Microsoft

マイクロソフト デジタル防衛レポート 2022

脅威の状況を明確に示し、デジタル防衛の強化方法を提示する

目次

このレポートに含まれるデータ、インサイト、イベントは、特に明記されていない限り 2021 年 7 月から 2022 年 6 月 (マイクロソフト会計年度 2022) までのものです。

このレポートをできる限り快適に表示してナビゲートするため、Adobe Reader の使用をお勧めします。Adobe Reader は、Adobe Web サイトから無料でダウンロードできます。

カスタマー セキュリティ & トラスト担当コーポレート バイス プレジデントの Tom Burt によるイントロダクション

「マイクロソフトが世界にまたがる製品およびサービスのエコシステムから分析した何兆ものシグナルにより、世界中のデジタル脅威の凶暴性、範囲、規模が明らかになります」

現在の状況に関する豆知識…

生じている脅威の範囲と規模

パスワード攻撃の量は、1 秒ごとに推定 921 件増えています。わずか 1 年で 74% の増加です。

サイバー犯罪の根絶

現在までに、マイクロソフトはサイバー犯罪者によって使用されている 1 万件以上のドメインを削除しました。600 件は、国家のアクターによって使用されていました。

脆弱性への対処

ランサムウェア インシデント対応エンゲージメントのうち 93% で、特権アクセスと侵入拡大に関する統制が不十分であることが明らかになりました。

2022 年 2 月 23 日、サイバーセキュリティの世界は新しい時代、つまりハイブリッド戦争の時代を迎えました。その日、ミサイルが発射されて戦車が国境を越える数時間前に、ロシアのアクターがウクライナ政府、テクノロジ、金融セクターの標的に対して大規模で破壊的なサイバー攻撃を開始しました。これらの攻撃とそこから学べる教訓について詳しくは、「マイクロソフト デジタル防衛レポート」(MDDR) 第 3 年次版の「国家レベルの脅威」の章をご覧ください。これらの教訓の鍵は、クラウドはサイバー攻撃に対する物理的および論理的な最高のセキュリティを実現し、ウクライナで価値が実証されたように脅威インテリジェンスとエンドポイント保護における進歩を可能にするという点です。

その年のサイバーセキュリティの動向に関する調査は必ずそこから始まりますが、今年のレポートではるかに多くのことが明らかになっています。レポートの最初の章ではサイバー犯罪者の活動に焦点を当て、第 2 章では国家レベルの脅威について扱います。どちらの陣営も攻撃の巧妙さを大幅に高めており、その行動の影響は劇的に高まっています。ロシアは見出しを操った一方で、イランのアクターは大統領の権限を移行した後攻撃をエスカレートさせ、イスラエルを標的とする破壊的な攻撃を開始しました。また、米国の重要インフラを対象とし、ランサムウェアとハック アンド リークを稼働させています。さらに、中国は、米国の影響力に対抗し、重要なデータと情報を盗むため、東南アジアをはじめとするグローバル サウスでのスパイ活動を強化させています。

また、第 3 章で説明するように、外国のアクターは、非常に効果的な手法を使って世界中の地域でプロパガンダの影響力を強めています。たとえば、ロシアはウクライナへの侵略が正当なものであることを、自国の国民や他の多くの国の国民が信じ込むよう力を尽くしています。さらに、西側諸国で新型コロナウィルス感染症ワクチンへの不信を植え付けるプロパガンダ広めると同時に、自国ではその効果を宣伝しています。加えて、第 4 章で説明するように、アクターはネットワークと重要インフラへのエントリ ポイントとして、モノのインターネット (IoT) デバイスや運用技術 (OT) 制御デバイスを標的にしています。最後の章では、サイバー レジリエンスにおける今年の動向を見直しながら、マイクロソフトとお客様向けを標的とする攻撃から守るための過去 1 年間に得られたインサイトと教訓について説明します。

各章では、マイクロソフト独自の視点に基づいて得られた重要な教訓とインサイトを示します。マイクロソフトが世界にまたがる製品およびサービスのエコシステムから分析した何兆ものシグナルにより、世界中のデジタル脅威の凶暴性、範囲、規模が明らかになります。マイクロソフトでは、そのような脅威に対してお客様とデジタル エコシステムを保護するための対策を講じています。数十億ものフィッシング攻撃、ID 盗難、お客様に対する他の脅威を特定し、ブロックするのに役立つマイクロソフトのテクノロジについてお読みください。

Tom Burt によるイントロダクション
続き

マイクロソフトではさらに、法的および技術的な手段を使って、サイバー犯罪者や国家レベルのアクターによって使用されているインフラを押収およびシャットダウンし、国民レベルのアクターによって脅迫または攻撃されたときはお客様に通知しています。また、AI/ML テクノロジを使ってサイバー攻撃を特定してブロックし、セキュリティ担当者がサイバー侵入をよりすばやく効果的に防御して特定できるようにする、ますます効果的な機能とサービスの開発に取り組んでいます。

おそらく最も重要な点として、マイクロソフトは、MDDR を通じて、個人、組織、企業がこのような増え続けるデジタル脅威から防御するために実行できるステップについて最善のアドバイスを提供しています。優れたサイバー管理対策を採用することは最大の防御であり、サイバー攻撃のリスクを大幅に軽減できます。

サイバー犯罪の現状

サイバー犯罪者は、高度な営利企業として行動を続けています。攻撃者は、自身の技術を適応させて、実装するための新しい方法を見つけ出しているため、キャンペーン運用インフラをホストする方法や場所の複雑さが増しています。同時に、サイバー犯罪者はより質素にもなっています。攻撃者は、オーバーヘッドを減らして見た目の合法性を高めるため、フィッシング キャンペーンやマルウェアをホストしたり、さらには仮想通貨のマイニング目的でコンピューティング能力を使用したりするために、ビジネス ネットワークとデバイスを危険にさらしています。

詳しくは 6 ページをご覧ください

「ウクライナのハイブリッド戦争における サイバー兵器展開の到来は、新しい対立の時代の幕開けです。」

国家レベルの脅威

国家レベルのアクターは、検出を回避し、戦略的な優先事項に促進することを目的として、ますます高度なサイバー攻撃を始めています。ウクライナのハイブリッド戦争におけるサイバー兵器展開の到来は、新しい対立の時代の幕開けです。さらに、ロシアはプロパガンダを使用してロシア、ウクライナ、そして世界中の人々の意見に影響を与えることにより、情報の影響力を戦争に活かしていきました。ウクライナ以外では、国家レベルのアクターが活動範囲を拡大し、自動化、クラウド インフラ、リモート アクセス テクノロジの進歩を利用して、より広範な標的を攻撃し始めています。最終的な標的へのアクセスを可能にする企業の IT サプライ チェーンには、攻撃が頻繁に行われました。攻撃者は修正プログラムが適用されていない脆弱性をすばやく悪用して、高度な手法とブルートフォース手法の両方を使って資格情報を盗み、オープンソースや合法的なソフトウェアを使って活動をあいまいにしたため、サイバーセキュリティ管理手順がさらに重要になりました。加えて、イランは、定番の攻撃方法であるランサムウェアなどの破壊的なサイバー兵器を使用する点でロシアに加わっています。

このような動向が見られるため、人権を優先して、オンラインでの向こう見ずな行動から人々を保護する一貫したグローバル フレームワークを早急に採用する必要があります。すべての国が協力して、責任ある国家の行動に関する規範とルールを実装する必要があります。

詳しくは 30 ページをご覧ください

デバイスとインフラ

パンデミックに加えて、デジタル トランスフォーメーションを加速させた 1 つの要素としてあらゆる種類のインターネット接続デバイスが急速に導入されたため、デジタル世界の攻撃対象領域が大幅に増加しました。そのため、サイバー犯罪者と国家はすかさずそれを巧みに利用しています。近年、IT ハードウェアとソフトウェアのセキュリティは高まっていますが、IoT のセキュリティと OT デバイスのセキュリティは歩調が合っていません。脅威アクターは、それらのデバイスを悪用することにより、ネットワークへのアクセスを確立して侵入を拡大し、サプライ チェーン内での足場を確立したり、標的組織の OT 運用を中断したりしています。

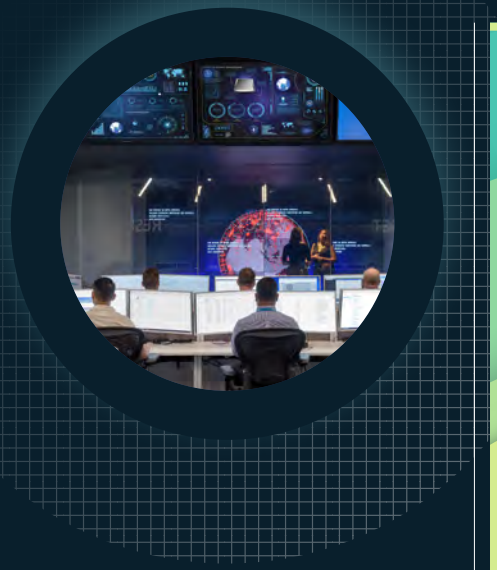
詳しくは 56 ページをご覧ください

Tom Burt によるイントロダクション
続き

サイバー影響工作

国家は、プロパガンダを広めて国内外の世論に影響を与えるため、高度な影響工作をますます利用するようになっています。このような活動は、信頼の低下、対立の激化、民主的プロセスへの脅威につながります。熟練した高度で継続的なマニピュレーター (Advanced Persistent Manipulator) アクターは、インターネットやソーシャル メディアと共に従来のメディアを利用して、活動の範囲、規模、効率を大幅に強化し、グローバル情報エコシステムにきわめて大きな影響を及ぼしています。過去 1 年間、ロシアによるウクライナでのハイブリッド戦争の一環としてそのような工作が利用されてきましたが、ロシアに加えて中国やイランなどの他の国々は、さまざまな問題に対するグローバルな影響力を広げるため、ソーシャル メディアを利用したプロパガンダ工作も次第に広げてきました。

詳しくは 71 ページをご覧ください



サイバー レジリエンス

セキュリティは、テクノロジが成功を収める上で重要な要素となります。イノベーションと生産性向上を実現するには、最新の攻撃からの回復力をできる限り高めるセキュリティ対策を導入することが必要です。パンデミックは、社員がどこで仕事をしていても保護できるよう、マイクロソフトがセキュリティ　プラクティスとテクノロジを転換させる点で挑戦となりました。この 1 年間、脅威アクターは、パンデミック時に露呈した脆弱性と、ハイブリッド作業環境への移行を利用し続けてきました。それ以降、さまざまな攻撃方法の蔓延や複雑さと国家活動の増加に対応することがマイクロソフトの主な課題となってきました。この章では、マイクロソフトが直面してきた課題と、15,000　を超えるパートナーのために実施された防御策について詳しく説明します。

詳しくは 86 ページをご覧ください

マイクロソフトのユニークなアドバンテージ

43 兆
高度なデータ分析と AI アルゴリズムを使ってデジタルの脅威やサイバー犯罪について理解し、保護するために、1 日あたりに合成されたシグナルの数。

8,500 以上
77 か国にまたがるエンジニア、研究者、データ サイエンティスト、サイバーセキュリティの専門家、脅威ハンター、地政学アナリスト、調査担当者、ファースト レスポンダーの人数。

15,000 以上
お客様のサイバー レジリエンスを高めるマイクロソフトのセキュリティ エコシステムのパートナーの数。

370 億
ブロックされたメールの数

347 億
ブロックされた ID の脅威

25 億
毎日分析する脅威シグナルの件数

2021 年 7 月 1 日～ 2022 年 6 月 30 日

Tom Burt によるイントロダクション
続き

マイクロソフトは、民間企業、政府、市民社会における他者との緊密なパートナーシップを通じ、独立した立場として、社会的な基盤を支えるデジタル システムを保護し、あらゆる場所のあらゆる人に安全かつセキュアなコンピューティング環境を促進する責任があると考えています。この責任は、2020 年以降毎年 MDDR を発表してきた理由となっています。このレポートは、マイクロソフトの膨大なデータと包括的な調査を最大限に活かしたものです。デジタルの脅威を取り巻く状況がどのように進化しているかについての独自のインサイトと、エコシステムのセキュリティを高める今すぐ実行できる重要なアクションが紹介されています。

マイクロソフトは、このドキュメントに加えて、1 年を通じてマイクロソフトから発行されるサイバーセキュリティに関する多数の文書に示されるデータとインサイトに基づいて、読者の皆さまが直ちに行動を起こすことができるように、緊急性が浸透することを期待しています。デジタル環境に対する脅威の重大さと、それが物理的な世界に与える影響を考慮に入れると、デジタルの脅威から自分自身、所属組織、企業を保護する対策を講じるために必要なものが十分に揃っていることを覚えておくのは重要です。

