューディット（Qudit と記述し、「d」は次元（Dimension）の可変数を表す）は、この概念をさらに発展させたものですが、たとえば国立科学研究所[12] の科学者が 2017 年に発表した、それぞれが 10 個の異なる状態を表現できる対のキューディットであれば、6 つのキュービットよりも高い計算能力が実現します。これを何百万ものキュービット（またはキューディット）と組み合わせれば、量子コンピュータの潜在的な計算能力はほとんど無限になります。

サイバーセキュリティの観点では、量子コンピュータはデータ暗号化のようなものの有効性を脅かすという点で壊滅的な役割を果たす可能性があり、非対称暗号化アルゴリズムはたちまち時代遅れのものになるでしょう（データ整合性を確保するために情報に「署名」するアルゴリズム、鍵交換の実行によって可能になる機密アルゴリズムによるデータの暗号化、人やデータの本人確認に使用されるアルゴリズムなどがこれに該当します）。事実、量子コンピュータによって 2027 年までに楕円曲線暗号が解読されるようになると予測されています。

もちろん、量子コンピュータが現段階で商用化されているわけではなく、少なくとも組織の大半がサイバー犯罪に悪用されるのではないかと心配するほどの機能を提供するものではありません。しかしながら、国家を後ろ盾に活動する犯罪集団も存在します。現在、量子コンピュータを保有している、あるいは開発中である国は多数あり、その大半は医学研究、天気予報、複雑な計算処理などの善意の目的で活用されていますが、スパイ活動などを専門とする政府機関がこのような高度なテクノロジーを活用しなかったことはありません。

サイバーセキュリティの観点では、量子コンピュータはデータ暗号化のようなものの有効性を脅かすという点で壊滅的な役割を果たす可能性があります。

数多くの政府機関が、長年にわたってデータスクレイピングと呼ばれるプロセスを利用し、自国に経済的な利益をもたらす国や企業から大量の暗号化されたデータを収集してきました。それらの情報は今もどこかに存在し、一度それを可能にするツールが登場すれば瞬く間に解読されてしまうでしょう。

そのため組織は、情報への「署名」、通信用の暗号鍵の確立、情報の整合性の保護に暗号を使用するあらゆる分野で、耐量子コンピューティングアルゴリズムへの移行を進める必要があります。世界中の大学、政府機関、専門のセキュリティ組織が現在、暗号化の俊敏性の原理を中心とした高度な暗号化ツールの開発に莫大なリソースを投入しています。アメリカ国立標準技術研究所（NIST：National Institute of Standards and Technology）のガイドライン[13]によれば、量子コンピュータ時代への備えとして「暗号化の俊敏性の維持が不可欠である」とされています。ハードコーディングされた暗号システムでは、脆弱性が一度発見されると保護や対策は不可能となります。技術的な俊敏性の実現には、新たな開発フレームワークとサービスソフトウェアを採用し、強力な暗号化テクノロジーを利用して常にアプリケーションとデータをシームレスに保護する必要があります。

組織は「セキュリティの俊敏性」を自らの運用セキュリティ方針に組み込む必要があり、耐量子非対称暗号アルゴリズムや量子鍵交換が利用可能になった段階で、セキュリティソリューションがそれらにシームレスに移行できることを確認しておくことも含まれます。NIST は現在、「耐量子コンピュータ暗号」規格の開発を進めています。組織、特に国家のスパイ活動の標的にされる可能性の高い組織が目標とすべきは、量子コンピュータの一般利用が可能になる数年前に耐量子アルゴリズムを採用することです。

組織が採るべき対策

一部の組織は、この新しいサイバー脅威の世界が現実であり、消えることはないのだと理解しています。彼らは、サイバー脅威への対策は「起きるかどうか」ではなく「いつ標的にされるか」の問題だということを新たな信条としています。これは、プロアクティブな防御だけでなく、効果的なインシデントレスポンスに対しても組織のリソースを投入する必要があることを意味します。なぜならば、侵害は不可避であり、進行中の攻撃を停止するには次に何をすべきか理解していることが、ネットワークの保護には不可欠だからです。

効果的で統合された次世代 AI システムであれば、攻撃者が目的を達成する前にレスポンスを実行し、高い確率でネットワークを保護できます。このようなシステムの実現には、人間の体を病気から守り、発病した場合は感染と戦って同じウイルスの抗体を作ってくれる、適応型の免疫システムに似た機能が必要です。

公共機関との緊密な連携

組織がすべてを自力で解決できるわけではありません。脅威インテリジェンスフィードのサブスクリプションを利用すると同時に、関連するコンソーシアムに所属し、地域や業界の他の組織や人と積極的にデータや戦略を共有することが重要です。また、法執行機関や教育機関などの公的機関と緊密なパートナーシップを築いているベンダーと協力する必要もあります。

教育分野における官民連携は、児童や学生が将来的に自らを保護し、安全なサイバー行動によって社会を尊重し、保護するようになるための教育だけでなく、新たなデジタル経済を破壊する脅威となる、拡大し続けるサイバーセキュリティのスキルギャップの解消にも役立ちます。高等教育機関だけに限定せずに義務教育の段階から教育を開始し、児童が「ダークサイド」に進む前に「ライトサイド」に参加するよう奨励することが重要です。

サイバーセキュリティのベンダーや脅威の研究者、そして業界のリーダーは法執行機関に協力する必要があり、そのような機関による捜査の範囲や規模に変化が見られるようになった今は、その重要性がさらに高まっています。法執行機関が直面している問題は多数存在しますが、中でもサイバー犯罪が政治的な境界を超えるようになったことは最大の課題の一つといえます。外国のコールセンターから発信される電話詐欺、海賊版ソフトウェア、データや金銭の盗難などの多くの犯罪が、国境を超えることで保護対策から逃れています。この問題を解決するために、法執行機関はグローバルな司令部の設置のみならず、民間企業との連携を強化することで、サイバー犯罪のリアルタイムでの特定と対応を進めています。

