


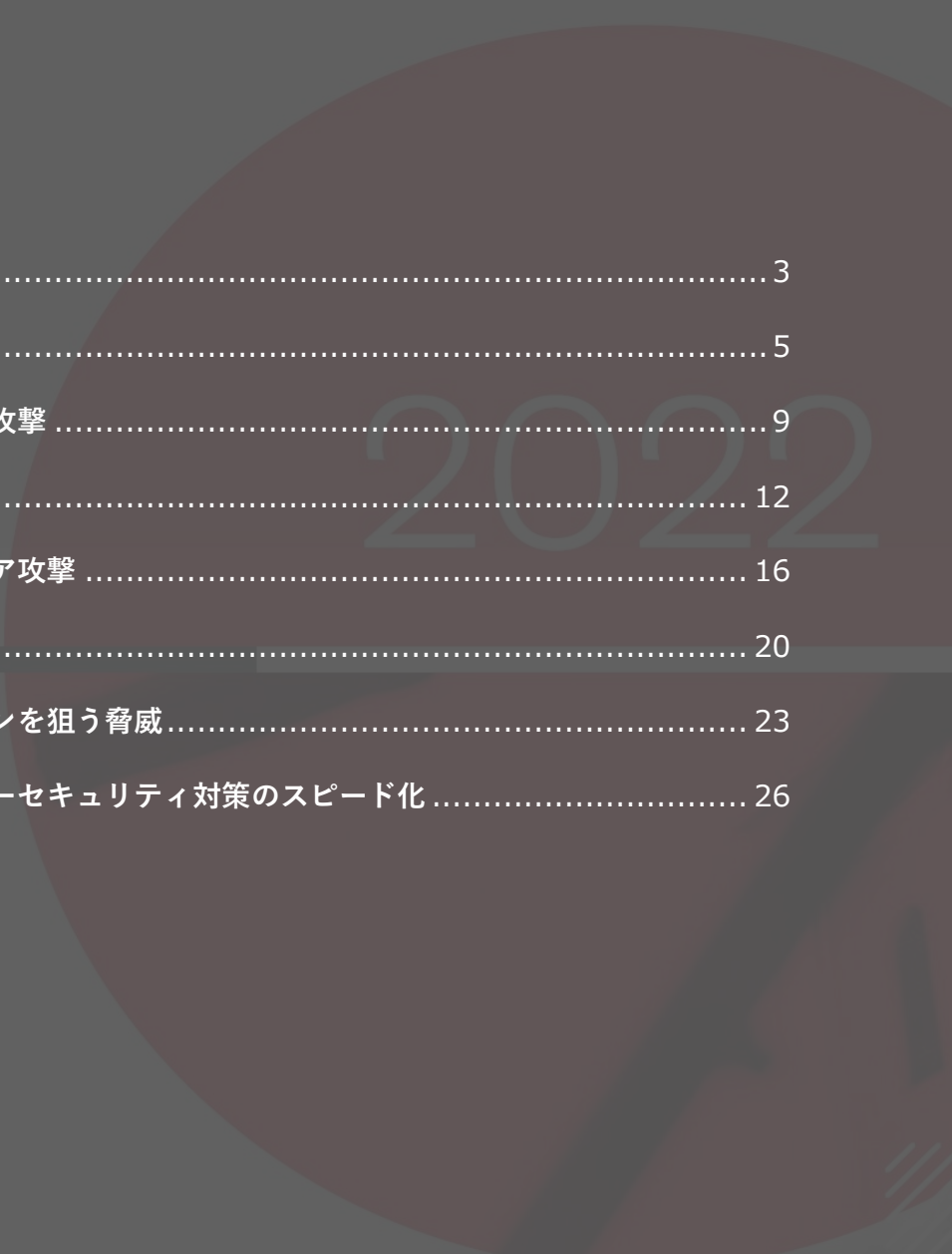


2022 年セキュリティ 脅威予測

TREND MICRO SECURITY PREDICTIONS FOR 2022





はじめに.....	3
クラウドの脅威.....	5
ランサムウェア攻撃.....	9
脆弱性攻撃.....	12
従来型マルウェア攻撃.....	16
IoTの脅威.....	20
サプライチェーンを狙う脅威.....	23
まとめ：サイバーセキュリティ対策のスピード化.....	26

はじめに

2021 年は、多くの企業にとってターニングポイントとなった年と言えるでしょう。各国でロックダウンの状態が続いたことで、多くの企業がデジタルトランスフォーメーション（DX）を加速させ、ハイブリッドワークモデルを採用しました。しかし新型コロナウイルスの世界的流行から1年以上が経過した今、これらの企業は、ハイブリッドワークモデルを優先し、パンデミックによる危機の終息が求められる中、「新たな日常」の足場を確かにするためにも、さらなる「ギアチェンジ」が必要となるでしょう¹。

サイバー犯罪者は、ビジネス環境がいまだに流動的である機会を狙って行動を起こそうとしています。デジタルトランスフォーメーションの推進により、企業の攻撃対象が再定義されていく中、新たな課題の発生は必至です。企業は、さまざまなツールやベストプラクティスによるセキュリティ対策を講じることで、これらの脅威を阻止することができます。

2022 年も引き続き、新たな脅威が世界中のサプライチェーンを狙ってきます。サイバー犯罪者は、ランサムウェアの多重恐喝モデルなどを駆使するため、被害は、攻撃対象だけでなく、その顧客やパートナーにも及び、さまざまな業務のオペレーションに混乱をもたらすでしょう。

クラウドを導入する企業は、多方面からの防御を強化する必要があります。特に試行錯誤を繰り返して新たな手法を展開してくる攻撃者に備えるためにも、こうした強化は不可欠となります。2022 年には新しい暗号資産が導入されるため、企業のセキュリティ部門は、社内のリソースを乗っ取ってクラウドコンピューティング機能を悪用するサイバー犯罪者を把握しておく必要があります。また、クラウドサービスやクラウドアプリケーションへのアクセスポイントとして、ビルドシステムや開発者の認証情報が狙われるケースの増加も予想されます。開発者は、自分の認証情報がシステムを危険にさらそうとする攻撃者の手に届かないようにする必要があります。

高額なバグ報奨金を獲得しようとする脆弱性ハンターが増加し、脆弱性へのメディアの注目度が高まる中、今後1年間でこれまでにない数の脆弱性が発見されると予想されます。これにより、ゼロデイ脆弱性の悪用件数が急増し、2021 年の件数を上回るようになることが予想されます²。修正パッチの対応が遅れがちな無防備な企業は、社内インフラの弱点を突こう

¹ <https://www.reuters.com/business/healthcare-pharmaceuticals/country-by-country-scientists-eye-beginning-an-end-covid-19-pandemic-2021-11-03/>

² <https://techhq.com/2021/10/2021-was-a-record-breaking-year-in-zero-day-exploits-and-thats-both-good-and-bad-news/>

とする攻撃者に翻弄されることになり、複数の脆弱性の積み重ねにより、新たなマルチプラットフォームの脅威を生み出すことになるでしょう。

2022年、ランサムウェアの脅威は、2つの傾向が顕著化してくるでしょう。最新のランサムウェアが標的型攻撃を先鋭化させる中、企業はこうした脅威への対処が迫られてくるでしょう。また、ランサムウェアの攻撃者は、情報暴露型の攻撃活動のため、情報窃取の手口などをますます巧妙化させてくるでしょう。多くの企業は、エンドポイントのセキュリティを注力している一方、サーバのセキュリティに改善の余地があるケースもあり、ランサムウェアの攻撃は、企業のセキュリティ部門にとって大きな課題となるでしょう。