今年のマイクロソフト デジタル防衛レポートをご覧いただき、ありがとうございます。デジタル エコシステムを総合的に防御するのに役立つ、貴重なインサイトと推奨事項が皆さまのお役に立てば幸いです。

カスタマー セキュリティ & トラスト
担当コーポレート バイス プレジデント
Tom Burt

このレポートの目的は次の 2 つです。

① 広範なエコシステムにまたがるお客様、パートナー、利害関係者の進化し続けるデジタル脅威の状況を明らかにするため、新たなサイバー攻撃と従来の持続的脅威の進化し続ける傾向の両方に光を当てる。

② お客様とパートナーが、サイバー レジリエンスを強化し、それらの脅威に対応できるようにする。

サイバー犯罪の現状

サイバー防衛が強化され、より多くの組織が予防のためプロアクティブなアプローチを取っているため、攻撃者は自身の技術を適応させています。

サイバー犯罪の **状況の概要**

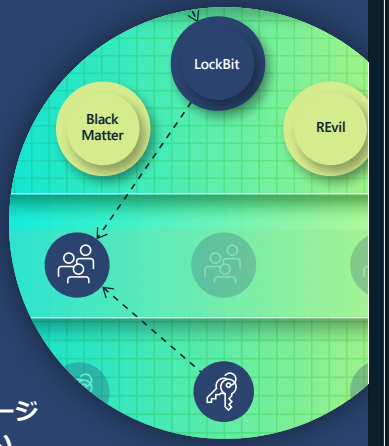
サイバー防衛が強化され、より多くの組織が予防のためプロアクティブなアプローチを取っているため、攻撃者は自身の技術を適応させています。

サイバー犯罪者は、高度な営利企業として行動を続けています。攻撃者は、自身の技術を適応させて、実装するための新しい方法を見つけ出しているため、キャンペーン運用インフラをホストする方法や場所の複雑さが増しています。同時に、サイバー犯罪者はより質素にもなっています。攻撃者は、オーバーヘッドを減らして見た目の合法性を高めるため、フィッシング キャンペーンやマルウェアをホストしたり、さらには仮想通貨のマイニング目的でコンピューティング能力を使用したりするために、ビジネス ネットワークとデバイスを危険にさらしています。

サイバー犯罪経済の産業化により、ツールやインフラにアクセスしやすくなって参入スキルの障壁が下がるにつれて、サイバー犯罪は増え続けています。

詳しくは 18 ページをご覧ください

ランサムウェアと恐喝の脅威は、政府、企業、重要インフラを標的とする攻撃を行うことでますます大胆になっています。

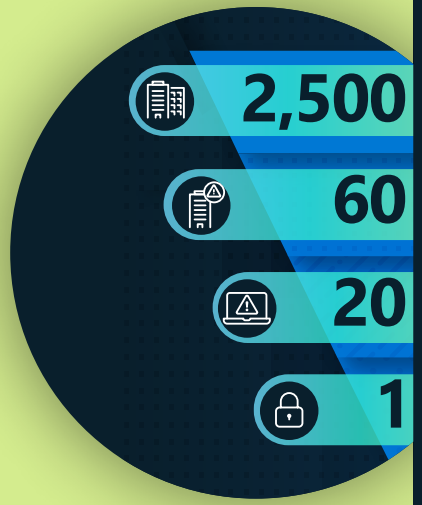


詳しくは 9 ページをご覧ください

攻撃者は、身代金を支払うよう仕向けるため、機密データをさらすと脅すことが多くなっています。

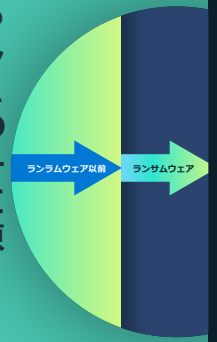
詳しくは 10 ページをご覧ください

人間によって操作されるランサムウェアを使用する犯罪者は、標的の 3 分の 1 の侵害に成功し、そのうち 5% は身代金が支払われるため、それらのランサムウェアは広く浸透しています。



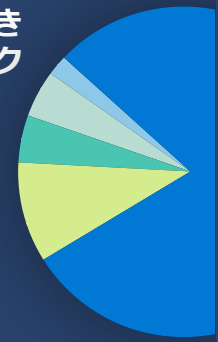
詳しくは 9 ページをご覧ください

ランサムウェアに対する最も効果的な防御として、多要素認証、セキュリティ修正プログラムの頻繁な適用、ネットワーク アーキテクチャ全体におけるゼロ トラストの原則などがあります。



詳しくは 13 ページをご覧ください

すべての受信トレイを無差別に標的とする資格情報フィッシング スキームが増加しており、請求詐欺などのビジネス メール詐欺が企業にとって大きなサイバー犯罪のリスクとなっています。



詳しくは 21 ページをご覧ください

サイバー犯罪者と国家アクターが持つ悪質なインフラを破壊するため、マイクロソフトは革新的な法的アプローチと官民のパートナーシップを利用しています。

詳しくは 25 ページをご覧ください

イントロダクション

サイバー犯罪は、ランダムな攻撃と標的型攻撃の両方が増え続けています。

サイバー防御が強化され、より多くの政府や企業が予防のためにプロアクティブなアプローチを講じるにつれて、攻撃者はサイバー犯罪を実行に移すのに必要なアクセス権を獲得するため、2 つの戦略を利用するようになっています。1 つ目のアプローチは、標的が広範で、ボリュームに依存しているキャンペーンです。もう 1 つは、監視とより的を絞った標的を利用して成功率を上げるアプローチです。収益を上げることが目的ではない場合でも (地政学的な目的を持つ国家の活動など)、ランダムな攻撃と標的型攻撃の両方が利用されます。この 1 年間、サイバー犯罪者は、キャンペーンの成功率を最大限に高めるため、ソーシャル エンジニアリングと時事問題の悪用を利用してきました。たとえば、新型コロナウィルスをテーマにしたフィッシング ルアーが利用される頻度は下がりましたが、ウクライナ国民を支援するための募金を利用することが増えました。

攻撃者は、自身の技術を適応させて、実装するための新しい方法を見つけ出しているため、キャンペーン運用インフラをホストする方法や場所の複雑さが増しています。マイクロソフトでは、サイバー犯罪者がより節約志向になっており、テクノロジにお金を使わなくなっている傾向を観察しています。攻撃者によっては、オーバーヘッドを減らして見た目の合法性を高めるため、フィッシング キャンペーンやマルウェアをホストしたり、さらには仮想通貨のマイニング目的でコンピューティング能力を使用したりするために、企業を侵害しようとする傾向が強くなっています。

この章では、ハクティビズム (社会的または政治的な目的を推し進めるため、民間人がサイバー攻撃を行って引き起こす混乱) の台頭についても考えます。エキスパートも初心者も含む何千何万人もの人々が、2022 年 2 月以降、Web サイトの無効化や、ロシア・ウクライナ戦争の一環として盗まれたデータの漏えいなどの攻撃を仕掛けてきました。戦争の終了後もこの傾向が続くかどうかを予測するにはまだ早すぎるでしょう。

組織は、サイバー攻撃から防御するため、アクセス制御を定期的に見直して強化し、セキュリティ戦略を導入する必要があります。しかし、他にもできることがあります。マイクロソフトのデジタル犯罪対策ユニット (DCU) が民事訴訟を利用し、サイバー犯罪者や国家アクターが使用している悪質なインフラを差し押さえてきた方法について説明します。官民のパートナーシップを通じて、この脅威に対して共に戦わなければなりません。過去 10 年間に得られた教訓を共有することにより、高まり続けるサイバー犯罪の脅威から自分自身と広範なエコシステムを保護するために実行できるプロアクティブな対策について理解し、検討できるようにしたいと考えています。

Amy Hogan-Burney
デジタル犯罪対策ユニット、
ゼネラル マネージャー

ランサムウェアと恐喝：国家レベルの脅威

増え続けるサイバー犯罪エコシステムを利用する犯罪者が重要なインフラ、あらゆる規模の企業、政府や地方自治体を標的としているため、あらゆる個人にとってランサムウェア攻撃の危険性が高まっています。

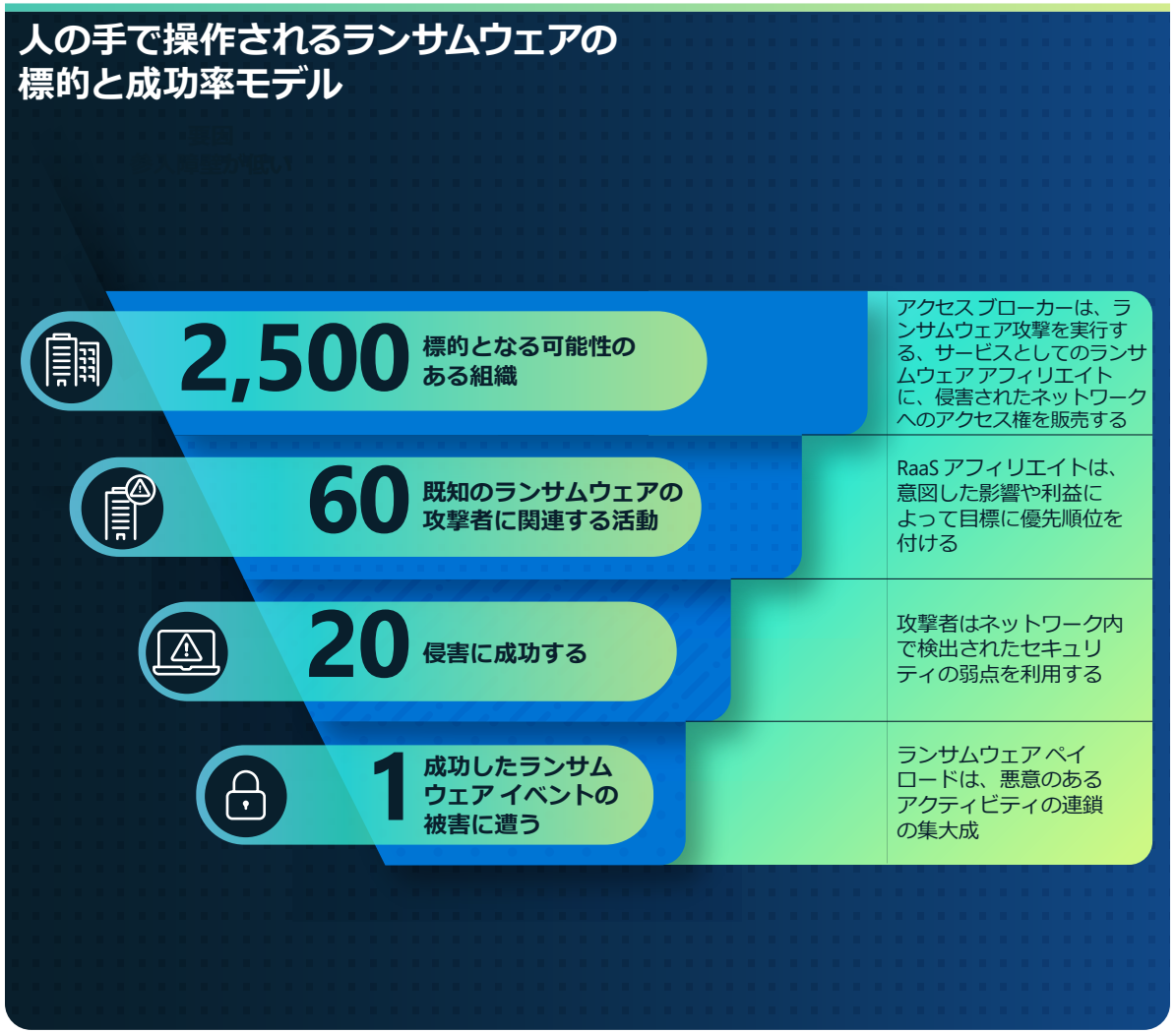
過去 2 年間にわたり、人目を引くランサムウェア インシデント (重要なインフラ、医療、IT サービス プロバイダーを巻き込んだインシデントなど) が人々の注目を集めてきました。ランサムウェア攻撃は範囲がより大胆になっているため、その影響もますます広がっています。2022 年既に見られている攻撃の例を以下に示します。

