Kaspersky Security Bulletin

2022 年 高度なサイバー脅威の予測

kaspersky BRING ON THE FUTURE

2022 年 高度なサイバー脅威の予測

この 1 年、APT（高度サイバー攻撃）のスタイルと深刻さは変化し続けました。常に変化し続ける性質を帯びてはいますが、2022 年に起こりうる事態を予測するために、最近の APT の動向から学べることは多くあります。

当社エキスパートの知識と洞察に基づき、標的となりうる方々が防御態勢を維持できるように、APT グループが次に狙うであろう対象について予測しました。まずは 2021 年の高度なサイバー脅威の予測について振り返ります。

APT 脅威アクターは、初期のネットワークアクセスをサイバー犯罪者から購入する

昨年末、APT 脅威アクターたちがディープウェブ市場を活用しているケースを確認しました。ここでは、侵入した企業へのアクセス権を犯罪者たちが売買しています。

当社は昨年、APTグループとサイバー犯罪者の間で、運用レベルでの関わりが深くなると予測しました。特に、APT 脅威アクターがディープウェブ市場を活用するようになると予想しました。ここでは、侵入した企業へのアクセス権を犯罪者たちが売買しています。この予測が正しかったことが、わずか数日前に明らかになりました。Blackberry は先日、同社が Zebra 2104 と呼ぶ、「初期アクセスブローカー」と考えられる主体を中心としたレポートを発表しました。同社の調査によれば、Zebra 2104 はランサムウェア攻撃のオペレーターに対して、一部の被害者への初期侵入の足掛かりを提供していたということです。しかし、さらに興味深いことに、StrongPity APT も Zebra 2104 のサービスを利用したと見られます（もっとも、その目的はインテリジェンスの収集に終始していました）。この種のやり取りは、攻撃の準備段階、つまり通常は私たちが目にすることのできない段階の活動であるため、気付かないうちに APT グループとサイバー犯罪者の間でもっと頻繁に行われている可能性があります。

サイバー戦略の一環として、法的手段に訴える国が増加する

当社は昨年、2021 年は敵対する APT グループの活動に関心を集めるため、各国政府が「名指しで非難」する戦略を取り入れると予測しました。実際、この傾向はこの 1 年でさらに強まっています。また、各国はあらゆる法律を駆使して敵対的な攻撃を妨害し罰則を科すようになるだろうとも予測しましたが、これも正しいことが実証されました。

2021 年 4 月 15 日、米国政府は、SolarWinds 社へのサプライチェーン攻撃についてロシア政府を公に非難しました。この発表に続いて、一連の攻撃を支援したと米財務省がみなす複数の企業に対して制裁措置が実施されました。

7 月 1 日、米国家安全保障局（NSA）、米連邦捜査局（FBI）、米サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）、および英国の国家サイバーセキュリティセンター（NCSC）が共同勧告の発行という形で、Sofacy（別名 APT28、Fancy Bear）によるブルートフォース（総当たり攻撃）が世界中で何百件も試行されていると警告しました。標的には政府機関や軍事機関、防衛関連事業者、政党や政治関連コンサルタント会社、物流会社、エネルギー会社、大学、法律事務所、メディア企業が含まれていました。

7 月 19 日、米国は NATO、EU、英国の支持を得て、「サイバー空間における無責任かつ不安定化を招く行為（irresponsible and destabilizing behavior in cyberspace）」を非難する意思があることを発表しました。ホワイトハウスの声明では、近年の Microsoft Exchange ゼロデイ脆弱性の悪用について具体的に言及しています。また、米司法省は、違法なコンピューターネットワーク活動を行ったとされる APT40 のメンバー4 人を告発しました。

イスラエル国防軍（IDF）は、攻撃者がなりすましによってイスラエル兵士にスパイウェアをインストールするよう仕向けていると主張しました。攻撃者は Facebook、Instagram、Telegram の 6 つのプロファイルを利用して男性ターゲットの注意を引き親密な関係を築いて、最終的に携帯電話にプライベートチャットの機能を提供すると称するアプリをインストールするよう仕向けていました。