企業が標的型攻撃の対策に追われる一方で、最新のツールボックスを備えた攻撃者は、コモディティ化したツールを販売するマルウェアブローカーを利用し、中小企業を狙った攻撃でも成功を収めることができるでしょう。2022年に登場するコモディティ化されたマルウェアの中では、複数のプラットフォームを侵害できる巧妙なサービスとしてのボットネットワーク（Botnet-as-a-Service）のモデルが含まれる可能性があります。

スマートデバイスがさらに進化すると、サイバー犯罪者たちの関心は、スマートデバイスだけでなく、モノのインターネット（IoT）へと拡大していくでしょう。とりわけ、増え続けるコネクテッドカーのデータに向けられるでしょう。このデータは、自動車メーカーの新たな収益源として注目されているからです。こうした状況は、セキュリティベンダと自動車メーカーが協力して、新しいクラスの安全なスマートカーのロードマップを作成する機会となるでしょう。

2022年は、企業にとってもサイバー犯罪者にとっても可能性に満ちた転換期となるでしょう。本レポートでは、企業がさまざまなセキュリティ分野でより多くの情報に基づいた意思決定を行えるよう、脅威の専門家による2022年のセキュリティに関する洞察と予測を詳しく紹介しています。

CLOUD THREATS

クラウドの脅威

企業は、クラウドセキュリティの基本を徹底することで、数多くのクラウドの脅威から自社の環境を守り、管理されたりリスクレベルを達成することができます。

クラウドの攻撃者は、開発工程の早い段階に着目するシフトレフトのトレンドに対応してさまざまな手法を駆使し、クラウドを採用している企業に大きな被害をもたらす攻撃を続けていくでしょう。

膨大な量のデータを保存・処理できる無限ともいえるクラウド環境³のおかげで、新型コロナのパンデミック発生後、企業は比較的容易にリモートワークに移行⁴することができました。そして 2020 年も、クラウドへの移行は、新たなビジネス運営の規範として重要な要素であり続けるでしょう。調査機関のガートナー社は、世界のクラウドサービスへの支出は、2022 年に 4,820 億米ドル以上に達し、2020 年の 3,130 億米ドルから 54%増加すると予想しています⁵。また、ユーザの継続的なクラウドへの移行に伴い、サイバー犯罪者もそれに追従することになるでしょう。

サイバー犯罪者は、金銭的な利益を最大化するため、あらゆる手段を駆使して試行錯誤を繰り返し、同時に新たな技術を導入し、自分たちの攻撃活動というゲームを優位に進めようとしています。

企業は、サービスとしてのソフトウェア（SaaS：Software-as-a-Service）モデルのアプリケーションやソリューションを引き続き利用するだけでなく、2022 年には利用規模がさらに拡大すると考えられます。ガートナー社の予測では、SaaS のユーザの支出は 2022 年に約 1,720 億米ドルに達すると見込んでおり、これはすべてのパブリッククラウドサービスの中で最も高い支出額です⁶。サイバー犯罪者が採用している手法（TTP: Tactics, Techniques, and Procedures）は今でも有効であり、特に SaaS のユーザを狙う攻撃にも有効である可能性が高く、2022 年も引き続き同種の手法が確認されるでしょう。

サイバー犯罪者は、クラウドのアプリケーションやサービスにアクセスする際、労力は少なくても大きな影響を与える戦略を取るでしょう。フィッシングメールを利用して認証情報を窃取する手法は、2022 年も継続されると思われます。また、サイバー犯罪者は、セキュリティ保護されていない機密情報⁷、更新されていないアクセスキー、信頼できない情報源⁸から入手されたセキュリティ保護のないコンテナイメージ、未成熟または不十分に実装された認証アクセスコントロールの管理ポリシーなどを突いて、SaaS のアプリケーションやサービスを狙い続けるでしょう。実際、彼らは、効果的な手法を使い続ける傾向があります。例

³ <https://www.trendmicro.com/vinfo/us/security/news/security-technology/the-cloud-what-it-is-and-what-it-s-for>

⁴ <https://www.trendmicro.com/vinfo/us/security/news/security-technology/cso-insights-databank-mark-houpt-on-looking-beyond-securing-infrastructures-in-the-new-normal/>

⁵ <https://www.forbes.com/sites/bernardmarr/2021/10/25/the-5-biggest-cloud-computing-trends-in-2022/>

⁶ <https://www.gartner.com/en/newsroom/press-releases/2021-08-02-gartner-says-four-trends-are-shaping-the-future-of-public-cloud>

⁷ https://www.trendmicro.com/en_us/research/21/f/secure_secrets_managing_authentication_credentials.html

⁸ https://www.trendmicro.com/en_us/devops/21/e/container-security-first-steps-image-and-registry-scanning.html

えば、多くの環境において修正パッチが適用されていない現在、既知の脆弱性の多くがいまだに悪用されています。こうして、2022年に発見されるであろう新たな脆弱性だけでなく、まだ機能している旧来の脆弱性もリスクとなるでしょう。

2022年も、TeamTNTのようなサイバー犯罪者グループが、クラウドのコンピューティング能力を悪用して暗号資産の不正なマイニングを行うことが予想されます⁹。さらなる多くのデジタル通貨登場に伴い、さまざまなサイバー犯罪者グループは、既存の攻撃手法を繰り返して、被害者となるクラウドコンピューティングのリソースを悪用し続けるでしょう。

その一方でサイバー犯罪者は、テクノロジーの動向も注視してくるでしょう。これまでもJava¹⁰、Adobe Flash¹¹、WebLogic¹²などの技術を標的にしてきたように、広く採用されている技術は、攻撃者にとって格好の有利なターゲットとなります。

セキュリティのプロセスを開発工程の早い段階に組み込むシフトレフトの動きは、逆に攻撃者がこのアプローチを攻撃に利用するようになるリスクも懸念されるでしょう。実際、すでにクラウドの統合開発環境（IDE）内のDevOps¹³ツールやパイプラインを標的とする攻撃者の存在が確認されています¹⁴。こうした中、サイバー犯罪者により、サプライチェーンや、Kubernetes環境、IaC（Infrastructure-as-Code）デプロイメント、パイプラインなど、DevOpsの原則を逆手に取った攻撃キャンペーンの増加が予測されます。また、開発者やビルドシステムが、サプライチェーン攻撃によって複数の企業にマルウェアを拡散させようとする攻撃の最初のエントリーポイントとなることも予想されます。開発者のトークンとパスワードは、企業のオペレーションの鍵を握っており、攻撃者は、窃取されたこうした開発者の認証情報を使用することで、マルウェアを水面下で展開する可能性が懸念されます。

クラウドの導入は、デジタルトランスフォーメーションの基本的な要素です。そのため、企業にとっては、責任共有モデル¹⁵の理解と適用、十分に設計されたフレームワーク¹⁶の使用、暗号化、修正パッチの適用¹⁷、適切なレベルの専門家の導入など、クラウドセキュリティの基本に立ち返ることで、クラウド環境を安全に保つことが重要です。また、企業は、ビルドシステムや開発者がチェックインするコードに対して、より厳しいセキュリティプロトコルを適用する必要があります。特に、提出されたコードが重要な生産プロセスに関与する場合

⁹ <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/teamtnt-activities-probed>

¹⁰ https://www.trendmicro.com/en_us/research/13/i/java-security-situation-quietly-got-much-worse.html

¹¹ https://www.trendmicro.com/en_us/research/15/b/trend-micro-discovers-new-adobe-flash-zero-day-exploit-used-in-malvertisements.html

¹² <https://www.zdnet.com/article/oracle-warns-of-attacks-against-recently-patched-weblogic-security-bug/>

¹³ <https://www.trendmicro.com/vinfo/us/security/definition/devops>

¹⁴ https://www.trendmicro.com/en_us/research/20/c/security-risks-in-online-coding-platforms.html

¹⁵ <https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/cloud-security-key-concepts-threats-and-solutions>