- 2 月、2 つの企業に対して行われた攻撃が、ドイツ北部にある数百ものガソリンスタンドの決済処理システムに影響を与えました。[1]
- 3 月 、ギリシャの郵便サービスに対する攻撃が、郵便配達を一時的に中断させ、金融取引の処理に影響を与えました。[2]
- 5 月下旬、コスタリカの行政機関に対するランサムウェア攻撃により、病院の運営が停止して、税関と徴税が中断した後、国家緊急事態が宣言されました。[3]
- さらに、5 月には、攻撃によりインド最大の航空会社の 1 つでフライトの遅延と欠航が発生し、数百人の乗客が足止めされました。[4]

このような攻撃が成功して現実世界に広範囲な影響を及ぼしたのは、サイバー犯罪経済が産業化した結果、ツールとインフラへのアクセスが可能になり、スキルの障壁が下がってサイバー犯罪の能力が高まったためです。

近年、ランサムウェアは、1 つの「ギャング」が、ランサムウェア ペイロードの開発と配布の両方を行うモデルからサービスとしてのランサムウェア (RaaS) に移行しました。RaaS により、1 つのグループがランサムウェア ペイロードの開発を管理し、データ漏えいを通じた支払いと恐喝のためのサービスを他のサイバー犯罪者 (実際にランサムウェア攻撃を仕掛けるサイバー犯罪者) に提供することが可能になりました。これは、利益が減少するため「アフィリエイト」と呼ばれています。サイバー犯罪経済のフランチャイズによって、攻撃者プールが拡大しました。サイバー犯罪ツールの産業化により、攻撃者は侵入を実行に移して、データを引き出し、ランサムウェアを展開することが簡単になりました。

人の手で操作されるランサムウェア[5] (標的のネットワークで発見された内容に基づいて攻撃のあらゆる段階で意思決定を行う人間が引き起こす脅威を表し、コモディティ ランサムウェア攻撃による脅威を描写するためにマイクロソフトの研究者によって作られた用語) は、組織にとって引き続き大きな脅威です。



Microsoft Defender for Endpoint (EDR) のデータに基づくモデル (2022 年 1 月 ～ 6 月)。

ランサムウェアと恐喝：国家レベルの脅威

(続き)

標準的な手法として二重恐喝収益化戦略が採用されるようになったため、ランサムウェア攻撃の影響力は高まっています。侵害されたデバイスからデータを引き出して、デバイス上のデータを暗号化した後、盗んだデータをさらしたり脅迫したりすることにより、被害者に身代金を支払わせるという手順で行われます。

ほとんどのランサムウェア攻撃者は、アクセス権を取得したネットワークにランサムウェアを日和見的に展開しますが、アクセス ブローカーとランサムウェア オペレーターのつながりを利用して他のサイバー犯罪者からアクセス権を購入している攻撃者もいます。

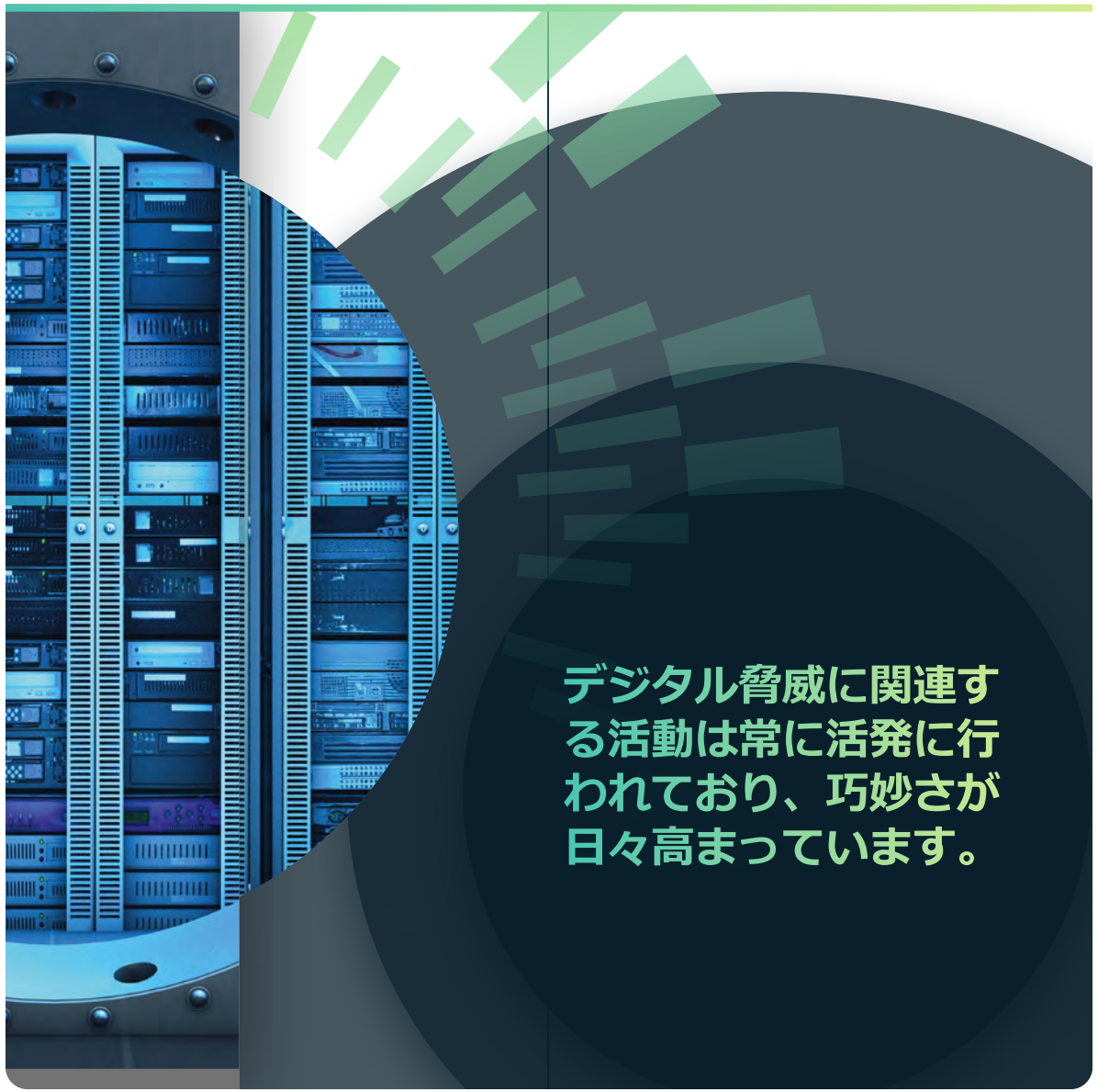
マイクロソフト独自の広範なシグナル インテリジェンスは、ID、メール、エンドポイント、クラウドなど、複数のソースから集められており、拡大し続けるランサムウェア経済に関するインサイトに加えて、技術面での能力があまり高くない攻撃者用に設計されたツールを含むアフィリエイト システムを提供します。

専門的なサイバー犯罪者との関係を広げることにより、ランサムウェア攻撃のペース、巧妙さ、成功率が高まっています。その結果、サイバー犯罪エコシステムの進化が促され、標的、支払いサービス、復号化または発行ツールやサイトへの初期アクセスにおいて、手法、目標、スキルセットの異なるコネクテッド プレーヤーと互いに支え合うことができるようになっています。

ランサムウェア オペレーターは、獲得したアクセス権を収益化することだけを主な目的とするブローカーから、組織や政府のネットワークへのアクセス権をオンラインで購入したり、資格情報とアクセス権を取得したりできるようになりました。

その後、購入したアクセス権を使って、ダーク ウェブ マーケットプレースやフォーラムを介して購入したランサムウェアを展開します。多くの場合、被害者との交渉は、オペレーター自身ではなく RaaS チームによって行われます。このような犯罪取引はシームレスであり、ダーク ウェブの匿名性と国家間で取り締まることの難しさのため、加わった人たちが逮捕されるリスクはほとんどありません。

この脅威に対する取り組みを持続可能なものとして成功させるには、政府全体の戦略を民間企業と緊密に連携して実行に移す必要があります。



ランサムウェア経済について理解する

ランサムウェアがメディアで描写される場合とは異なり、単一のランサムウェアの変種が 1 つのエンド ツー エンドの「ランサムウェア ギャング」によって管理されることはあまりありません。むしろ、マルウェアの構築、被害者に対するアクセス権の取得、ランサムウェアの展開、恐喝交渉の実行は、別個のエンティティが行います。犯罪エコシステムの産業化により、次のような役割が生まれました。

- アクセス権を奪い取って引き渡すアクセス ブローカー (サービスとしてのアクセス)
- ツールを販売するマルウェア開発者
- 侵入を実行に移す犯罪オペレーターとアフィリエイト
- アフィリエイトから収益化を引き継ぐ暗号化および恐喝サービス プロバイダー (RaaS)。

人の手で操作されるランサムウェアのキャンペーンはすべて、セキュリティの弱点に依存するという共通点があります。具体的に挙げると、攻撃者は通常、組織の貧弱なサイバー衛生を利用します。よくあるのは、修正プログラムを頻繁に適用していない場合や、多要素認証 (MFA) を実装していない場合などです。

ケース スタディ : Conti の解体

過去 2 年間で最も多く見られたランサムウェアの 1 つである Conti は、2022 年半ばに運用を停止し始めました。Microsoft Threat Intelligence Center (MSTIC) では 3 月下旬から 4 月上旬まで活動の大幅な減少を観察していました。Conti ランサムウェアの展開が最後に観察されたのは、4 月中旬です。しかし、他のランサムウェア運用の閉鎖と同様、Conti の解体はランサムウェア展開にあまり大きな影響を及ぼしませんでした。MSTIC では、Conti アフィリエイトが BlackBasta、Lockbit 2.0、LockbitBlack、HIVE など、他のランサムウェア ペイロードの展開に切り替えたのを観察したからです。これは過去数年間のデータと一致しており、ランサムウェア ギャングがオフラインになると、数か月後に再出現したり、技術的な能力やリソースを新しいグループに再分配したりすることが示唆されています。

マイクロソフトの脅威インテリジェンス チームは、ランサムウェアの脅威アクターを、利用されているマルウェアによって追跡するのではなく、特定のツールに基づいて個々のグループ (DEV としてラベル付け) として追跡しています。これは、Conti のアフィリエイトが解体されたとき、他のツールや RaaS キットを使ってそれらの DEV を追跡できたことを意味していました。次に例を示します。

- Trickbot とのアフィリエイト関係にある DEV-0230 は、Conti の有能なユーザーでした。4 月下旬、MSTIC は QuantumLocker を使ってこれを観察しました。
- DEV-0237 は、コスタリカの行政機関に対する 5 月 31 日の攻撃で HIVE を使うなど、Conti のランサムウェア キットから HIVE と Nokoyawa に移行しました。
- Conti ランサムウェア キットのもう 1 つの有効なユーザーである DEV-0506 は、BlackBasta を使っていることが観察されました。

RaaS プログラム間ですばやく移行しているアフィリエイト (DEV-0237) の例

Conti のような RaaS プログラムが停止すると、ランサムウェアのアフィリエイトはほぼ瞬時に別のもの (Hive) に移行します。

RaaS により、ランサムウェア エコシステムが進化し、特定が妨げられている

人の手で操作されるランサムウェアは個々のオペレーターによって実行されるため、攻撃パターンは標的に応じて変化し、攻撃の期間を通じて入れ替わります。これまで、1 つのランサムウェア型の各キャンペーンにおいて、初期エントリ ベクター、ツール、ランサムウェア ペイロードの選択肢に密接な関係があることがわかっています。これにより、特定が容易になりました。しかし、RaaS アフィリエイト モデルではこの関係が壊れています。そのため、マイクロソフトはランサムウェア ペイロード開発者をオペレーターとして追跡するのではなく、特定の攻撃でペイロードを展開するランサムウェアのアフィリエイトを追跡しています。

もう 1 つの方法として、HIVE 開発者が HIVE ランサムウェア攻撃の背後にあるオペレーターであると想定することをやめました。ほとんどの場合はアフィリエイトだからです。

サイバーセキュリティ業界は、開発者とオペレーターの間におけるこの図式を十分に把握することに苦労しています。業界は依然としてペイロード名ごとにランサムウェア インシデントを報告することが多いため、単一のエンティティ (つまり、ランサムウェア ギャング) がその特定のランサムウェア ペイロードを使用しているあらゆる攻撃の背後におり、それに関連するすべてのインシデントが同じ手法とインフラを共有しているという誤解を与えています。ネットワークの防御者を支えるには、データ流出や追加の永続化メカニズムなど、アフィリエイトのさまざまな攻撃に先立って現れるステージと、考えられる検出と保護のチャンスについて詳しく理解することが重要です。