9 月 24 日、EU は、2017 年 3 月から現在まで続き、NATO の信用低下を意図した、「Ghostwriter」と呼ばれる偽情報キャンペーンに関する声明を発表しました。このキャンペーンでは、ニュースサイトや政府関係者のソーシャルメディアアカウントに侵入し、選挙の揺さぶりや地方政治エコシステムの攪乱、NATO の信用低下を目的として、偽造文書やフェイクニュース、ミスリードにつながる見解の公表が行われたと言われています。脅威ではあるものの、EU は最終的に制裁を課さないことを決定しました。

全体的には、サイバーインシデントする対処方法に明らかな変化が見られ、外交ルートを通さずに、告訴などの法的手段が講じられるようになってきています。

ゼロデイブローカーに対して行動を起こすシリコンバレー企業が増える

昨年の予測のリリース直後、Facebook の NSO に対する法廷闘争に、Microsoft、Google、Cisco、Dell も加わりました。この一連の訴訟は現在も続いています。

当社が昨年の脅威予測を発表した直後、Facebook がスパイウェアを販売する NSO に対する法廷闘争に、Microsoft、Google、Cisco、Dell も加わりました。この一連の訴訟は現在も続いており、当社が知る限り、ほかのゼロデイまたは侵入するためのソフトウェアを販売するベンダーに対する訴訟は始まっていません。

手短に言えば、予測がすぐに的中した形になりました。今後、シリコンバレーの企業がこの最初の訴訟の結果を待って、ほかのブローカーに対する手続きに入る可能性もあります。一方で、米商務省は 11 月 3 日に、「サイバーツール内のトラフィック」の観点で米国の国家安全保障に反する活動を行っている複数の企業（NSO、Positive Technologies、COSEINC、Candiru）を、取引を制限するエンティティリストに追加することにより、ゼロデイ市場に非常に強い警告を示しました。現時点では、この警告が進行中の手続きにどのような影響を及ぼすかは不明です。

ネットワーク機器が狙われるケースが増える

当予測の執筆時点では、主に VPN 機器を標的とした悪意のある活動が続いていくと考察していました。しかし、本記事の最初に言及したとおり、最も顕著に見られたソフトウェア脆弱性は、各種プログラム（Microsoft Exchange など）に影響を及ぼすものでした。それでも、APT10 などの一部の攻撃者がこれらの脆弱性を悪用して VPN セッションの乗っ取りを行っていたことが確認されています。

また、この予測は別の方面でも的中しました。APT グループの APT31 が首謀者となった、極めて興味深いキャンペーンが 2021 年に表面化しました。その中で、この攻撃者は感染済みの SOHO ルーターのネットワーク（具体的には、Pakedge RK1、RE1、RE2 の機種）を利用し、匿名化ネットワークとして、また、指令サーバーをホストするために使用していました。

5G の脆弱性が出現する

2020 年は 5G テクノロジーの開発をめぐり緊張が高まった年でした。2021 年はこの緊張がさらに高まり、それを示す事象の 1 つとして、5G 関連製品あるいは 5G プロトコル自体の脆弱性が発見され公表されることになるだろうと予測していました。実際は主に法的分野に限定された論争が起こったようですが、一方で、攻撃者が認証情報や位置情報を抽出できるセキュリティ上の問題を指摘した興味深い研究も見られました。

「脅迫して」金銭を要求する

ランサムウェア問題への対応が組織化されつつあります。

2019 年から確認されている「強化された」ランサムウェアの手口は、サイバー犯罪者の戦略に欠かせないものになるほどの効果を発揮しています。一方で、各方面で逮捕者が出ていることや、多数の法執行機関や当局から共同宣言が出されていることから判断すると、ランサムウェア問題への対応が組織化されつつあることは明白です。米政府は 2021 年 10 月に、ランサムウェア攻撃活動 REvil の活動を阻止するための積極的な対策を実施しました。