セキュリティ ファブリックは、法執行機関と公共 / 民間組織とのこのような関係から生まれたソリューションと、脅威インテリジェンスで構成されるものでなければなりません。これには脅威フィードのサブスクリプションも含まれ、これによってセキュリティリソースとセキュリティチームが常に新たな脅威に対応できるようになります。その結果、サイバー犯罪者を確実に特定して対応し、犯罪者や犯罪行為の阻止を可能にする、より効果的なプレイブックを企業が作成し、導入できるようになります。今後数年間で、国際的な法執行機関や国や地域の法執行機関、政府、企業、セキュリティエキスパートの協力の下、より統一されたアプローチの推進を目的とするイニシアチブが増えていくでしょう。サイバーセキュリティテクノロジーの継続的な進歩がこれに加わることで、情報のタイムリーかつ安全な交換とレスポンスが促進され、重要なインフラストラクチャを保護してサイバー犯罪に対抗し、サイバー犯罪者を廃業に追い込むことが可能になるのです。

FortiGuard Labs について

FortiGuard Labs は、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。業界トップクラスの脅威インテリジェンスを提供し、悪意のある活動や高度なサイバー攻撃からフォーティネットのお客様を保護することをミッションとしています。FortiGuard Labs は、世界中の専門の脅威研究所で活動し、業界で最も豊富な知識を持つ脅威ハンター、研究者、アナリスト、エンジニア、データサイエンティストによって組織されています。FortiGuard Labs は、数百万台のネットワークセンサーを活用し、数百のインテリジェンス共有パートナーと協力して、世界中の攻撃対象領域を継続的に監視しています。これらの情報を、AI（人工知能）を始めとする革新的なテクノロジーを利用して分析し、処理することで、新しい脅威のデータマイニングを実行しています。これらの取り組みによって得られた実用的な脅威インテリジェンスをフォーティネットのセキュリティ製品アップデートという形でタイムリーに提供し、お客様が直面する脅威と攻撃を仕掛けるサイバー犯罪者の理解に役立つプロアクティブな脅威リサーチを実施し、お客様のセキュリティリスクの特定と対策強化を支援する専門のコンサルティングサービスを提供しています。詳細は、フォーティネットの Web サイト[14]、ブログ[15]、FortiGuard Labs の脅威インテリジェンス[16] ページをご覧ください。

[1]「Fortinet FortiGuard Labs 2018 Threat Landscape Predictions」、Derek Manky 著、フォーティネットセキュリティブログ、フォーティネット、2017 年 11 月 14 日（英語）：https://www.fortinet.com/blog/business-and-technology/fortinet-fortiguard-2018-threat-landscape-predictions

[2]「50,000 home cameras reportedly hacked, footage posted online」、Amer Owaida 著、WeLiveSecurity、2020 年 10 月 14 日（英語）：https://www.welivesecurity.com/2020/10/14/50000-home-cameras-reportedly-hacked-footage-posted-online/

[3]「A Patient Dies After a Ransomware Attack Hits a Hospital」、Dan Goodin 著、WIRED、2020 年 9 月 19 日（英語）：https://www.wired.com/story/a-patient-dies-after-a-ransomware-attack-hits-a-hospital/

[4]「Defending Against an Automated Attack Chain: Are You Ready?」、Derek Manky 著、フォーティネットセキュリティブログ、フォーティネット、2018 年 6 月 18 日（英語）：https://www.fortinet.com/blog/industry-trends/defending-against-an-automated-attack-chain--are-you-ready-

[5]「Gerardo Beni」、Wikipedia（英語）：https://en.wikipedia.org/wiki/Gerardo_Beni

[6]「Decentralization」、Wikipedia（英語）：https://en.wikipedia.org/wiki/Decentralization

[7]「Self-organization」、Wikipedia（英語）：https://en.wikipedia.org/wiki/Self-organization

[8]「Collective behavior」、Wikipedia（英語）：https://en.wikipedia.org/wiki/Collective_behavior

[9]「HEH, a new IoT P2P Botnet going after weak telnet services」、JiaYu 著、360 Netlab Blog、2020 年 10 月 6 日（英語）：https://blog.netlab.360.com/heh-an-iot-p2p-botnet/

[10]「Fortinet 2017 Cybersecurity Predictions: Accountability Takes the Stage」、Derek Manky 著、フォーティネットセキュリティブログ、フォーティネット、2016 年 11 月 21 日（英語）：https://www.fortinet.com/blog/industry-trends/fortinet-2017-cybersecurity-predictions-accountability-takes-the-stage

[11]「Quantum superposition」、Wikipedia（英語）：https://en.wikipedia.org/wiki/Quantum_superposition

[12]「National Institute of Scientific Research」、Wikipedia（英語）：https://en.wikipedia.org/wiki/National_Institute_of_Scientific_Research

[13]「アメリカ国立標準技術研究所（NIST：National Institute of Standards and Technology）のガイドライン」、National Institute of Standards and Technology, U.S. Department of Commerce（英語）：https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf

[14]「フォーティネットの Web サイト」、フォーティネットジャパン：https://www.fortinet.com/jp

[15]「フォーティネットセキュリティブログ：脅威リサーチ」、フォーティネットジャパン：https://www.fortinet.co.jp/blog/threat-research.html

[16]「FortiGuard Labs の脅威インテリジェンス」、フォーティネットジャパン：https://www.fortinet.com/jp/fortiguard/labs

フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

WP-Cyber-Threat-Predictions-for-2021-202012-R1