攻撃者は、マルウェアよりも、運用を成功させるために資格情報を必要としています。人の手で操作されるランサムウェアを組織全体に感染させるには、高い特権を持つアカウントへのアクセス権を取得することが必要です。

脚光を浴びる人の手で操作されるランサムウェア攻撃

過去 1 年間、マイクロソフトのランサムウェアの専門家が、100 件以上の人の手で操作されるランサムウェアのインシデントについて詳細な調査を実施して攻撃者の手法を追跡し、お客様の保護を強化する方法を解明しました。

ここで説明する分析は、オンボーディング済みのマネージド デバイスにのみ当てはまる点に注意してください。オンボーディングされていない管理対象外のデバイスは、組織のハードウェア資産の中でセキュリティが最も低い部分を占めています。

最も広く利用されているランサムウェア フェーズ手法 :

75%
管理ツールを使う人の割合。

75%
高い特権を持つユーザー アカウントを乗っ取って使用し、SMB プロトコル経由で悪質なペイロードを拡散する人の割合。

99%
OS に組み込まれたツールを使って、検出されたセキュリティおよびバックアップ製品の改ざんを試みる人の割合。

典型的な人の手で操作される攻撃

人の手で操作されるランサムウェア攻撃は、ランサムウェア前のフェーズとランサムウェア展開のフェーズに分類できます。ランサムウェア前のフェーズでは、攻撃者は組織のトポロジとセキュリティ インフラを調べることによってネットワークに潜入する準備を行います。

ランサムウェアの展開フェーズに到達する前に攻撃者を阻止する	展開!
ランラムウェア以前	ランサムウェア
このフェーズは、数日間から数週間または数か月に及ぶことがありますが、過去 2 年の間に短縮しました。	このフェーズはわずか数分で終了する
攻撃者は、トポロジとセキュリティ インフラについて可能な限り学習することにより、ネットワークに潜入する準備を整えます。攻撃者は、このフェーズでデータを引き出すこともできます。	攻撃者は可能な限り多くのデータを暗号化することを目指す

マイクロソフトの調査によると、人の手で操作されるランサムウェア攻撃の背後にいるアクターのほとんどは、似たようなセキュリティ弱点を利用し、共通の攻撃パターンと手法を使っています。

耐久性の高いセキュリティ戦略

このような性質を持つ攻撃に対抗して防ぐには、組織のマインドセットを変える必要があります。攻撃者に時間をかけさせ、ランサムウェア前のフェーズからランサムウェア展開のフェーズに移行できないようにするための包括的な保護に焦点を当てる必要があります。

企業は、攻撃のレベルを下げることを目標とし、セキュリティのベスト プラクティスを一貫性のある方法で積極的にネットワークに適用する必要があります。人の手で意思決定を行うと、それらのランサムウェア攻撃により、一見異なるように見える複数のセキュリティ製品アラートが生成される可能性があるため、方法がわからなくなったり、時間内に対応できなかったりすることがあります。アラートは間違いなく負担となるため、セキュリティ オペレーション センター (SOC) は、アラートの傾向を見つけたり、アラートをインシデントにグループ化して全体像を把握できるようにすることで、負担を軽減できます。そうすれば、SOC は攻撃対象領域縮小ルールなどの強化機能を使ってアラートを減らすことができます。よくある脅威に対して強化措置を施すことにより、アラートの量が減るだけでなく、多くの攻撃者をネットワークへのアクセス前に阻止することもできます。

組織は、人の手で操作されるランサムウェア攻撃から保護するため、継続的に高いレベルを保つセキュリティ対策とネットワーク衛生を維持する必要があります。

実用的なインサイト

単純に利益を上げることがランサムウェア攻撃者の動機なので、セキュリティの強化によって攻撃のコストを高めることが、サイバー犯罪の経済を混乱させる上で重要です。

1. 資格情報の検疫を構築する。攻撃者は、マルウェアよりも、運用を成功させるために資格情報を必要としています。人の手で操作されるランサムウェアが組織全体に感染するには、ドメイン管理者などの高い特権を持つアカウントへのアクセス権を取得したり、グループ ポリシーを編集したりできる必要があります。
2. 資格情報の暴露を監査する。
3. Active Directory 更新プログラムの展開を優先させる。
4. クラウドの強化を優先させる。
5. 攻撃対象領域を減らす。
6. インターネットに接続された資産を強化し、境界を把握する。
7. ネットワークの強化により、優先度の高いインシデントに合わせてボリュームを削減し、帯域幅を維持することで、SOC アラートの負担を軽減する。

詳しい情報のリンク

- RaaS: サイバー犯罪のギグ エコノミーを理解して自己防衛する方法 | マイクロソフト セキュリティ ブログ
- 人の手で操作されるランサムウェア攻撃 : 最悪の事態は回避できる | マイクロソフト セキュリティ ブログ

現場担当者によるランサムウェアのインサイト

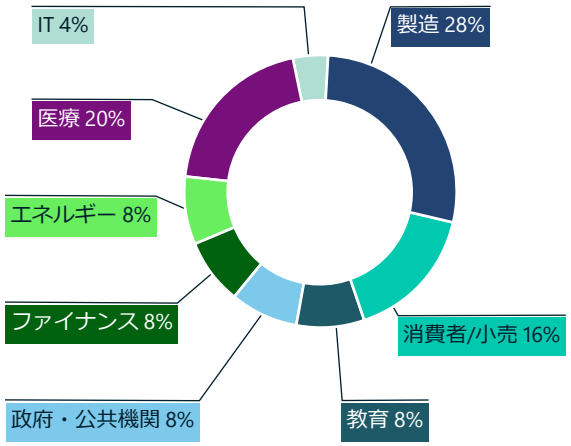
2019 年以降、人の手で操作されるランサムウェア攻撃は世界中の組織で着実に増加しています。しかし、昨年の法執行機関による活動と地政学的な事象はサイバー犯罪組織に大きな影響を及ぼしました。

マイクロソフトのセキュリティ サービス ラインは、調査から封じ込めおよび復旧活動まで、サイバー攻撃全体を通じてお客様をサポートします。対応および復旧サービスは、緊密に統合された 2 つのチーム (復旧のための調査と基盤づくりに重点を置くチームと、封じ込めおよび復旧に重点を置くチーム) によって提供されます。このセクションでは、過去 1 年間におけるランサムウェア エンゲージメントに基づく調査結果の概要を示します。

93%

ランサムウェア復旧エンゲージメント中、不十分な特権アクセスと侵入拡大の制御が明らかになったマイクロソフト調査の割合。

業界別のランサムウェア インシデントおよび復旧エンゲージメント

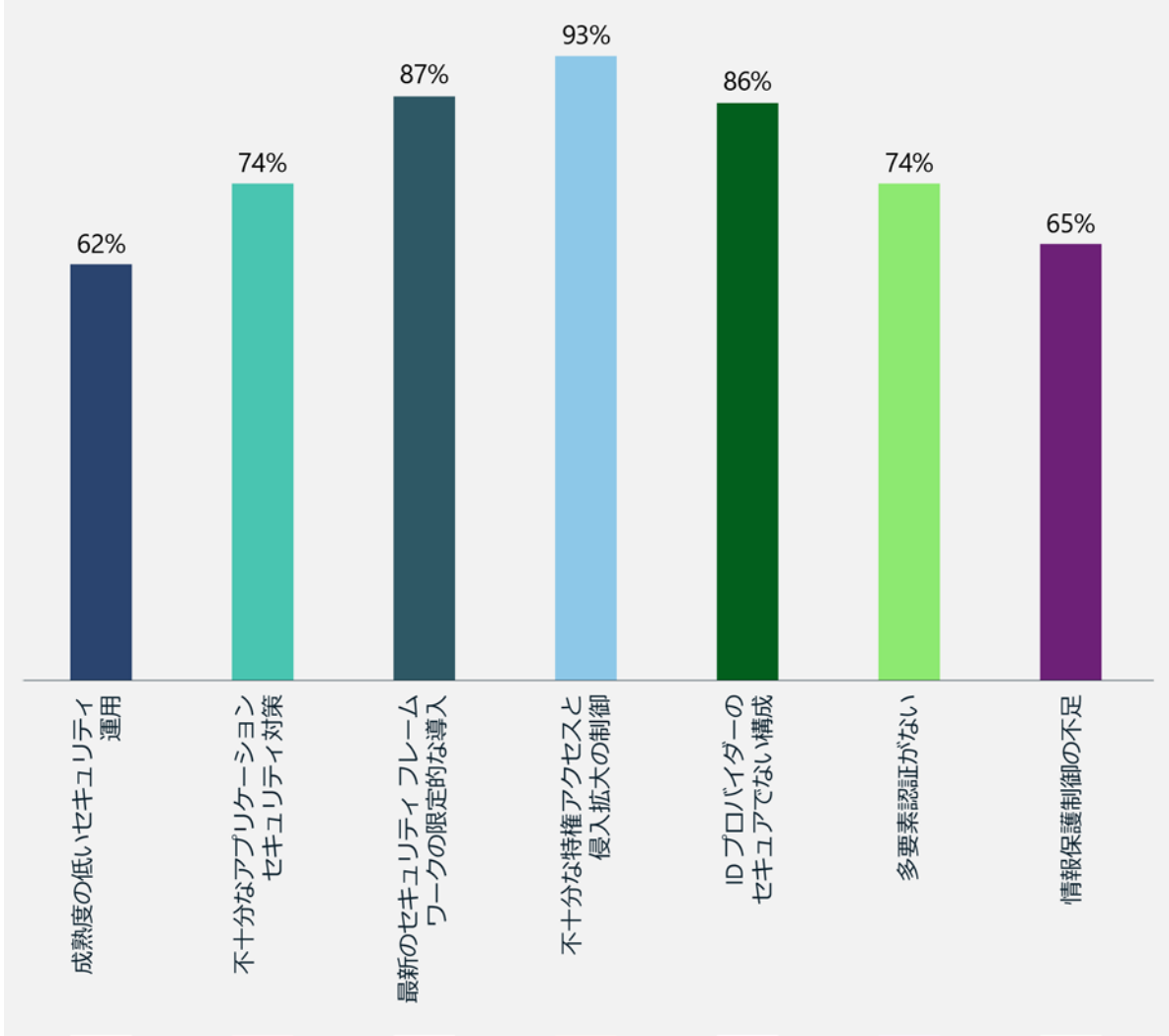


小規模な新しいグループや脅威が出現すると、防御側のチームは、それまで未知であったランサムウェア マルウェア ファミリーから保護すると同時に、進化し続けるランサムウェアの脅威について認識する必要があります。犯罪グループが利用しているすばやい開発アプローチにより、使いやすいキットにパッケージ化されたインテリジェント ランサムウェアの作成が可能になっています。これにより、より多くの標的に広範囲な攻撃を実行する点での柔軟性が高まっています。

次のページでは、ランサムウェアに対する保護が弱い組織で最もよく観察される要因について詳しく説明し、調査結果を次の 3 つのカテゴリに分類します。

1. 弱い ID 管理
2. 効果的ではないセキュリティ運用
3. 限られたデータ保護

ランサムウェア対応エンゲージメントにおいて最もよくある調査結果のまとめ



ランサムウェア インシデント対応エンゲージメントで最もよくある調査結果として、不十分な特権アクセスと侵入拡大の制御がありました。

現場担当者によるランサムウェアのインサイト

（続き）

オンサイトでの対応エンゲージメントで見られる 3 つの主な要因：

① **弱い ID 管理**：資格情報の盗難攻撃は、依然として上位の要因の 1 つである

② **効果的ではないセキュリティ運用**プロセスは、攻撃者にとってチャンスとなるだけでなく、復旧にかかる時間にも大きな影響を及ぼす

③ 最終的にはデータに影響が及ぶ一組織はビジネス ニーズに沿った効果的な**データ保護戦略**を実装するのに苦労している

① 弱い ID 管理

人の手で操作されるランサムウェアは進化を続けており、従来は標的型攻撃に関連していた資格情報の盗難と侵入拡大の方法を採用しています。攻撃に成功すると、多くの場合、Active Directory (AD) などの ID システムの侵害を伴うキャンペーンが長期間実行され、人間のオペレーターが資格情報を盗み出したり、システムにアクセスしたり、ネットワークで永続的な状態を維持したりできるようになります。

Active Directory (AD) と Azure AD のセキュリティ

88%

影響を受けたお客様のうち、AD と Azure AD のセキュリティ ベスト プラクティスを採用していなかった割合。これは、攻撃者が重要な ID システムにおける誤構成や弱いセキュリティ対策を悪用し、広範なアクセス権を取得してビジネスに影響を与える際によく見られる攻撃ベクトルとなってきました。