¹⁶ https://www.trendmicro.com/en_us/devops/20/l/well-architected-framework-guide.html

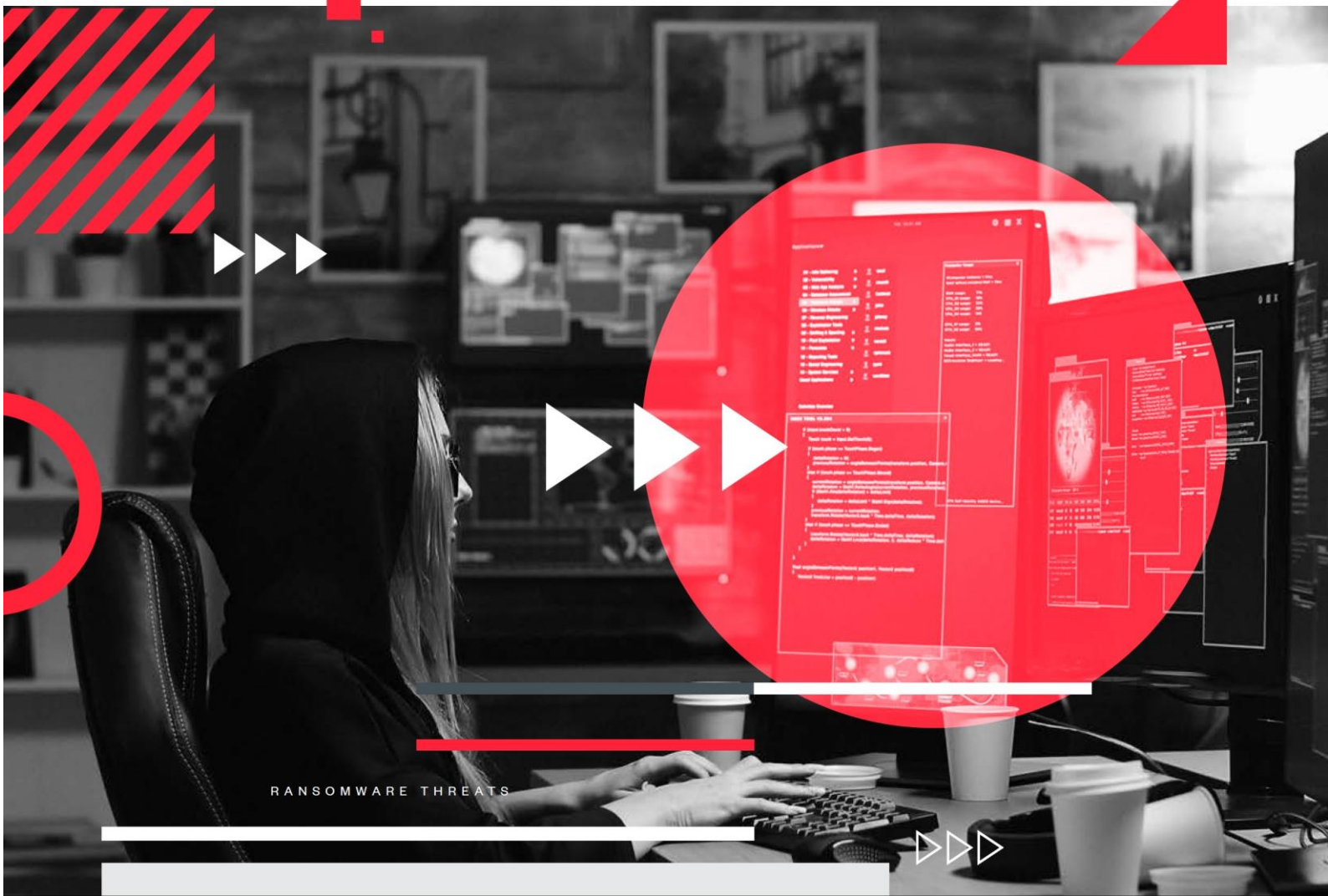
¹⁷ <https://www.trendmicro.com/vinfo/us/security/news/security-technology/security-101-virtual-patching>

はなおさらです。こうした状況に対処するため、企業のセキュリティ部門は、短命のアクセストークンによる権限の管理、コマンドラインツールによる監査証跡の作成、オープンソースのセキュリティ管理ソフトウェアによるパイプラインの監視などの対策を講じることができます。



ランサムウェア攻撃

進化するランサムウェアの脅威から身を守るため企業は、厳格なサーバのハードニングやアプリケーションコントロールのポリシーによるサーバの防御が不可欠となるでしょう。



RANSOMWARE THREATS



ランサムウェアにとって、サーバは格好の標的となるでしょう。

他の狡猾なサイバー犯罪と同様、ランサムウェア¹⁸も着実に進化しながら生き残り、被害を出し続けています。旧来のランサムウェアは、エンドポイントを主な侵入口としており、被害者は不正なメールを開いたり、ランサムウェアのペイロードが密かに展開される Web サイトにアクセスしたりすることで、攻撃の餌食となっていました¹⁹。しかし、パンデミックの発生に伴い、ランサムウェアの攻撃者の手法に明らかな変化が見られました。

企業へのアクセスを試みる攻撃者は、公開されたサービスやサービスサイドの構成要素に注目しています。また、ハイブリッドワーク（従業員がリモートとオンサイトの両方で働くモデル）が企業の新たな勤務スタイルとなっており²⁰、この傾向は 2022 年も続くことが予想されます。ハイブリッドワークモデルには、柔軟性や生産性の向上など多くの長所がありますが、サイバーセキュリティ上の短所があることも否めません。安全性の低い在宅勤務環境からのアクセスやクラウド上のリソースなど、攻撃対象が増えるため、サイバー犯罪者がどのように侵入して攻撃を仕掛けてくるのか、企業のセキュリティ部門がランサムウェアの攻撃をどのように阻止するのかを正確に把握することが困難になります。

また、2021 年に確認されたセキュリティインシデントに基づく、2022 年はランサムウェアに 2 つの大きな進展があると予測されます²¹。第一には、ランサムウェアによる攻撃がより標的型攻撃化および凶悪化の傾向を帯び、企業がこれらの攻撃からネットワークやシステムを防御することが難しくなることです。最新のランサムウェアが新たな手法を駆使してくる中、企業はエンドポイントに対する投資と同じように、クラウドを含めたサーバに対するランサムウェア対策の投資がまだ不十分である可能性が懸念されます。さらに、熟練したサイバーセキュリティの専門家の人材不足も、ランサムウェアの脅威から企業を守る上での懸念となっています²²。ランサムウェアの攻撃者が駆使する TTP は今後も変わることはないでしょうが、より複雑なターゲットへのより巧妙な攻撃で使用されることになり、これまでの主要なものより大規模な標的が狙われる可能性があります。

第二にランサムウェアの攻撃者は、より洗練された手段を用いて、いわゆる「state-sponsored」と呼ばれるレベルの高度な標的型攻撃手法に似た手口で、恐喝を行うことが予想されます²³。攻撃者は、被害者の環境に侵入すると、暗号化やアクセスブロックのステッ

¹⁸ <https://www.trendmicro.com/vinfo/us/security/definition/ransomware>

¹⁹ <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/-spam-be-ransomware-the-continuing-abuse-of-email-by-old-and-new-threats>

²⁰ <https://www.forbes.com/sites/forbestechcouncil/2021/06/04/going-hybrid-the-future-of-work-is-here/>

²¹ <https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/attacks-from-all-angles-2021-midyear-security-roundup>

²² <https://www.darkreading.com/careers-and-people/cybersecurity-talent-gap-narrows-as-workforce-grows>

²³ <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/modern-ransoms-double-extortion-tactics-and-how-to-protect-enterprises-against-them>