このような圧力の高まりや、それがもたらす本質的な脅威が、ランサムウェアのエコシステムにおける現在の動向にも反映されています。盗み出したデータを利用した脅迫戦術は十分に試行され手法として確立されたため、現時点で犯罪グループの焦点にはなっていないものと思われます。

破壊的な攻撃が増える

昨年のこの予測も正しいことが実証されました。2021 年の最も象徴的な事件の 1 つが、Colonial Pipeline へのランサムウェア攻撃です。この攻撃の過程で、燃料供給のパイプラインを管理する機器がランサムウェアに感染し、その結果、米国で重大な燃料供給不足の問題が発生しました。このインフラは非常に重要だったため、被害を受けた企業は 440 万ドルの身代金を支払わざるを得ませんでしたが、幸いにも 230 万ドルが米国司法省によって取り戻されました。

2021 年 7 月、未確認のワイパー型マルウェア（Meteor）がイランの鉄道システムを麻痺させました。さらに、立ち往生した利用者に対して、地元の当局に電話で苦情を伝えるような誘導があったため、鉄道会社とは別に苦情を受けた政府機能のサービス品質に影響を及ぼしたと思われます。その後 10月にも同様の攻撃があり、イラン国内のすべてのガソリンスタンドが影響を受けました。いずれの攻撃についても、その犯行を認めたサイバー犯罪グループはいません。

サイバー攻撃者は新型コロナウイルス感染症の蔓延を悪用し続ける

2020 年、複数の APT グループが新型コロナウイルスのワクチン開発に携わる学術機関や研究センターを標的としていることが確認されました。これには DarkHotel と APT29（別名 CozyDuke、CozyBear）が含まれ、WellMess マルウェアを使用していました（英国の国家サイバーセキュリティセンター（NCSC）によるアトリビュート）。2021 年には、ScarCruft、LuminousMoth、EdwardsPheasant、BountyGlad、Kimsuky、ReconHellcat など複数の APT グループが、新型コロナウイルス感染症のトピックスを利用して標的を探していることが確認されました。当社が追跡した活動の中でも興味深いある一群は、後に SideCopy との呼び名で知られる攻撃者によるもので、アジアおよび中東地域の外交関係の政府機関を標的としていることが特定できました。攻撃では、悪意のある HTA ファイルや JS ファイルをホストしている侵害された Web サイトを利用し、新型コロナウイルス関連の情報をフックにしていました。この攻撃には、実行チェーン、使用しているマルウェア、インフラの重複、PDB ファイルのパス、そのほかの TTPs（戦術、技術、手順）など複数の側面で、同地域で活動するほかの攻撃グループ（SideWinder、OrigamiElephant、Gorgon Group、Transparent Tribe など）を想起させます。しかし、これらの類似性は、一連の活動を既知の攻撃グループに関連づけるほどの強いものではありません。

次に、今後に目を向け、当社が 2022 年に起こりうると考える展開について紹介します。

民間企業が新たな APT 攻撃者の流入を後押し

前述したとおり、今年は民間のベンダーが開発した監視ソフトウェアの使用が注目を集めました。このビジネスの潜在的な収益性の高さと、標的となる組織に対する影響の大きさを考慮すると、少なくとも政府がその使用の規制を検討し始めるまでは、このようなソフトウェアベンダーの役割は大きくなると考えられます。その兆候はすでに確認されています。2021 年 10 月、米商務省産業安全保障局（BIS）は、商用の監視ソフトウェアに対して輸出許可が求められる場合の条件を定義した最終規則の中間結果を報告しました。その目的は、安全保障に関する合法的なセキュリティの研究や取引を継続しつつ、軍備管理対象国への監視ツールの配布を防止することです。

しばらくは、**マルウェアベンダーや軍事攻撃用セキュリティ産業界は、その攻撃の実施において、既存のプレイヤーだけでなく新しいプレイヤーの活動の支援も目指すことになるでしょう。**