最小特権アクセスと特権アクセスワークステーション (PAW) の使用

影響を受けた組織のうち、独自システムやビジネス クリティカルなアプリケーションなどの重要な ID と価値の高い資産を管理する際、専用ワークステーションを介して管理資格情報の分離と最小限特権アクセスの原則を適切に実装している組織はありませんでした。

特権アカウントのセキュリティ

88%

機密性の高い特権アカウント用に MFA が実装されていないため、攻撃者が資格情報を侵害し、正当な資格情報を使ってさらに攻撃を行うことができるセキュリティ ギャップが残っていたエンゲージメントの割合。

84%

84% の組織の管理者は、侵害された特権資格情報の悪用を防ぐため、ジャストインタイム アクセスなどの特権 ID 制御を使用していませんでした。

現場担当者によるランサムウェアのインサイト

（続き）

② 効果的ではないセキュリティ運用

マイクロソフトのデータは、ランサムウェア攻撃を受けた組織のセキュリティ運用、ツール、情報テクノロジ資産ライフサイクル管理に大きなギャップがあることを示しています。入手可能なデータによると、以下のギャップが最も多く観察されました。

修正プログラムの適用：

68%

影響を受けた組織のうち、効果的な脆弱性および修正プログラム管理プロセスがなく、修正プログラムの自動適用よりも手動プロセスに対する依存度が高いため、重大なセキュリティ ホールが生まれていた組織の割合。製造業と重要インフラは、レガシーの業務テクノロジ (OT) システムのメンテナンスと修正プログラム適用に苦労し続けています。

セキュリティ運用ツールの不足：

ほとんどの組織は、セキュリティ ツールの不足や構成ミスによりセキュリティをエンド ツー エンドで把握できなかったため、検出と対応の有効性が低下したと報告しました。

60%

基本的な検出および対応テクノロジである EDR[6] ツールを使用していないと報告した組織の割合。

60%

セキュリティ情報およびイベント管理 (SIEM) テクノロジに投資していなかったため、サイロを監視する必要があり、エンド ツー エンドの脅威と非効率的なセキュリティ運用を検出するのが難しかった組織の割合。自動化は、SOC のツールおよびプロセスにおいて引き続き主なギャップとなっているため、SOC スタッフはセキュリティ テレメトリの把握に数え切れないほどの時間を費やしています。

84%

影響を受けた組織のうち、複数のクラウド環境をセキュリティ運用ツールに統合していなかった組織の割合。

対応および復旧プロセス：

76%

影響を受けた組織の 76% で観察された重要な分野として、効果的な対応計画がないため、組織として危機への備えが十分にできておらず、対応と復旧にかかる時間にマイナスの影響を与えていました。

③ 限られたデータ保護

侵害された多くの組織では、適切なデータ保護プロセスがないため、復旧にかかる時間と通常業務に戻る能力に大きな影響が及びました。観察された最もよくあるギャップは次のとおりです。

不変バックアップ：

44%

影響を受けたシステムの不変バックアップを持っていなかった組織の割合。データは、管理者が AD などの重要な資産のバックアップおよび復旧計画を持っていなかったことも示しています。

データ損失防止：

攻撃者は通常、組織の脆弱性を悪用してシステムを侵害する方法を見つけ出し、脅迫、知的財産の盗難、または収益化を目的として重要なデータを盗み出します。

92%

影響を受けた組織のうち、リスクを軽減する効果的なデータ損失防止制御を実装していなかったため、重要なデータを損失した組織の割合。

ランサムウェアが減少した地域と増加した地域がある

今年、北米とヨーロッパの対応チームに報告されたランサムウェアの事例の総数が前年と比べて低下していることが観察されました。同時に、中南米では報告事例が増加しました。

この観察に対する 1 つの解釈として、サイバー犯罪者が、法執行機関の監査を誘発するリスクが高いと認識されている分野から、より甘い標的に切り替えたことが挙げられます。マイクロソフトは、ランサムウェア関連のサポートへの問い合わせの減少を説明できるほど世界中で企業ネットワークセキュリティの大幅な改善は観察していないため、最もありうる理由として、2021 年と 2022 年の法執行活動によって犯罪活動のコストが増加したことと、2022 年の地政学的な事象が合わさったものと考えることができます。

最も広く利用されている RaaS 運用の 1 つは、2019 年に活動を始めた REvil (別名 Sodinokibi) として知られるロシア語圏の犯罪グループに属しています。2021 年 10 月、REvil のサーバーは、国際的な法執行である GoldDust 作戦の一環としてオフラインになりました。[7] 2022 年 1 月、ロシアは容疑のかかった 14 人の REvil メンバーを逮捕し、25 の拠点を強制捜査しました。[8] これは、ロシアが自国の領土でランサムウェア オペレーターに対して初めて行動を取った事例です。

2022 年、法執行活動は捜査のペースを緩めたと思われますが、脅威アクターは今後の取り締まりを回避する新しい戦略を生み出す可能性があります。さらに、ロシアのウクライナ侵攻に伴うロシアと米国の緊張は、ランサムウェアに対する世界的な闘いに対してロシアが始めつつあった協力に終止符を打ちました。REvil の逮捕により不確実な状態が短期間続いた後、米国とロシアはランサムウェア アクターを追跡する点での協力関係を解消しました。つまり、サイバー犯罪者がロシアをもう一度安全な避難所と見なす可能性があります。

先に目を向けると、マイクロソフトでは、ランサムウェア活動のペースは以下の重要な質問がどうなるかによって変わると予測しています。

1. 各国政府は、ランサムウェアの犯罪者による自国内での活動を防止する措置を取るのか、それとも国外から活動を行うアクターを阻止しようとするのか？
2. ランサムウェア グループは、戦術を変更してランサムウェアの必要性を排除し、恐喝スタイルの攻撃を用いるか？
3. 組織は、犯罪者による脆弱性の悪用よりもすばやく IT 運用を最新化して変革させることができるか？
4. 身代金の支払いを追跡およびトレースする技術が進歩した結果、身代金を受け取る攻撃者は戦術と交渉方法を変化させざるを得なくなるか？

2022 年、法執行活動は捜査のペースを緩めたと思われますが、脅威アクターは今後の取り締まりを回避する新しい戦略を生み出す可能性があります。

2 倍

いくつかの地域ではランサムウェア攻撃が減少しましたが、身代金の要求額は 2 倍以上になっています。

実用的なインサイト

1. すべてのランサムウェア ファミリーは同じセキュリティの弱点を利用してネットワークに影響を与えるため、総合的なセキュリティ戦略に注力します。
2. 多層防御保護の基本レベルを高めてセキュリティ運用を最新化するため、セキュリティの基礎を更新して維持します。クラウドに移行することで、脅威をすばやく検出し、迅速に対応できるようになります。

詳しい情報のリンク

- ランサムウェアから組織を保護する | マイクロソフト セキュリティ
- 侵害から環境を守る 7 つの方法 | マイクロソフト セキュリティ ブログ
- AI ベースの防御を強化し、人の手で操作されるランサムウェアを阻止する | Microsoft 365 Defender Research Team
- Security Insider: 最新のサイバーセキュリティのインサイトと更新情報を確認する | マイクロソフト セキュリティ

サービスとしてのサイバー犯罪

サービスとしてのサイバー犯罪 (CaaS) は拡大と進化を続けており、世界中のお客様にとって脅威となります。マイクロソフト デジタル犯罪対策ユニット (DCU) の観察によると、CaaS エコシステムは拡大を続けており、オンライン サービスの増加は、BEC や人の手で操作されるランサムウェアなど、さまざまなサイバー犯罪の一因となりました。フィッシングは、今でもサイバー犯罪者から好まれている攻撃手法です。アカウントを盗み出してそのアクセス権を販売することから大きな利益を得ることができるからです。

CaaS 市場の拡大に対応するため、DCU はリスニング システムを強化し、インターネット、ディープ ウェブ、綿密に審査されたフォーラム[9]、専用 Web サイト、オンライン ディスカッション フォーラム、メッセージング プラットフォームのエコシステム全体で CaaS サービスを検出および識別できるようにしました。

サイバー犯罪者は、一定の成果を上げるため、複数のタイム ゾーンと言語にまたがって協力するようになりました。たとえば、アジアにいる人が管理しているある CaaS Web サイトはヨーロッパで運用されており、アフリカで悪意のあるアカウントを作成しています。このような運用では、管轄区域が複数にまたがるため、法律と執行に関する複雑な課題が発生します。これに対応するため、DCU は、CaaS 攻撃に利用される悪意のある犯罪インフラを使えなくし、世界中の法執行機関と協力して犯罪者に責任を取らせることに重点を置いています。

サイバー犯罪者は、リーチ、範囲、利益を最大化するため、分析を利用することが増えています。合法的な企業と同様、CaaS Web サイトでは製品とサービスの有効性を実証し、確固とした評判を維持する必要があります。たとえば、CaaS Web サイトは、侵害したアカウントへの定期的なアクセスを自動化し、侵害した資格情報の有効性を確保しています。サイバー犯罪者は、パスワードがリセットされたり脆弱性に修正プログラムが適用されたりした場合は、特定のアカウントの販売を中止します。マイクロソフトの観察による、品質管理プロセスとして購入者にオンデマンド検証を提供している CaaS Web サイトが増えています。その結果、CaaS の Web サイトがアクティブなアカウントとパスワードを販売していることを購入者が確信できると同時に、盗んだ資格情報が販売前に修正された場合に CaaS 提供者に生じる潜在的なコストを抑えることができます。

さらに、DCU は、特定の地理的な場所、指定されたオンライン サービス プロバイダー、具体的に的を絞った個人、職業、業界から盗んだアカウントを購入するオプションを購入者に提供する CaaS Web サイトも観察しました。頻繁に注文のあるアカウントは、CFO や「売掛金勘定」など、請求を処理する担当者や部門に集中しています。同様に、公共事業に参加している業界は、入札プロセスを通じて入手可能な情報の量が多いため、標的となることがよくあります。

DCU による CaaS の調査では、次のようにいくつかの重要なトレンドが明らかになりました。

サービスの数が増え、巧妙さがますます高まっている。

例として、フィッシング攻撃を自動化するために使用される、侵害された Web サーバーで構成される Web シェルの進化が挙げられます。DCU は、CaaS リセラーが、専用の Web ダッシュボードを通じてフィッシング キットやマルウェアのアップロードを簡略化していることを観察しました。それに続き、CaaS 提供者は、スパム メッセージ サービスや、地理的な場所や職業などの定義済みの属性に基づくスパム受信者リストなど、ダッシュボードを通じて脅威アクターに追加のサービスを販売しようとすることがよくあります。単一の Web シェルが複数の攻撃キャンペーンに使用されている事例も観察されています。これは、脅威アクターが侵害したサーバーへの永続的なアクセスを維持している可能性を示唆しています。さらに、CaaS エコシステムの一部として提供される匿名化サービスや、仮想プライベート ネットワーク (VPN) および仮想プライベート サーバー (VPS) アカウントのサービスの増加も観察されています。ほとんどの場合、提供される VPN/VPS は、元々は盗まれたクレジット カードを通じて調達されたものです。また、CaaS Web サイトでは、サイバー犯罪攻撃をオーケストレーションするためのプラットフォームとして、リモート デスクトップ プロトコル (RDP)、セキュア シェル (SSH)、cPanel も多く提供されていました。CaaS 提供者は、さまざまな種類のサイバー攻撃を可能にする適切なツールとスクリプトを使って RDP、SSH、cPanel を構成しています。

仮想通貨での支払いを求めるホモグリフ ドメイン作成サービスが増えている。

ホモグリフ ドメインは、外見が他の文字と同一文字かほぼ同一の文字を使って正当なドメイン名を偽装しています。目的は、ホモグリフ ドメインが正規のドメインであるとユーザーに勘違いさせることです。このようなドメインは、ありふれた脅威であり、多くのサイバー犯罪の入り口となっています。CaaS サイトでは、カスタム ホモグリフ ドメイン名が販売されるようになりました。そのため、購入者は特定の企業やドメイン名の偽装をリクエストできるようになっています。支払いを受け取ると、CaaS 提供者はホモグリフ生成ツールを使ってドメイン名を選択し、悪意のあるホモグリフを登録します。このサービスの支払い方法は、ほとんどの場合仮想通貨に限定されています。

2,750,000

世界的なサイバー犯罪に利用するつもりであった犯罪者に先手を打つため、今年 DCU によって阻止されたサイト登録の数。

サービスとしてのサイバー犯罪

(続き)