プを完全に省略して、機密データの窃取だけを実行し、その上で直ちに被害者への恐喝に遂行することができます。恐喝の主な手段としては、暗号化などによる機密情報へのアクセス拒否だけでなく、窃取した機密情報をさまざまな恐喝の手段として利用することに重点が置かれるでしょう。また、標的型メール（スパイフィッシング）、仮想プライベートネットワーク（VPN）やリモートデスクトッププロトコル（RDP）経由の侵入など、現在のランサムウェアの攻撃者が企業を狙う際に使用する常套手段は、今後も引き続き活用されるでしょう。その一方で 2022 年には、クラウド環境がより頻繁に狙われるようになるでしょう。多くの企業がクラウドに移行する中、機密情報やリソースもクラウド環境に保存されるようになり²⁴、サイバー犯罪者もそれに追随するでしょう²⁵。

サーバの安全性を確保するため、セキュリティのベストプラクティスを採用するだけでなく、関連するすべてのオペレーティングシステムやアプリケーションのサーバ・ハードニングガイドラインを厳密に遵守することで、企業は有益な対策を講じることができます。サーバが適切に設定されていることは、ランサムウェア攻撃やその他の脅威から企業を守ることにつながります。

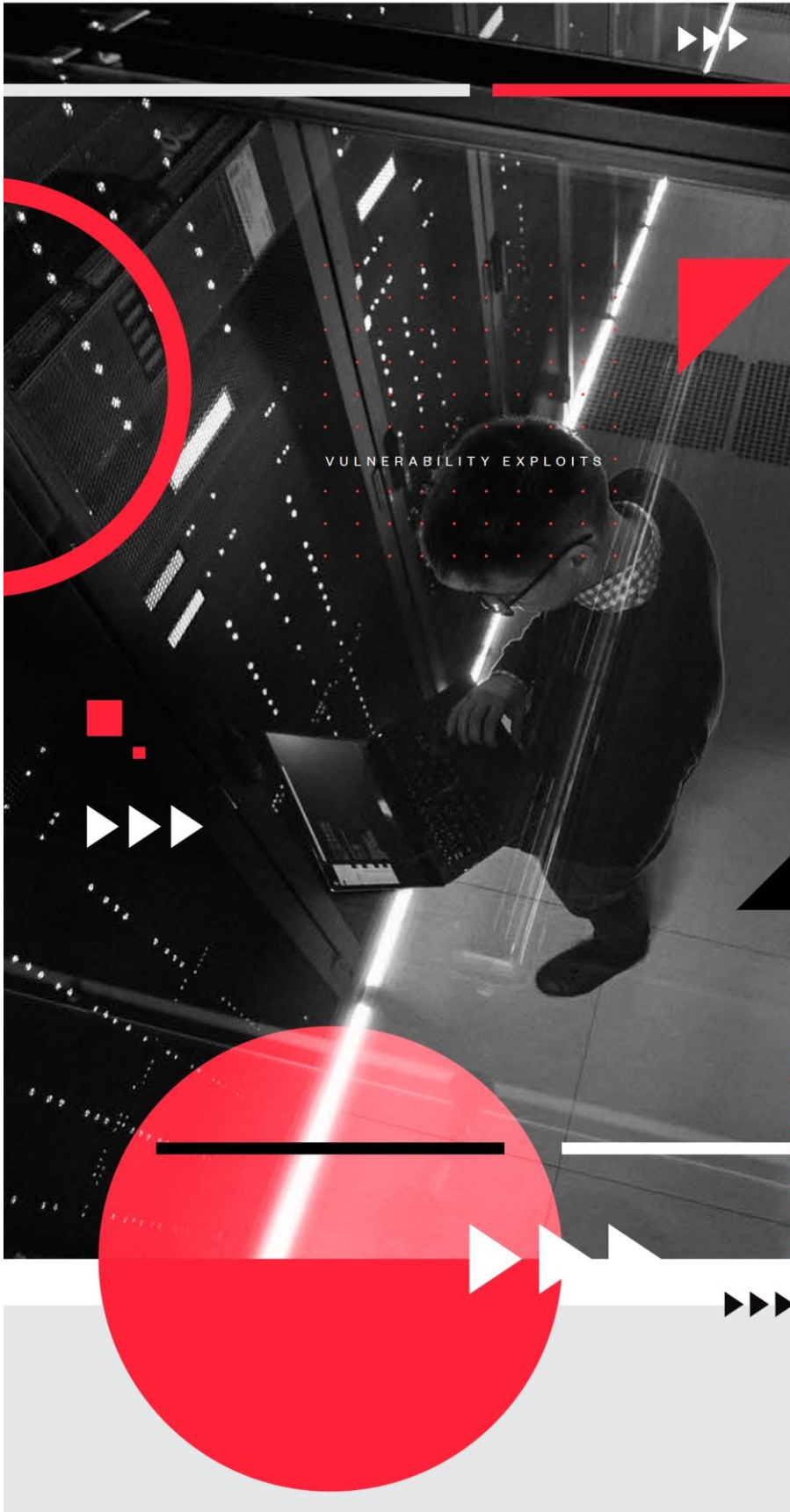
サーバには、その役割に基づいて使用するアプリケーションの特定が可能なため、アプリケーションコントロールを採用することも望ましいでしょう。企業の IT 部門がセーフリストに登録したアプリケーション以外のアプリケーションをブロックまたは制限することにより、強固なセキュリティが実現できます。

²⁴ <https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/undertaking-security-challenges-in-hybrid-cloud-environments>

²⁵ <https://techmonitor.ai/technology/cybersecurity/ransomcloud>

脆弱性攻撃

企業では、古い脆弱性の再利用や、新たに発見された脆弱性をすぐに悪用するような脆弱性攻撃への対策が必要になるでしょう



2021 年過去最高のゼロデイ脆弱性の攻撃への対処が迫られた中、企業は、より多くの脆弱性の発見が予想される 2022 年、潜在的な修正パッチ対応のギャップに対する警戒心を強めています。

2021 年には、過去最高規模のゼロデイ脆弱性の攻撃が脅威状況に影響を与えましたが、2022 年もこれに匹敵する事態が懸念されています。2021 年には、本稿執筆時点（2021 年 11 月）で、66 件のゼロデイ脆弱性攻撃が報告されており、これは過去のどの年よりも多い件数です²⁶。2022 年には、さらに多くのゼロデイ脆弱性攻撃が予測されますが、これは必ずしもソフトウェアやアプリケーションにおけるコードの質の低下を示唆するものではなく、他のさまざまな要因で生じるものと思われます。要因としては、ニュースになるような脆弱性を取り上げるメディアでの関心の高まり、ゼロデイ攻撃を防ぐためにトレンドマイクロの Zero Day Initiative (ZDI) が提供しているように、バグバウンティ²⁷で高額な賞金を獲得しようとする脆弱性ハンターの増加²⁸、デジタルトランスフォーメーションを行う企業の増加に伴って発生する実装上のミスや見落としなどが挙げられます。積極的に悪用されている脆弱性のうち、サイバーセキュリティ業界で発見されるものは一部に限られる可能性があるため、より多くの脆弱性が発見されることは、効果的な検出方法や情報公開に対する考え方にも変化をもたらすでしょう²⁹。バグバウンティプログラムは、企業にとって脆弱性の早期発見に大きく貢献しており、2019 年には ZDI のインセンティブがトレンドマイクロの顧客向けソリューションの開発に貢献しました。トレンドマイクロのセキュリティソリューション「TippingPoint™」では、ベンダが公開したパッチよりも平均 81 日早く仮想パッチが提供されたことからわかるように、その効果は絶大だったと言えます³⁰。