モバイルデバイスが幅広い攻撃にさらされる

Android ベースの端末は多数のサイバー犯罪型マルウェアに悩まされる一方、iOS は主に国家の支援を受けた高度なサイバースパイ活動の標的となっています。

モバイルデバイスを標的としたマルウェアは、10 年以上にわたり途切れることなくニュースになってきました。これは、主要 OS の普及率との強い相関関係があります。現在のところ、普及率の高いモバイルデバイス用 OS は iOS と Android の 2 つです（これに加えて、Android/Linux ベースのクローン OS も存在します）。これらの OS の理念は元々大きく異なり、iOS は審査を通ったアプリのみが許可される閉じられた環境の App Store を利用してきたのに対して、Android はよりオープンで、ユーザーがサードパーティが開発したアプリをデバイスに直接インストールすることができます。結果として、これら 2 つのプラットフォームを標的とするマルウェアの種類にも大きな違いが生じ、Android ベースの端末は多数のサイバー犯罪型マルウェアに悩まされる一方（APT 攻撃とは無縁ではありませんが）、iOS は主に国家の支援を受けた高度なサイバースパイ活動の標的となっています。2021 年、Pegasus Project による調査の結果では、iOS のゼロクリック・ゼロデイ攻撃の実態が明らかになり、例年と比較して多くの iOS ゼロデイ攻撃が報告されました。

攻撃者の視点から見ると、モバイルデバイスは理想的なターゲットです。所有者と一緒にほぼどこにでも移動し、プライベートな詳細情報を保存していながら、マルウェア感染の防止や検知が困難です。ユーザーがセキュリティ製品をインストールできる Windows PC や Mac とは異なり、iOS の場合はそのような製品は無効化されているか、存在しません。これは、APT グループにとって非常に大きなチャンスであり、国家の支援を受ける攻撃者にとって見逃すことはできません。**2022 年は、モバイルデバイスに対する高度な攻撃がより多く確認され対処され、攻撃者は当然、否定的な態度をとると予想されます。**

サプライチェーン攻撃がさらに増加

2021 年はサプライチェーン攻撃が目立ちました。APT 脅威グループがこの手法を利用していることについては、前述しました。一方で、侵害を受けた企業の顧客を侵害する目的で、サイバー犯罪者がサプライヤーのセキュリティ上の弱点を利用するケースも見られます。その顕著な例が、5 月の米石油パイプラインシステムに対する攻撃、6 月の世界的な食肉生産企業に対する攻撃、そして 7 月の MSP（マネージドサービスプロバイダー）とその顧客を標的とした攻撃です。この種の攻撃は、サプライチェーン内のどこかで信頼が損なわれていることを意味しています。攻撃者にとっては、ほかの多数の標的への足掛かりが一挙に得られるため、特に価値があります。このことから、**2022 年以降もサプライチェーン攻撃は増加傾向になるでしょう。**

在宅勤務を狙った攻撃が続く

多くの従業員が今後しばらくは在宅勤務を継続することになりそうです。このことは、攻撃者が企業ネットワーク内に侵入する機会を与えることにもなります。

世界各地で新型コロナウイルス対策のロックダウン規制が緩和されていますが、多くの従業員が在宅勤務を続けており、今後しばらくはその傾向が続くと見られます。このことは、攻撃者が企業ネットワーク内に侵入する機会を与えてしまうことになるでしょう。ソーシャルエンジニアリングによって認証情報を取得したり、保護が適切ではないサーバーを見つけようと企業が使用するサービスに総当たり攻撃を仕掛けるケースも含まれます。さらに、多くの従業員が企業の IT 部門によりロックされた機器ではなく個人保有の機器を使用し続けると、サイバー**攻撃者はセキュリティ保護がされていない、あるいはパッチが適用されていない自宅用コンピューターを企業ネットワークへの侵入経路として利用するための新たな機会を模索するようになるでしょう。**