侵害した資格情報を購入できるようにしている CaaS 提供者が増えている。

侵害した資格情報を使うと、メール メッセージング サービス、企業のファイル共有リソース、OneDrive for Business などのユーザー アカウントに不正アクセスが可能になります。管理者の資格情報が侵害された場合、不正なユーザーが機密ファイル、Azure リソース、会社のユーザー アカウントにアクセスする可能性があります。DCU の調査によると、多くの事例で、資格情報の検証を自動化する手段として、複数のサーバーで同じ資格情報が不正に使用されていることがわかりました。このパターンは、侵害されたユーザーが複数のフィッシング攻撃の被害に遭ったか、ユーザーのデバイスに存在するマルウェアによりボットネット キーロガーが資格情報を収集できるようになっていることを示唆しています。

検出を回避するため、機能が強化された CaaS サービスおよび製品が登場している。

ある CaaS 提供者は、検出および防止システムを迂回する目的で複雑さと匿名化機能を高めたフィッシング キットを、1 日あたりわずか 6 米ドルという価格で提供しています。このサービスは、次のレイヤーやサイトへのトラフィックを許可する前にチェックを実行する一連のリダイレクトを行います。その 1 つは、デバイスのフィンガープリンティング (仮想マシンであるかどうかなど) を実行し、使用されているブラウザーとハードウェアに関する詳細情報を収集するため、90 を超えるチェックを実行します。すべてのチェックに合格した場合、フィッシングに使用されるランディングページにトラフィックが送信されます。

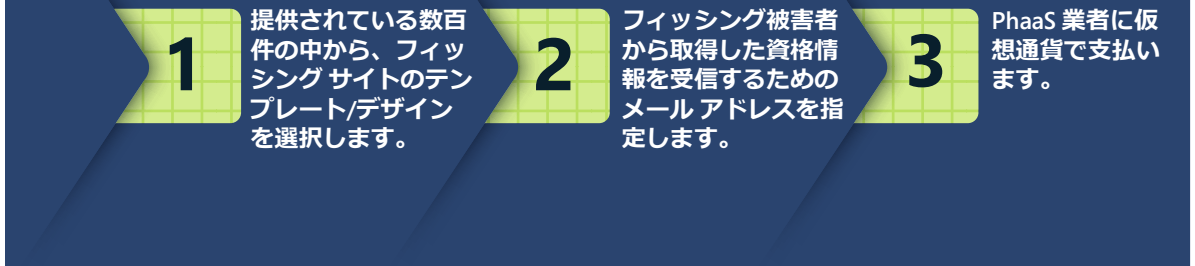
エンド ツー エンドのサイバー犯罪サービスが、マネージド サービスへのサブスクリプションを販売している。

運用セキュリティが低い場合、通常はオンライン犯罪の各ステップで脅威アクターの存在が発覚する可能性があります。複数の CaaS サイトからサービスを購入した場合は発覚と特定のリスクが高まります。DCU は、ダーク ウェブで気になるトレンドを観察しました。ソフトウェア コードを匿名化し、Web サイト テキストを一般名かして発覚を減らすサービスが増加しているのです。エンド ツー エンドのサイバー犯罪サブスクリプション サービス プロバイダーは、すべてのサービスを管理し、OCN にサブスクライブする際の発覚リスクを減らすという結果を保証しています。リスクが低下するため、エンド ツー エンド サービスの人気が高まっています。

サービスとしてのフィッシング (PhaaS) は、エンド ツー エンド サイバー犯罪サービスの一例です。PhaaS は、完全検出不可能サービス (FUD) として知られる以前のサービスの進化形であり、サブスクリプション ベースで提供されます。一般的な PhaaS の契約条件には、フィッシング Web サイトを 1 か月間アクティブに保つことなどがあります。

さらに、DCU は、サブスクリプション モデルで分散型サービス拒否 (DDoS) を提供する CaaS 提供者を特定しました。このモデルでは、攻撃を実行するのに必要なボットネットの作成と保守を CaaS 提供者に外注します。各 DDoS サブスクリプションの顧客は、運用セキュリティと 24 時間年中無休のサポートを強化するため、暗号化されたサービスを受け取ります。DDoS サブスクリプション サービスでは、さまざまなアーキテクチャと攻撃方法が用意されているため、購入者が攻撃対象のリソースを選択するだけで、提供者は攻撃を実行するボットネット上の一連の侵害されたデバイスに対するアクセスを提供できます。DDoS サブスクリプションのコストはわずか 500 米ドルです。

PhaaS のサイバー犯罪者は、単一のサブスクリプションで複数のサービスを提供しています。通常、購入者は次の 3 つのアクションを実行するだけでかまいません。



これらのステップが完了すると、PhaaS 業者は、特定のユーザーを標的にするための 3 ～ 4 層からなるリダイレクトおよびホスティング リソースを備えたサービスを作成します。その後、キャンペーンが開始されて、被害者の資格情報が収集され、確認された後、購入者から指定されたメール アドレスに送られます。プレミアムとして、多くの PhaaS 業者が、パブリック ブロックチェーン上のフィッシング サイトをホストし、どのブラウザーからでもアクセスして、リダイレクトによってユーザーを分散台帳のリソースにポイントできるようにしています。

CaaS サイバー犯罪者を特定して阻止するツールと手法を開発する DCU の取り組みは続いています。CaaS サービスが進化しているため、特に仮想通貨での支払いを阻止するという点で大きな課題があります。

犯罪における仮想通貨の使用

仮想通貨の採用が一般的になるにつれて、犯罪者は法執行機関やマネー ロンダリング防止 (AML) 対策を回避するために仮想通貨を利用することが増えています。その結果、法執行機関がサイバー犯罪者に対する暗号通貨の支払いを追跡し、トレースするのが難しくなっています。

ブロックチェーン ソリューションに対する世界全体での支出は過去 4 年間で約 340% 増加し、新しい仮想通貨ウォレットは約 270% 増加しました。一意のウォレットは世界全体で 8,300 万件以上あり、すべての暗号通貨の総時価総額は、2022 年 7 月 28 日現在約 1.1 兆米ドルでした。[10]

出典 : Twitter.com — @PeckShieldAlert (PeckShield は、中国を拠点とするブロックチェーン セキュリティ企業です)。

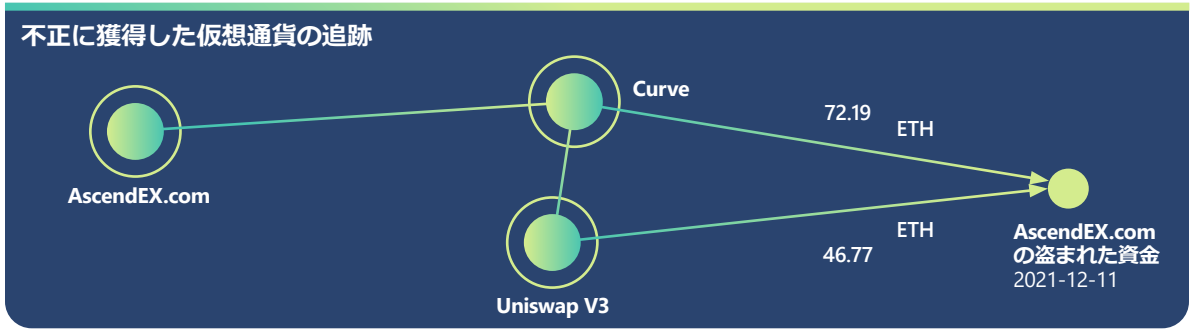
ランサムウェアの支払いの追跡

ランサムウェアは、不法に獲得される仮想通貨の最大要因の 1 つです。ランサムウェア攻撃で使用される悪意のある技術インフラを停止させるため (たとえば、2022 年 4 月の Zloader の機能停止 [11])、マイクロソフトの DCU は犯罪者のウォレットを追跡し、仮想通貨の追跡および回収機能を実現しました。

DCU の調査担当者は、ランサムウェア アクターが、被害者とのコミュニケーション戦術を進化させ、通貨の流れを隠していることを観察しました。サイバー犯罪者は最初、ビットコイン アドレスを身代金メモに含めていました。しかし、その場合はブロックチェーンでの支払いトランザクションに追いやすかったため、ランサムウェア アクターはウォレット アドレスを含めるのをやめ、メール アドレスやチャット Web サイトのリンクを添付して被害者に身代金の支払いアドレスを伝えていました。セキュリティ調査担当者や法執行機関が被害者のふりをしてウォレット アドレスを入手するのを防ぐため、被害者ごとに固有の Web ページとログインを作成していたアクターもいます。犯罪者が足跡を隠そうとしているにもかかわらず、法執行機関やブロックチェーン上の動きを追跡できる暗号分析企業と連携することにより、一部の支払い済み身代金を回収することができます。

トレンド : 不正な収益の DEX ロンダリング

サイバー犯罪者にとって重要な問題は、仮想通貨を法定通貨に換金することです。サイバー犯罪者には、換金に利用できる手段がいくつかあり、それぞれにリスクの程度が異なります。リスクを軽減する 1 つの方法として、中央集権型取引所 (CEX)、ピア ツー ピア (P2P)、店頭取引 (OTC) など、利用可能な現金化オプションを使って現金化する前に、分散型取引所 (DEX) を通じて収益をロンダリングする方法が使用されます。DEX は、多くの場合 AML 対策に従っていないため、ロンダリングの場所としては魅力的です。



マイクロソフトのデジタル犯罪対策ユニットは、仮想通貨調査ツール Chainalysis を使って、AcendEX のハッカーが Uniswap に加えて小規模な DEX である Curve で資金をスワップしたことを検出しました。この図は、チームが発見したロンダリング ルートを示しています。各円はウォレットのクラスターを表し、各行の数字は、ロンダリング目的で送信されたイーサリアムの合計金額を表しています。

2021 年 12 月、ハッカーたちが世界中の仮想通貨取引プラットフォームである AscendEx を攻撃し、顧客が所有する暗号通貨約 7,770 万米相当を盗みました。[12] AscendEx は、ブロックチェーン分析企業に依頼し、他の CEX と連絡を取ったため、盗まれた資金を受け取ったウォレットをブラックリストに登録できできました。さらに、コインが送信されたアドレスは、イーサリアム ブロックチェーン エクスプローラーである Etherscan でそのようにラベル付けされました。[13] アラートとブラックリスト入りを回避するため、ハッカーたちは 2022 年 2 月 18 日、イーサリアムから世界最大の DEX の 1 つである Uniswap に 150 万米ドルを送金しました。[14]

DEX により強力な AML 対策が採用されたため、そのプラットフォームでロンダリング活動を防げたため、サイバー犯罪者はコイン タンブリングや無認可の取引所など、他の難読化手法を使用せざるを得なくなりました。例として、Uniswap は最近、ブラックリストを使用することで、違法行為に関与していることがわかっているウォレットの同取引所での取引を禁止すると発表しました。[15]

実用的なインサイト

1. サイバー犯罪の被害に遭い、仮想通貨を使用して犯罪者に支払った場合、お近くの法執行機関にお問い合わせください。失った資金の追跡と回収に役立つ可能性があります。
2. DEX を選択するときは、実施されている ALM 対策をよく調べてください。

詳しい情報のリンク

- ますます複雑化するクロプトジャッキングに対するハードウェア ベースの脅威防御 | Microsoft 365 Defender Research Team

進化するフィッシング脅威の状況

資格情報フィッシング スキームは増加傾向にあり、すべての受信トレイを無差別に標的としているため、場所にかかわらずユーザーにとって大きな脅威となっています。マイクロソフトの研究者が追跡して保護している脅威のうち、フィッシング攻撃は他のすべての脅威より桁違い多くなっています。

マイクロソフトは、Defender for Office のデータを使って、悪意のあるメールや侵害された ID アクティビティを確認しています。Azure Active Directory Identity Protection も、侵害された ID イベント アラートを通じて、より多くの情報を提供しています。マイクロソフトは、Defender for Cloud Apps を使って、侵害された ID データ アクセス イベントを調べており、Microsoft 365 Defender (M365D) により製品間の相関関係が提供されています。侵入拡大メトリックは、Defender for Endpoint (攻撃行動アラートおよびイベント) と Defender for Office (悪意のあるメール) から取得されており、この場合も M365D から製品間の相関関係が提供されています。

7 億 1,000 万
1 週間あたりにブロックされているフィッシング メールの数。

1 時間 12 分
フィッシング メールの被害に遭った場合に攻撃者が個人データにアクセスするまでにかかる平均時間。[16]

1 時間 42 分
デバイスが侵害された後、攻撃者が企業ネットワーク内で侵入を拡大し始めるまでにかかる平均時間。[17]