しかし、過去の Pwn2Own ハッキングコンテスト³¹が示唆するように、今や脆弱性の悪用までの時間は数日から数時間にまで短縮されています。そのため、ユーザ向けに修正パッチがリリースされる前、ベンダによる修正パッチの準備段階で、脆弱性悪用ツールが登場することになるでしょう。修正パッチのギャップとは、脆弱性が発見されてから、その脆弱性に対処するための修正パッチが提供されるまでの時間のことですが、チャンスを狙う攻撃者にとっては、重要な修正対応が遅れることは、脆弱性を悪用するための十分な時間が確保できるという点で、格好の攻撃機会となり続けるでしょう。修正パッチの配布自体の遅れも、ソフ

²⁶ <https://www.technologyreview.com/2021/09/23/1036140/2021-record-zero-day-hacks-reasons>

²⁷ <https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/trends-and-shifts-in-the-underground-n-day-exploit-market>

²⁸ <https://newsroom.trendmicro.com/2021-05-19-Trend-Micros-Zero-Day-Initiative-Enhances-Position-as-Worlds-Largest-Vulnerability-Disclosure-Player>

²⁹ <https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks/>

³⁰ https://www.trendmicro.com/en_us/research/21/d/how-trend-micro-helps-manage-exploited-vulnerabilities.html

³¹ <https://www.zdnet.com/article/microsoft-july-2021-patch-tuesday-117-vulnerabilities-pwn2own-exchange-server-bug-fixed/>

トウェアでのテストの必要がある場合に発生することがあり、Google Chrome の JavaScript エンジン「V8」の修正プログラムは、実際に作成されてから 1 ヶ月後の 2019 年 9 月に「Chrome 77」のリリースにあわせて提供されました³²。このため、企業は、修正パッチ作成までの時間よりも早く実行される攻撃、修正パッチの配布・実装に要する時間の遅延という 2 つの課題に直面し、厳しい状況に置かれることになります。エンドポイントへの修正パッチ適用は、サーバへのパッチ適用よりも迅速に実施できるものの、いずれにせよ、ダウンタイムによるコストが発生することが多く³³、脆弱性への対応は一筋縄にはいきません。

攻撃者は、コードに欠陥がないか大規模な調査をする代わりに、システムの穴を示す便利な指標として修正パッチに注目し、そこからマルウェアの不正コードを作成するようになるでしょう。2022 年、サイバー犯罪者の一部は、企業を注視しつつ、公開された脆弱性や修正パッチ適用の際を突いた攻撃に展開してくるでしょう。

攻撃者は、新しく発見された脆弱性だけでなく、古い脆弱性も利用し続けるでしょう。そのため、企業とそのパートナーであるベンダは、修正パッチの管理体制を優先する必要性があります。攻撃者の中には、過去に発見された脆弱性を再利用したり、組み合わせたりして、攻撃手法を強化してくるため、過去の脆弱性に関しても注意が必要です。

同様に、複数のソフトウェア製品をまとめて狙う攻撃も登場するでしょう。例えば、Google Chrome の脆弱性と Microsoft Windows の脆弱性をデジチェーン接続することで、一度にシステムへの特権的アクセスを獲得するような複合的な攻撃が増加するでしょう。こうした攻撃の増加に伴い、セキュリティ専門家は、これまであまり調査されてこなかった攻撃対象にも関心を向けることになるでしょう。例えば今後、Microsoft Exchange や SharePoint などのプラットフォームの弱点を明らかにし、こういった攻撃によるエンドユーザーへの影響を軽減するためのサーバ側の技術に特化した研究が進むことが期待されます。

クラウドネイティブのセキュリティは、パンデミックの影響でデジタルトランスフォーメーションを加速させた後にクラウドを採用した企業の多くにとっても優先事項となっています。クラウドネイティブのプロジェクトの多くは、オープンソースソフトウェアで構築されたライブラリに依存しているため、既知の脆弱性を悪用した攻撃にさらされる可能性³⁴があります。企業のセキュリティ部門チームにとっては、クラウドの欠陥について信頼できる情報源を見つけることが、クラウドの資産を保護する上で重要となります。なぜなら、オンプレミスの脆弱性に比べて、クラウドに関連する共通の脆弱性および公開情報（CVE 番号）の報告がまだ不足しているからです³⁵。

³² <https://www.zdnet.com/article/security-researchers-expose-another-instance-of-chrome-patch-gapping/>

³³ <https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-nightmares-of-patch-management-the-status-quo-and-beyond>

³⁴ <https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/minding-the-gaps-the-state-of-vulnerabilities-in-cloud-native-applications>

³⁵ <https://searchsecurity.techtarget.com/news/252508948/Why-cloud-bugs-dont-get-CVEs-and-why-its-an-issue>

企業はこれまで以上に、IT セキュリティ部門がこうした攻撃の急増に適応し、対処するための体制を整える必要があります。そのためには、資産管理によって IT 環境のデバイスを把握し、ベンダからのセキュリティアップデートを監視して、脆弱性が公開されたらすぐに対応できるようにした上で、仮想パッチの適用³⁶や端末の隔離によって潜在的な脅威の侵入口を阻止するなど、必要なサポートやリソースを確保する必要があります。

³⁶ <https://www.trendmicro.com/vinfo/us/security/news/security-technology/security-101-virtual-patching>



従来型マルウェア攻撃

攻撃者が今後も中小企業を狙ってくる中、クラウドを多用する中小企業は、コモディティ化された従来型マルウェアの攻撃を回避するためのセキュリティ対策を講じるでしょう



ランサムウェアに注目が集まる一方で、従来型の攻撃手法や攻撃サービスは、より洗練されたツールの開発に時間を費やすでしょう。

大企業は今後も、巨額の報酬を狙うランサムウェアの攻撃者の格好の餌食となるでしょう。一方、さまざまな攻撃者が一攫千金を狙う中、サービスとしてのランサムウェア（RaaS）のやコモディティ化されたマルウェアが活用され、中小企業も、小規模なサイバー犯罪者の格好の餌食となるでしょう³⁷。

ここ数年、世間の注目がランサムウェアに集まる中、ランサムウェア自体は、コモディティ化されたマルウェアのサービスモデルと見なされてくるでしょう。一方、リモートアクセスツール（RAT）、情報窃取型マルウェア、コインマイナー、ドロPPER、ローダーなどのその他の既存のさまざまなマルウェアもサイバー犯罪者の間で流通し続けるでしょう。これにより、一般的なマルウェアの市場は、陰湿かつ手ごわい脅威へと成長していくでしょう。ランサムウェアの攻撃者は、攻撃をより効果的にするため、各種の従来型マルウェアや一般的なツールを利用しています³⁸。またその他にも、標的型攻撃の攻撃者も自らの攻撃キャンペーンを展開するために、一般的なツールを利用しています³⁹。ランサムウェアの攻撃者も同様に、Cobalt Strike、Koadic、PowerShell Empire、Metasploit⁴⁰などの汎用的なツールを、既存のシステム管理ユーティリティと組み合わせて使用することが確認されています。これは、以前から標的型攻撃の基本戦略となってきた「環境寄生型（living off the land）」と呼ばれる攻撃手法であり、検知の回避などで活用されます⁴¹。

これらの一般的な各種ツールは、より高度な機能を備え、価格も手ごろであるため、ツールボックスを増やそうとする攻撃者にとって、利用しやすいものとなっています⁴²。これらのツールによりカスタマイズされたマルウェアの多くは、最終的にサイバー犯罪アンダーグラウンド市場で商品化され、他の攻撃者やサイバー犯罪者が利用できるようになります⁴³。このことから、次世代の攻撃者やサイバー犯罪者は、15年ほど前にランサムウェアを開発した攻撃者よりも、より革新的で優れた能力を備えていることが考えられます⁴⁴。コモディティ化された攻撃ツールの市場は、新規参入の攻撃者やサイバー犯罪者とともに成熟していくだけでなく、彼らによってネットワークが拡大し、同じ目的を持つサイバー犯罪者たちとつながるための手段として活用されることも予想されます。実際、こうしたツールの販売者は、