META（中東、トルコ、アフリカ）地域、特にアフリカで APT 攻撃による侵入が増加

同地域全般の地政学的緊張の高まりを受けて、スパイ活動を基にしたサイバー攻撃が増えています。地政学は、経済、技術、外交などの要因と並んで、国家安全保障のための機密データの窃取を目的としたサイバー侵入に影響を与える主な要因となってきました。世界全体に影響を及ぼしている新型コロナウイルスの状況をよそに、少なくとも 2020 年 1 月以降、中東地域とトルコで地政学的緊張が著しく高まっており、今後もその傾向が続くと見られます。

アフリカは急速に都市化が進んでいる地域であり、多額の投資対象となっています。同時に、アフリカ大陸の多くの国々が海上貿易における戦略的な立場にあります。このことと、地域の防衛能力が継続的に向上していることから、**2022 年は META 地域、特にアフリカにおいて大規模な APT 攻撃が発生すると考えられます。**

クラウドセキュリティやアウトソーシングサービスに対する攻撃が爆発的に増加

クラウドプロバイダーは国家機関の関心を引くほど大量のデータを集積しており、今後、高度な攻撃の主要な標的になるでしょう。

クラウドコンピューティングには高い利便性とスケーラビリティがあることから、ビジネスモデルにクラウドコンピューティングを組み込む企業が増えています。DevOps の考えが普及したことで、多くの企業がマイクロサービスをベースとしたソフトウェアアーキテクチャを取り入れ、サードパーティのインフラ上で実行するようになりました。こういったインフラは通常、1 つのパスワードまたは API キーを突破されるだけで乗っ取られてしまいます。

このような最近のパラダイムには、開発者側が完全に理解していないセキュリティ上の影響があります。これは、防御側もほとんど見通すことができておらず、APT グループもこれまであまり調査していないような影響です。当社では、この状況に先に対応できるのは APT グループだと考えています。

この予測を広義に捉えると、オンラインドキュメント編集、ファイルストレージ、メールホスティングなどのアウトソーシングサービスも関係します。サードパーティの**クラウドプロバイダーは、国家背景の攻撃者が注目するほどの大量データを集積しているため、今後は高度な攻撃の主要な標的の一つとなるでしょう。**

ローレベルの攻撃が復活し、ブートキットが再び「ホット」に

ローレベルの埋め込みプログラムは、時々攻撃者に敬遠される傾向があります。性質上システム障害を引き起こすリスクがあること、作成に高度な技術が必要であることが主な理由です。当社が 2021年に発行した複数のレポートでは、ブートキットにおける攻撃的な研究が頻繁におこなわれていることに触れています。これは、隠れた利益がリスクを上回るようになった、あるいはローレベルの開発が実施しやすくなったことを示しています。2022年には、この種の高度な埋め込みプログラムの検知件数が増えると予想されます。さらに、**セキュアブートの普及が進んだことから、攻撃者はそれを迂回するために、このセキュリティ機構のエクスプロイトや脆弱性を探し出し、**ツールの展開を継続する必要があるでしょう。

各国が許容するサイバー攻撃活動を明確化

サイバー攻撃の分類法を発表し、禁止される攻撃経路の種類や行動を詳細に示す国も出てくるでしょう。

過去 10 年の間、業界全体の動向として、特にサイバー戦争の観点から、サイバー空間がますます政治的になっていく傾向を観察してきました。当社は昨年、攻撃側の作戦に対してコストを強いる目的で、西側諸国において法的手段が戦略の重大な部分を占めるようになると予測しました。

しかし、自国へのサイバー攻撃を非難している国々が、自らもサイバー攻撃を仕掛けているという問題があります。それらの国々で抗議の説得力を増すために、許容できるサイバー攻撃と許容できないサイバー攻撃の違いを明確化することが必要になるでしょう。2022　年は、**サイバー攻撃の分類法を発表し、禁止される攻撃経路の種類（例：サプライチェーン）や行為（例：破壊的なもの、市民インフラに影響を及ぼすものなど）を詳細に示す国が出てくる**と考えられます。

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com

kaspersky.com

kaspersky BRING ON THE FUTURE