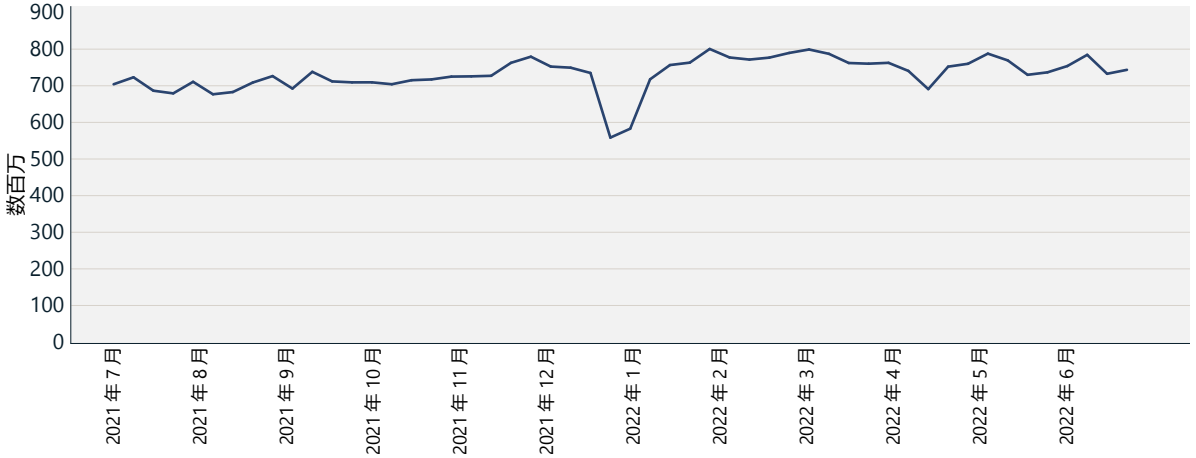
Microsoft 365 の資格情報は、攻撃者が最も欲しがっているアカウントの種類の 1 つです。ログイン資格情報が侵害されてから攻撃者が行う行動は多くありますが、たとえば、企業内でしか利用できないコンピューター システムにログインして、マルウェアやランサムウェアへの感染を促し、SharePoint ファイルにアクセスすることにより会社の機密データと機密情報を盗み出します。また、Outlook を使って悪意のあるメールを送信し続けることにより、フィッシングをさらに広めます。

標的がより広範なキャンペーン、資格情報、寄付、個人情報のフィッシングに加えて、攻撃者は多額の収益を得るために特定のビジネスを標的にしています。企業に対する金銭的な利益を狙ったメール フィッシング攻撃は、「BEC 攻撃」と総称されています。マイクロソフトは、毎月数百万通もの BEC メールを検出しています。これは、全フィッシング メールの 0.6% に相当します。2022 年 5 月に発表された IC3 によるレポート[18] は、BEC 攻撃による損失が上昇傾向にあることを示しています。

フィッシング攻撃で使用される手法は、ますます複雑になっています。攻撃者は、対策を回避しようと自身の技術を実装できるように新しい方法を適応させているため、キャンペーン運用インフラをホストする方法や場所の複雑さが増しています。つまり、組織は、悪意のあるメールをブロックして、個々のユーザー アカウントのアクセス制御を強化するためのセキュリティ ソリューションを実装する戦略を定期的に見直す必要があります。

531,000
マイクロソフトのデジタル犯罪対策ユニットは、Defender for Office によってブロックされた URL に加えて、マイクロソフト外でホストされている 531,000 件の一意のフィッシング URL の解体を指示しました。

フィッシング メールの検出数



1 週間あたりのフィッシング検出数は増加を続けています。12 月から 1 月の減少は季節的な要因であり、昨年のレポートでも報告されています。出典 : Exchange Online Protection のシグナル。

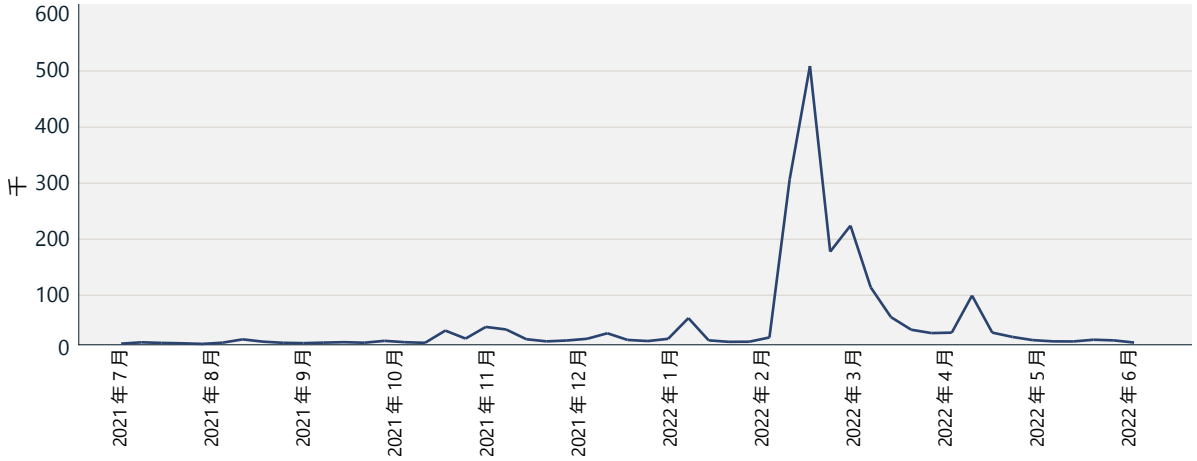
進化するフィッシング脅威の状況

(続き)

フィッシング メールは、前年比で増加し続けています。2020 年と 2021 年のリモート ワークへの移行により、変化する職場環境に乗じることを目的としたフィッシング攻撃の大幅な増加が見られました。フィッシング オペレーターは、COVID-19 パンデミック、Google Drive や OneDrive ファイル共有などのコラボレーションおよび生産性向上ツールに関係するテーマなど、世界の主要イベントに合わせたルアーを使った新しいメール テンプレートをすばやく採用しています。COVID-19 のテーマは減少していますが、2022 年 3 月上旬からはウクライナでの戦争が新たなルアーとなりました。マイクロソフトの研究者は、ウクライナ国民を助けるとして、暗号通貨 (ビットコインとイーサリアム) での寄付を呼びかける合法的な組織になりすましたメールが驚くほど増加したのを観察しました。

2022 年 2 月下旬にウクライナでの戦争が始まってからわずか数日後、企業のお客様の間で見つかったイーサリアム アドレスを含むフィッシング メールの検出数が大幅に増加しました。3 月の第 1 週には、50 万件のフィッシング メールにイーサリウム ウォレット アドレスが含まれており、このとき合計検出数がピークに達しました。戦争が始まる前、フィッシングとして検出された他のメールに含まれていたイーサリウム ウォレット アドレスの数はかなり少なく、平均すると 1 日あたり数千件のメールでした。

イーサリウム ウォレット アドレスが記載されたフィッシング メール



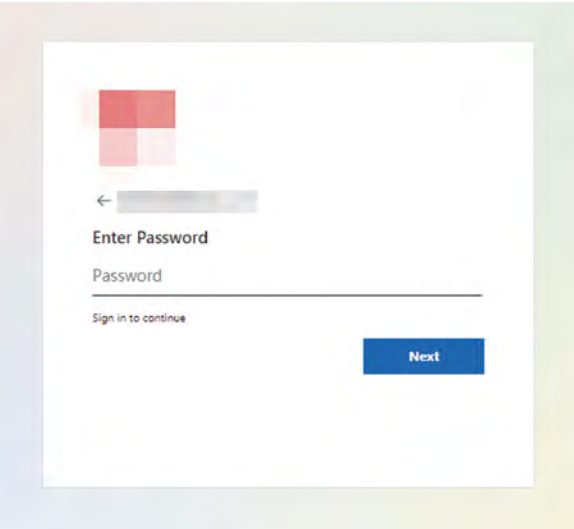
イーサリアム ウォレット アドレスを含むフィッシングとして検出されたメールの合計数は、ウクライナとロシアの紛争が始まったときに増加し、初期の急増後、徐々に減少しました。

フィッシング詐欺師は、合法的なインフラを使って運用することがこれまで以上に多くなっており、運用のさまざま側面を侵害することを目的としたフィッシング キャンペーンが増えているため、自分で購入、ホスト、運用を行う必要がありません。たとえば、悪意のあるメールは、侵害された送信者アカウントから送信される可能性があります。攻撃者は、評判スコアが高く、新たに作成されたアカウントやドメインより信頼できると見られているそれらのメール アドレスを使ってメリットを享受できます。さらに高度なフィッシング キャンペーンでは、DMARC[19] が誤って「アクションなし」ポリシーで設定したドメインから攻撃者が送信したりなりすましたりし、メールなりすましのドアを開けていることがわかっています。

大規模なフィッシング運用では、クラウド サービスとクラウド仮想マシン (VM) を使って大規模な攻撃を運用化する傾向があります。攻撃者は、SMTP メール リレーまたはクラウド メール インフラを使用して VM からのメールを展開および配信するプロセスを完全に自動化し、そのような正規のサービスの高い配信率と良い評判を利用することができます。これらのクラウド サービスを通じて悪意のある電子メールの送信が許可された場合、防御者は強力なメール フィルタリング機能を使用してメールが環境に侵入するのを阻止する必要があります。

マイクロソフト アカウントは、Microsoft 365 ログイン ページを偽装する多数のフィッシング ランディング ページから明らかなように、フィッシング オペレーターの最大の標的であり続けています。たとえば、フィッシング詐欺師は、受信者に合わせてカスタマイズされた一意の URL を生成することにより、マイクロソフトのログイン エクスペリエンスを自身のフィッシング キットを一致させようとしています。この URL は、資格情報を収集するために開発された悪意のある Web ページに転送されますが、URL 内のパラメーターには特定の受信者のメール アドレスが含まれることになります。標的がそのページに移動すると、フィッシング キットはメール受信者に合わせてカスタマイズされたユーザー ログイン データと企業ロゴを事前入力し、標的となった会社のカスタム Microsoft 365 ログイン ページの外観をミラーリングします。

動的コンテンツを使ってマイクロソフト ログインを偽装したフィッシング ページ

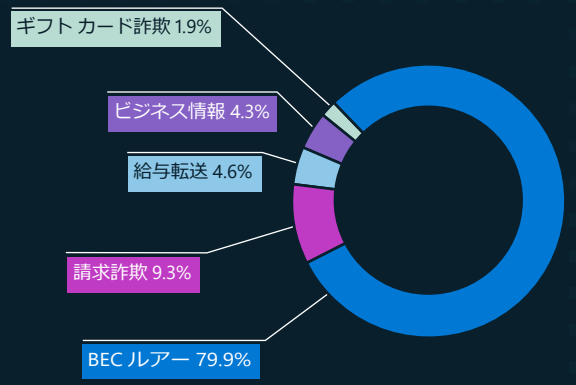


注目すべきビジネス メール詐欺

サイバー犯罪者は、セキュリティ設定を突破し、個人、企業、組織を標的とする、ますます複雑なスキームと手法を開発しています。マイクロソフトは、それに対応して BEC 施行プログラムをさらに強化するため、リソースに多額の投資を行っています。

BEC は、最も犠牲の大きい金融サイバー犯罪であり、2021 年の修正損失額は 24 億米ドルと推定されています。これは、世界中のインターネット犯罪による損失上位 5 件の 59% 超を占めています。[20] 問題の規模と、BEC からユーザーを保護する最善の方法を理解するため、マイクロソフトのセキュリティ研究者は、攻撃で最もよく使用されているテーマを追跡してきました。

BEC のテーマ (2022 年 1 月～ 6 月)



BEC のテーマ (発生率別)

BEC のトレンド

BEC 攻撃者は通常、エントリ ポイントとして、潜在的な被害者との会話を開始し、親密な関係を築こうとします。同僚やビジネス上の知人になりすまし、攻撃者は金銭を送金する方向に会話を徐々にリードしています。BEC のルアーとして追跡されている導入メールは、検出された BEC メールの 80% 近くを占めています。過去 1 年間にマイクロソフトのセキュリティ研究者によって特定されたその他のトレンドは、次のとおりです。