³⁷ <https://apnews.com/press-release/pr-businesswire/7f2907b6661b426c855e4875511266e1>

³⁸ <https://shop.bsigroup.com/articles/how-your-business-can-adapt-to-cybersecurity-trends>

³⁹ <https://about.fb.com/news/2021/11/taking-action-against-hackers-in-pakistan-and-syria/>

⁴⁰ <https://blogs.vmware.com/security/2021/10/moving-left-of-the-ransomware-boom.html>

⁴¹ <https://www.csoonline.com/article/3541810/ryuk-ransomware-explained-a-targeted-devastatingly-effective-attack.html>

⁴² https://www.trendmicro.com/en_us/research/21/i/apt-c-36-updates-its-long-term-spam-campaign-against-south-ameri.html

⁴³ <https://www.ncsc.gov.uk/guidance/white-papers/common-cyber-attacks-reducing-impact>

⁴⁴ <https://www.trendmicro.com/vinfo/us/security/definition/ransomware>

すぐに使えるマルウェアだけでなく、攻撃にあたってのノウハウを伝える、説明書、ヒント、トラブルシューティングガイドなどを提供してきました⁴⁵。

このため、マルウェアを一度だけ購入するのではなく、サービス契約の一部として販売するサービスモデルは、経験の浅いサイバー犯罪者に適しています。そして彼らが経験豊富な攻撃者に成長するにつれ、より巧妙化されたツールを必要とすることから、信頼できるサイバー犯罪活動のパートナーを求めるようになるでしょう。このような協力関係は、サイバー犯罪活動の回復力を高めることにつながります。例えば、Emotet の攻撃者は、法執行機関によって Emotet のインフラが破壊されたわずか数カ月後に、バンキングマルウェア Trickbot のボットネットを利用して Emotet のボットネットを再構築することができました⁴⁶。このように、コモディティ化された従来型の攻撃は、2022 年、攻撃者が自らオーダーメイドのマルウェアを開発する必要性がほとんどなくなるレベルに成熟することが予想されます。複雑な標的型攻撃の場合でも、さまざまなツールやサービスを提供する他のサイバー犯罪者をよりよく管理することが主要な活動となるでしょう。

この点から、コモディティ化されたマルウェアの市場では、攻撃者が自身の手法をアップグレードできるような、より洗練された攻撃ツールが待ち望まれています。2022 年には、Zeus ボットネットの改良版⁴⁷のように、クラウドベースと IoT プラットフォームの両方を同時に侵害して制御するように設計されたサービスとしてのボットネットが登場する可能性があります。このようなツールは、革新的なマルウェアが多いことで知られるロシアのサイバー犯罪者のアンダーグラウンド市場から登場する可能性があります⁴⁸。ボットネット FreakOut などは、機能を追加して進化を続けており、そうしたサービスの候補の 1 つとなっているようです⁴⁹。

ただし、このようにコモディティ化された攻撃手法は、当然ながら攻撃ごとの変化は少ないため、機械学習を用いたセキュリティシステムなど大企業の環境で見られる強固な防御を侵害することは難しい可能性があります⁵⁰。そのため、コモディティ化された従来型の攻撃は、比較的セキュリティの防御力が低い中小企業などを主なターゲットとして狙うようになることが予測されます。コモディティ化されたマルウェアのツールは、ターゲットを対象に定めて、他のサイバー犯罪者との競争が少ないことを望む攻撃者に採用されるでしょう。具体的には、中小企業が使用する IoT デバイスが、こうした攻撃の主要なターゲットになると予測

⁴⁵ <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/crimeware-for-sale-the-commoditization-of-atm-malware-in-the-cybercriminal-underground>

⁴⁶ <https://www.bleepingcomputer.com/news/security/emotet-malware-is-back-and-rebuilding-its-botnet-via-trickbot>

⁴⁷ <https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/16/the-zeus-zbot-and-kneber-connection>

⁴⁸ <https://www.newyorker.com/news/news-desk/how-hacking-became-a-professional-service-in-russia>

⁴⁹ <https://www.zdnet.com/article/new-freakout-botnet-targets-linux-systems-running-unpatched-software/>

⁵⁰ <https://www.trendmicro.com/vinfo/us/security/definition/machine-learning>

されます。そのため、IoT デバイスを導入する中小企業は、ベンダを選ぶ目を養い、しっかりとした修正パッチの履歴を誇るメーカーから IoT 機器を購入する必要があるでしょう。

中小企業が自社のセキュリティ部門を持つことは稀であり、持っていたとしても、限られた資金の中で制約を受け、サイバーセキュリティは単なる運営費の一部に過ぎないと考えられがちです。世界的に見て、サイバーセキュリティ関連の支出は 2021 年末までに 1,500 億米ドルを超える見込み⁵¹ですが、中小企業が IT セキュリティのソリューションに費やす費用は、年間 400 億米ドル強に過ぎず、成熟した中小企業だけが社内にセキュリティ人材を確保するなど、十分なサービスが行き渡っていない市場となっています⁵²。多くの中小企業は、予算が限られていることから、エンドポイントのセキュリティ確保を最優先し、その次にネットワークの防御を講じるという優先順位になると考えられます。他方、中小企業の中には、他の企業よりもさらに準備ができていないケースもあるでしょう。例えば、クラウドベースのサービスやプラットフォームを多く利用するオンラインベースの中小企業は、そのビジネスの性質上、一般的なマルウェア攻撃が自社の重要業務に及ぼすリスクをより強く認識しているでしょう。こうした企業は、セキュリティを全社的な課題の一部と見なしてサイバーセキュリティのソリューションを売上原価の一部として計上する傾向があります。

⁵¹ <https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem>

⁵² <https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/securing-small-and-medium-size-enterprises-whats-next>



IoT の脅威

企業は、IoT の導入によって生じる脅威から IT 環境を守るためにネットワークの監視と可視性の向上に努めるでしょう。



IoT に関連する情報は、サイバー犯罪アンダーグラウンド市場でも注目されるようになり、企業は情報漏えいや改ざんが懸念されるセキュリティギャップにより一層の注意を払うようになるでしょう。

IoT デバイスの多くは計算能力が限られており、セキュリティソリューションを組み込む余地が少ないため⁵³、攻撃者にとって格好の標的となってきました。侵入された IoT デバイスは、DDoS (Distributed Denial of Service) 攻撃⁵⁴など、さまざまな攻撃に利用されてきました。世界的な金融不安の中、競争力の維持や業務改善のため、デジタルトランスフォーメーションを迫られる企業が増える中、特にスマート製造業の企業は、ハイブリッドワークモデルへの移行やリモート接続サービスの継続的な利用に伴い、より多くの脅威にさらされることになると予想されます。

IoT デバイスを利用している企業では、2022 年、侵入防止・検知システム (IPS/IDS)、ネットワークフォレンジックツール (NFT)、ネットワーク動作異常検知 (NBAD) ツール、ネットワーク検知・応答 (NDR) ツールなどを利用してネットワークの動きを監視するセキュリティ対策が増加してくるでしょう。そうした中、クラウド導入に移行してサードパーティのセキュリティベンダに依存する企業の場合、クラウドのリソース使用状況に異常がないか、クラウドのインフラ内で発生する攻撃から仮想プライベートクラウド (VPC) が保護されているか、候補のセキュリティベンダの機能が自社のニーズに合っているかなどの確認が不可欠となるでしょう。

2022 年、サイバー犯罪者は、IoT デバイスを攻撃拠点やネットワーク内で水平移動に利用するだけでなく、より高度な標的を狙うようになるでしょう。例えば、ゼネラルモーター、ホンダ、トヨタなどの大手自動車メーカー⁵⁵によるコネクテッドカーがもたらすデータトラフィックに狙いを定めることで、攻撃者は、新たな領域のサイバー犯罪ゴールドラッシュに参加することになるでしょう。これらのコネクテッドカーには、カメラやレーザーなどのセンサーが多数搭載されており、走行速度や距離のほか、乗客が利用したエンターテインメントメディアの種類など、走行状況やドライバーの行動の記録が可能になります。こうしたリアルタイムの情報は、広告効果の測定、消費者の需要の把握、運転データに基づく自動車保険の割引決定など、商業顧客にとって無数のビジネス用途があります⁵⁶。また、自動車メーカーにとっては、このデータを利用して自動車部品の性能をモニタリングすることで、自社のサプライチェーンを強化することができます⁵⁷。

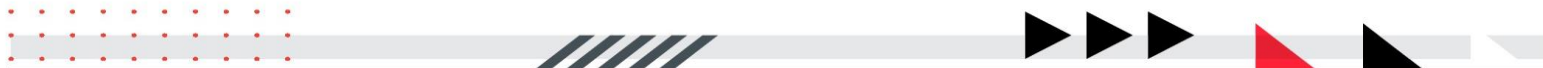
⁵³ <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/smart-yet-flawed-iot-device-vulnerabilities-explained>

⁵⁴ <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-security-101-threats-issues-and-defenses>

⁵⁵ https://www.trendmicro.com/en_us/research/21/j/honda-to-start-selling-smart-car-data.html

⁵⁶ <https://asia.nikkei.com/Business/Technology/Honda-joins-400bn-gold-rush-to-monetize-smart-car-data>

⁵⁷ <https://www.techradar.com/news/amazon-and-nxp-team-up-on-smart-car-cloud-computing-deal>



こうしたコネクテッドカーの情報に関する需要は、2030年までに約4,500~7,500億米ドルの価値があると予測され⁵⁸、衰えることのない新しいビジネスになると考えられています。そして2025年には、コネクテッドカーから毎月10エクサバイトのデータが得られると予測されています⁵⁹。そうした中、コネクテッドカーの増加に伴い、サイバー犯罪者は、それらの接続情報から利益を得ようとし、リスクデータの報告をブロックする違法なデータフィルタや、コネクテッドカーの記録から悪質な運転を消去するハッカーの需要が高まると考えられます。コネクテッドカーのアーキテクチャは、より複雑なデータ収集機能やプロセスをクラウドに移行させることで、さらに合理化が進むでしょう。実際、最新のコネクテッドカーのモデルで使用されている多くのアプリケーションやシステムは、すでにバックエンドのクラウドサーバ上にホストされているため⁶⁰、自動車メーカーは、これらのサーバを狙ったサービス妨害（DoS）攻撃や中間者（MitM）攻撃などの別の脅威にさらされる可能性があります⁶¹。

2022年の自動車メーカーは、自社製品の将来性を確保するために、セキュリティベンダと緊密に連携し、どのようにセキュリティを実装するかセキュリティ対策の判断が迫られることとなります。このようなパートナーシップの取り組みはすでに始まっています。初期の取り組みとしては、Mobility in Harmony（MIH）コンソーシアムやそのパートナーであるArm社、Microsoft社、トレンドマイクロが主導しているOpen EV Software Platformが挙げられます⁶²。また、フォルクスワーゲンとMicrosoft社は、共同で自動車メーカーがコネクテッドカー向けのより高度で安全な自動運転ソリューションを開発するためのクラウドベースのプラットフォームを構築しようとしています⁶³。このようなプロジェクトが増えれば、自動車業界がコネクテッドカー向けの専用OSを開発するための基盤が整い、統一されたOS上に構築された自動車のエコシステムが最終的な目標となって、将来のコネクテッドカーに標準的なセキュリティ機能を搭載することが可能になります。

⁵⁸ <https://www.forbes.com/sites/markminevich/2020/07/13/the-automotive-industry-and-the-data-driven-approach/>

⁵⁹ <https://global.toyota/en/detail/18135029>

⁶⁰ <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/in-transit-interconnected-at-risk-cybersecurity-risks-of-connected-cars>

⁶¹ https://www.trendmicro.com/en_us/research/21/b/connected-cars-5g-the-cloud-opportunities-and-risks.html

⁶² <https://www.mih-ev.org/en/news-info/?id=695>

⁶³ <https://news.microsoft.com/2021/02/10/volkswagen-group-teams-up-with-microsoft-to-accelerate-the-development-of-automated-driving>





サプライチェーンを 狙う脅威

企業は、多様化や地域化によってサプライチェーンのより強固なセキュリティに注力するとともに、ゼロトラスト原則を導入して環境をより安全なものにしましょう。

企業がサプライチェーンのオペレーションを進化させていく一方、グローバルのサプライチェーンは四重の脅威にさらされることになります。

新型コロナの世界的な流行では、企業のサプライチェーンが厳しい批判の目にさらされました。経済活動の不足や遅延などが、需要増加⁶⁴、輸送コンテナや労働力の不足⁶⁵、ジャストインタイム製造モデル⁶⁶のスリムな生産システムへの長年の依存など、いくつかの要因が重なって発生しました。そしてサプライチェーンの問題が世界規模に拡大したことで、苦境に立たされた企業だけでなく、新型コロナの流行に伴って勢いを増すサイバー犯罪者にとっても、サプライチェーンの価値が明らかになりました。特に2021年は、Quanta Computer 社⁶⁷、JBS Foods 社⁶⁸、Kaseya 社⁶⁹などの大企業を狙ったランサムウェア REvil/Sodinokibi⁷⁰の攻撃に代表されるように、サプライチェーンを狙った攻撃とランサムウェア攻撃キャンペーンとの関連性が強くなってきました。

そして2022年、サプライチェーンを巡る混乱を利用して悪化させるため、攻撃者による四重の恐喝モデルが急増することが予想されます⁷¹。つまり、被害者の機密情報を質に身代金を要求する、機密情報を公表すると脅す、被害者の顧客を狙うと脅す、被害者のサプライチェーンやベンダを攻撃する、という4つの恐喝手法を用いて、被害を受けた大企業を恐喝して大金を支払わせるなど、さまざまな手口を最大限に活用してくるでしょう。

2021年、サイバー犯罪集団「DarkSide」は、米国最大の精製石油パイプラインシステムのColonial Pipeline社を標的に攻撃を仕掛けました。彼らは、同社のコンピュータシステムへのアクセスを妨害し、100GB以上の企業データを盗み出しました⁷²。また、このサイバー犯罪集団は、他の攻撃者向けにDDoSサービスやコールセンターサービスを提供し、攻撃戦略を常に革新化させています⁷³。これにより、DarkSideのサービスを利用するアフィリエイトは、サプライチェーンに大きな影響を与える四重の恐喝技術を展開することができます。その結果、攻撃者は、攻撃された企業において製造秘密などの重要なデータへの使用不能にし

⁶⁴ <https://www.forbes.com/sites/garthfriesen/2021/09/03/no-end-in-sight-for-the-covid-led-global-supply-chain-disruption/>

⁶⁵ <https://www.nytimes.com/2021/10/04/books/book-publishing-supply-chain-delays.html>

⁶⁶ <https://www.nytimes.com/2021/06/01/business/coronavirus-global-shortages.html>

⁶⁷ https://www.trendmicro.com/en_us/research/21/a/sodinokibi-ransomware.html

⁶⁸ <https://www.crn.com/news/security/apple-menaced-after-revil-ransomware-attack-against-supplier>

⁶⁹ https://www.trendmicro.com/en_us/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html

⁷⁰ https://www.trendmicro.com/en_us/research/21/g/it-management-platform-kaseya-hit-with-sodinokibi-revil-ransomwa.html

⁷¹ <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti>

⁷² <https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/attacks-from-all-angles-2021-midyear-security-roundup>

⁷³ <https://krebsonsecurity.com/2021/05/a-closer-look-at-the-darkside-ransomware-gang/>

たり、製造に使用する機械へのアクセスできなくさせたり、顧客や関係者への攻撃を実行したりして、恐喝による金銭の支払いを迫ることができます。

サービスとしてのアクセス (AaaS、access-as-a-service) の運営者もサプライチェーンに注目するでしょう。AaaS の運営者は、脆弱な企業の実環境への侵害が確認されると、それに乗じて、企業のネットワークアクセス、管理アカウント、認証情報などをさまざまな価格でサイバー犯罪者に販売します。

新型コロナの世界的流行を契機とした経済的变化により、企業はサプライチェーン開発プロセスへの投資を余儀なくされます。そして多角化のアプローチにより、さらに強固なサプライチェーンオペレーションを構築することに注力するでしょう。長年、各国はグローバル化を推進してきましたが、多くの国が単一の地理的ソースからの供給に過度に依存している構図が批判されてきました⁷⁴。今後、グローバル化に代わって、サプライチェーンのオペレーションは地域化され、企業は需要の増加や生産コストの変動に対応できるようになります。こうした多角化の戦略は企業によって異なり、サプライチェーンの拠点のいくつかは地元であり、その他は、海外の国や地域にあるといった状況も想定されます。

しかし、多角化を適切かつ安全に行うことは容易ではなく、コストとリソースを要する努力が必要となります。経済的なリスクを軽減してビジネスを維持することを優先するため、身近なベンダやサプライヤーに固執する企業は、知らず知らずのうちにセキュリティリスクへの扉を開いているかもしれません。長年取引してきたサプライヤーが別の企業に取って代わられる際、その新たな取引先のセキュリティ評価が必要になります。これらの新しいベンダがクラウドアプリケーションやサービスを提供していても、そのセキュリティポリシーが適切ではないかもしれませんし、最悪の場合、クラウドセキュリティをまったく優先していないかもしれません。

取引する企業同士が双方のプロセスを調整する期間は非常に重要です。攻撃者は、新しいパートナーシップに伴う変化や不慣れさを利用して、標的型攻撃を仕掛けることができます。例えば、新しいサプライヤーの人物になりすまして不正な Web サイトに関連する企業情報を入力するよう受信者に要求するスパイフィッシングメールを送信することも可能です。

企業が戦略を進化させていく中でサプライチェーンを安全に保つためには、セキュリティ対策にゼロトラストアプローチを適用する必要があります⁷⁵。ゼロトラストモデルは、企業が他の企業と交流し、データを交換する際に、接続の有効期間中に継続的な検証を行うことで、その安全性を確保します。このモデルにより、企業は、ユーザ、デバイス、アプリケーション、サービスの健全性が常に監視され、評価されていることを確認できます。

⁷⁴ <https://www.nytimes.com/2021/10/14/opinion/supply-chain-america.html>

⁷⁵ https://www.trendmicro.com/en_us/ciso/21/h/what-is-zero-trust-and-why-does-it-matter.html



まとめ：サイバーセキュリティ対策のスピード化

本稿「2022 年セキュリティ予測」では、差し迫ったセキュリティ上の懸念や技術に関して、トレンドマイクロのセキュリティ専門家による調査、確認、洞察などから浮かび上がってきた脅威やリスクの概要を示しています。これらの問題に対処するためには、以下のようなセキュリティ上の推奨事項を含む、総合的かつ多層的なサイバーセキュリティ戦略が有効です。

セキュリティの基本に立ち返る：

単純なことのようには思えるかもしれませんが、まず何よりも、セキュリティのベストプラクティスを順守することで、2022 年に迫り来る新旧の脅威の大半に対抗することができます。攻撃者は、システムやアプリケーションの古い脆弱性を悪用し続けるため、企業はパッチマネジメントポリシーを常に把握すると共に、技術的回避策を検討しておくことが重要です。また、クラウドを利用する企業は、責任共有モデルを理解して適用し、クラウド上の機密情報を適切に暗号化しておく必要があります。

ゼロトラストモデルを実装し、自社環境とアプリケーションを安全に保つ：

企業は、ゼロトラストモデルを適用することで、セキュリティ体制を向上させることができます。このモデルでは、アプリケーションやシステムに接続しようとするユーザやデバイスは、ネットワーク内であるかどうかに関わらず、アクセスを許可される前に必ず検証され、その後も継続的に検証されることになります。

サーバのセキュリティを強化し、アクセスコントロールを採用する：

ハイブリッドワークモデルへの移行に伴い、ネットワークにおける境界線の曖昧化が進むことを考慮したセキュリティポリシーを策定し、導入することが求められます。アクセスコントロールとアプリケーションコントロールを導入することで、従業員がさまざまなデバイスから機密性の高い重要な業務向けのアプリケーションや情報にどこからアクセスしても、企業は全体的なセキュリティをより適切に管理することができます。

可視性を優先する：

2022 年、社員がクラウドのアプリケーション、サービス、システム、データベースにリモートでアクセスするようになると、企業にとっては、サイバーセキュリティの防御を強化するため、可視性を前面に押し出すことが重要になります。企業のセキュリティ部門は、すべてのクラウドプロバイダ、アカウント、サービスを把握し、それらが可能な限り安全に構成されていることを確認する必要があります。これにより、意図しない暴露や設定ミスリスクを最小限に抑えることができます。

適切なソリューションとレベルの高い専門知識による強固なセキュリティ対策を導入する：

日々進化する脅威からシステムや環境をうまく保護するため、企業は、メール、エンドポイント、ネットワーク、サーバ、クラウドのワークロードなどの各レイヤーにおける攻撃を効率的に検知する柔軟で自動化された高度なセキュリティソリューションを必要としています。そしてこのような複数のレイヤーから複数の対策技術により検知される攻撃の兆候を、横串で相関分析できるソリューションも必要とされています。また常に変化する脅威に対応し続けるためには、広範なセキュリティ分析、強力なセキュリティソリューション、そしてグローバルな脅威情報にアクセスできる専任のセキュリティアナリストチームによる徹底した調査の詳細やセキュリティの知見が必要とされます。

TREND MICRO

本書に関する著作権は、トレンドマイクロ株式会社へ独占的に帰属します。

トレンドマイクロ株式会社が書面により事前に承諾している場合を除き、形態および手段を問わず本書またはその一部を複製することは禁じられています。本書の作成にあたっては細心の注意を払っていますが、本書の記述に誤りや欠落があってもトレンドマイクロ株式会社はいかなる責任も負わないものとし、本書およびその記述内容は予告なしに変更される場合があります。

本書に記載されている各社の社名、製品名、およびサービス名は、各社の商標または登録商標です。

〒151-0053

東京都渋谷区代々木 2-1-1 新宿マインズタワー

大代表 TEL : 03-5334-3600 FAX : 03-5334-4008

<http://www.trendmicro.com>

トレンドマイクロはサイバーセキュリティのグローバルリーダーとしてデジタル情報を安全に交換できる世界の実現に貢献します。私たちの革新的なソリューションはデータセンター、クラウド、ネットワーク、エンドポイントにおける多層的なセキュリティをお客様に提供します。

当社のリーダーシップの根幹であるトレンドマイクロリサーチは、多くのエキスパートに支えられています。それは最新の脅威を発見し、重要なインサイトを公に共有し、サイバー犯罪の防止を支援することに情熱を注ぐ人材です。当社のグローバルチームは、日に数百万もの脅威を特定し、脆弱性の開示を先導し、標的型攻撃・AI・IoT・サイバー犯罪等における革新的な研究結果を公表しています。私たちは次に来る脅威を予測し、セキュリティ業界が進むべき方向を示しうる示唆に富んだ研究成果を提供するため、継続的に取り組んでまいります。



© 2021 Trend Micro Incorporated. All Rights Reserved.