- 2022 年に BEC 攻撃で最もよく使われた手法はスプーフィング [21] と偽装でした。[22]
- 被害者に最も多額の金銭的被害をもたらした BEC サブタイプは、請求詐欺でした (マイクロソフトの BEC キャンペーン調査で確認された量と要求金額に基づく)。
- 買掛金報告書や顧客連絡先などのビジネス情報を盗難することにより、攻撃者は信ぴょう性のある請求詐欺を作ることができます。
- ほとんどの給与転送要求は無料のメール サービスから送信され、侵害されたアカウントから送信されることはほとんどありませんでした。これらの送信元からのメールの量は、最も一般的な給与支払日である毎月 1 日と 15 日に急増しています。
- 詐欺の手段としてよく知られているにもかかわらず、ギフト カード詐欺は検出された BEC 攻撃の 1.9% に過ぎませんでした。

実用的なインサイト

フィッシングに対する防御

組織がフィッシング被害に遭う可能性を減らすため、IT 管理者は以下のポリシーと機能を実装することをお勧めします。

1. 不正アクセスを制限するため、すべてのアカウントで MFA の使用を必須にする。
2. 高度な特権を持つアカウントの条件付きアクセス機能を有効にし、通常は組織のトラフィックが生成されない国、地域、IP からのアクセスをブロックする。
3. 経営陣、支払いまたは購入アクティビティに関与する社員、その他の特権アカウントに物理的なセキュリティ キーの使用を検討する。
4. Microsoft SmartScreen などのサービスをサポートするブラウザーの使用を強制し、不審な行動が行われた URL を分析して、既知の悪意のある Web サイトへのアクセスをブロックする。[23]
5. メールが受信トレイに届く前にフィッシングの可能性が高いメールを隔離し、URL と添付ファイルをサンドボックスで実行する機械学習ベースのセキュリティ ソリューション (Office 365 の Microsoft Defender など) を使用する。[24]
6. 組織全体で、偽装となりすましの保護機能を有効にする。
7. DomainKeys Identified Mail (DKIM) と Domain-based Message Authentication Reporting & Conformance (DMARC) アクション ポリシーを構成し、評判の高い送信者を偽装している可能性のある非認証メールの配信を防ぐ。
8. テナントとユーザーが作成した許可ルールを監査し、ドメインと IP ベースの広範な例外を削除する。これらのルールは多くの場合優先され、メール フィルタリングを通じて既知の悪意のあるメールが許可される可能性があります。
9. フィッシング シミュレーターを定期的に実行して、組織全体で潜在的なリスクを測定し、脆弱なユーザーを特定して教育する。

詳しい情報のリンク

- Cookie の盗難から BEC へ : 攻撃者が AiTM フィッシング サイトをさらなる金融詐欺のエントリ ポイントとして利用する | Microsoft 365 Defender Research Team、Microsoft Threat Intelligence Center (MSTIC)

ホモグリフ詐欺

BEC とフィッシングは、よくあるソーシャル エンジニアリング戦術です。ソーシャル エンジニアリングは犯罪において重要な役割を果たし、信頼を得ることで犯罪者とやり取りしてもよいと標的に信じ込ませます。

物理的な商取引では、製品やサービスの出所に対する信頼を確保するために商標が使用されますが、偽造品は商標を不正利用していることになります。同様に、サイバー犯罪者は、フィッシング攻撃の際に標的になじみのある連絡先を装い、ホモグリフを使って潜在的な被害者をだまします。

ホモグリフは、BEC でメール通信に使用されるドメイン名であり、標的をだますため、文字を同一の文字かほぼ同一の文字に置き換えます。

BEC で使用されるホモグリフ手法

通常、BEC には 2 つのフェーズがあり、最初のフェーズでは資格情報が侵害されます。このような種類の資格情報の漏えいは、フィッシング攻撃や大規模なデータ漏えいの結果生じる可能性があります。その後、資格情報がダーク ウェブで販売または取引されます。

2 つ目のフェーズは、攻撃者が侵害された資格情報を利用し、ホモグリフ メール ドメインを使って高度なソーシャル エンジニアリングを行う詐欺フェーズです。

BEC 攻撃の順序

手法	ホモグリフの手法を示すドメインの割合
l を l に置き換え	25%
I を i に置き換え	12%
g を q に置き換え	7%
m を rn に置き換え	6%
.com を .cam に置き換え	6%
o を 0 に置き換え	5%
I を ll に置き換え	3%
i を ii に置き換え	2%
w を vv に置き換え	2%
ll を l に置き換え	2%
a を e に置き換え	2%
m を nn に置き換え	1%
I を ll に置き換え、i を l に置き換え	1%
u を o に置き換え	1%

2022 年 1 月～ 7 月に行われた 1700 件を超えるホモグリフ ドメインの分析。170 個のホモグリフ手法が使用されましたが、ドメインの 75% で使用されていた手法はわずか 14 個にすぎません。

ホモグリフの事例

被害者が認識しているメール ドメインと同じに見えるホモグリフ ドメインは、同一のユーザー名でメール プロバイダーに登録されています。その後、新しい支払い手順が記載されている乗っ取られたメールが、乗っ取られたドメインから送信されます。

犯罪者は、オープン ソースのインテリジェンスとメール スレッドへのアクセスを利用し、請求と支払いの責任者を特定します。次に、個々の送信請求書のメール アドレスを偽装します。この偽装は、本物の送信者のホモグリフである同一のユーザー名とメール ドメインで構成されています。

攻撃者は、正当な請求書を含むメール チェーンをコピーし、請求書を変更して自身の銀行口座情報を含めます。次に、修正されたこの新しい請求書は、ホモグリフ偽装メール アドレスから標的に再送信されます。状況の筋が通っており、メールは本物のように見えるため、多くの場合、標的は詐欺の指示に従います。

実用的なインサイト

1. Safe Links や SmartScreen など、不審な行動が行われた URL を分析して、既知の悪意のある Web サイトへのアクセスをブロックするサービスをサポートするブラウザーの使用を強制します。[25]
2. メールが受信トレイに届く前にフィッシングの可能性が高いメールを隔離し、URL と添付ファイルをサンドボックスで実行する機械学習ベースのセキュリティ ソリューションを使用します。

詳しい情報のリンク

- インターネット犯罪苦情センター (IC3) | ビジネスメール詐欺 : 430 億件の詐欺
- なりすましインテリジェンス インサイトー Office 365 | マイクロソフト ドキュメント
- 偽装インサイトー Office 365 | マイクロソフト ドキュメント

マイクロソフトによるコラボレーションの初期段階からのボットネット阻止のタイムライン

DCU は、10 年以上にわたりサイバー犯罪を未然に防ぎ、26 件のマルウェアと国家レベルの脅威を阻止してきました。DCU チームがより高度な戦術とツールを使ってそのような不正運用を止めているため、一歩先を行く試みの点でサイバー犯罪者もそのアプローチを進化させています。ここでは、DCU が阻止したボットネットのサンプルと、それらを停止するためにマイクロソフトが採用した戦略を示すタイムラインを紹介します。

2008 年

Conficker ボットネット

説明： Windows OS を標的とした急速に拡散するワームで、共通のネットワークにある何百万台ものコンピューターとデバイスに感染します。世界中でネットワークの停止を引き起こしました。

コラボレーション： このような種類としては初めてのコンソーシアムである Conficker Working Group を設立。マイクロソフトは、世界中の 16 の組織と連携してボットを打破しました。

マイクロソフトの対応： このグループは、多くの国際的管轄区域でコラボレーションし、Conficker の停止に成功しました。

2009 年

Waledac ボットネット

説明： メール アドレスと分散スパムを収集した米国のドメインを持つ、複雑なスパム ボットネット。世界中で最大 9 万台のコンピューターに感染しました。[26]

コラボレーション： もう 1 つのコンソーシアムとして、マイクロソフト マルウェア プロテクション センター (MMPC) を設立。学者との緊密なコラボレーションに焦点を当てています。[27]

マイクロソフトの対応： マイクロソフトは、C2 の階層型阻止アプローチを使い、警告なしで米国ベースのドメインを押収することによって、悪意のあるアクターを驚かせました。[28] また、マイクロソフトは Waledac のサーバーによって使用されていたほぼ 280 件のドメインの一時的な所有権を付与しました。

2011 年

マイクロソフト デジタル犯罪対策ユニットが設立される

コラボレーション： 調査担当者、弁護士、エンジニアから成るチーム全体を緊密に統合することで、マイクロソフト エコシステムに影響を与えるサイバー犯罪を阻止することを目的としていました。

マイクロソフトのアプローチ： 目標は、さまざまなマルウェアの技術的側面をよりよく理解し、効果的な阻止戦略を策定するため、マイクロソフトの法務チームにそれらのインサイトを提供することです。

2013 年

Rustock ボットネット

説明： インターネット プロバイダーをプライマリ C2 として利用するバックドア トロイの木馬型スパム メール ボット。医薬品の販売を目的としています。

コラボレーション： マイクロソフトは、Rustock によって販売される医薬品について理解し、オランダの法執行機関と緊密に協力するため、Pfizer Pharmaceuticals とパートナーシップを築きました。[29]

マイクロソフトの対応： マイクロソフトは、米国連邦保安官およびオランダの法執行機関と協力し、同国の C2 サーバーを停止しました。今後のドメイン ジェネレーター アルゴリズム (DGA) をすべて登録し、ブロックしました。

Sirefef/Zero Access ボットネット

説明： マルウェアをインストールしたり個人情報を盗み出したりする危険な Web サイトにユーザーを誘導するよう設計された広告ボットネット。主に米国と西ヨーロッパにおいて 200 万台を超えるコンピューターに感染し、広告主の損失は 1 か月あたり 270 万米ドル以上になります。

コラボレーション： FBI および欧州警察のサイバー犯罪センターと緊密に連携し、ピア ツー ピア インフラを停止させました。

マイクロソフトの対応： Zero Access ネットワークに参加して、犯罪者の C2 サーバーを置き換え、ダウンロード サーバー ドメインの押収に成功しました。

2019 年

Trickbot ボットネット

説明： 金融サービス業界を標的とし、世界中に断片化されたインフラを持つ高度なボットネット。IoT デバイスを侵害しました。

コラボレーション： マイクロソフトは、Financial Services Information Sharing and Analysis Center (FS-ISAC) と連携し、Trickbot を停止しました。[30]

マイクロソフトの応答： DCU は、さまざまな国の具体的な法律を考慮に入れ、ボット インフラを特定して追跡するシステムを構築し、アクティブなインターネット プロバイダー向けの通知を生成しました。

2022 年

阻止に重点を置き続ける

説明： マイクロソフトは、過去 1 年間に 7 つの脅威アクターのインフラを解体し、追加のマルウェアの配布、被害者のコンピューターの制御、さらなる被害者の攻撃を防ぐことができました。

コラボレーション： インターネット サービス プロバイダー、政府、法執行機関、民間企業との連携により、マイクロソフトは世界中の 1700 万を超えるマルウェア被害者の救済するための情報を共有しました。

将来を見据えて

DCU はイノベーションを続けており、ボットネットの阻止における経験を活かして、マルウェア以外でも組織的な活動を行うことを目指しています。継続的な成功を収めるには、独創的なエンジニアリング、情報の共有、革新的な法理論、官民のパートナーシップが必要です。

サイバー犯罪によるインフラの悪用

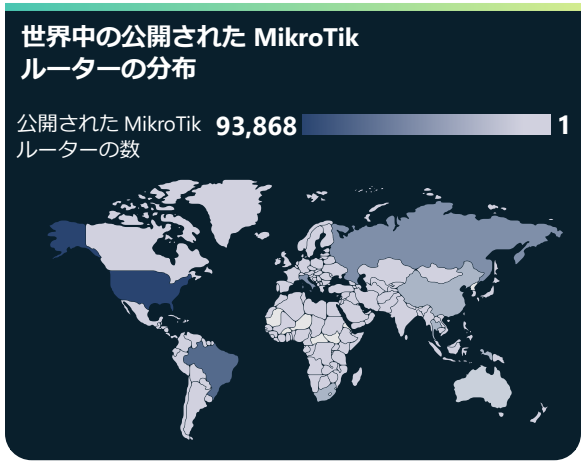
犯罪者指揮統制インフラとしてのインターネット ゲートウェイ

サイバー犯罪者は、広範囲に及ぶボットネットを使って IoT デバイスを標的にすることが増えています。修正プログラムが適用されていない状態でルーターがインターネットに直接接続されていると、脅威アクターはそれらのルーターを悪用してネットワークへのアクセスを取得し、悪意のある攻撃を実行したり、その運用をサポートしたりすることもできます。

Microsoft Defender for IoT チームは、レガシーの産業制御システム コントローラーから、最先端の IoT センサーまで、機器に関する調査を行っています。同チームは、IoT および OT 固有のマルウェアを調査することで、侵害の兆候となる共有リストの作成に貢献しています。

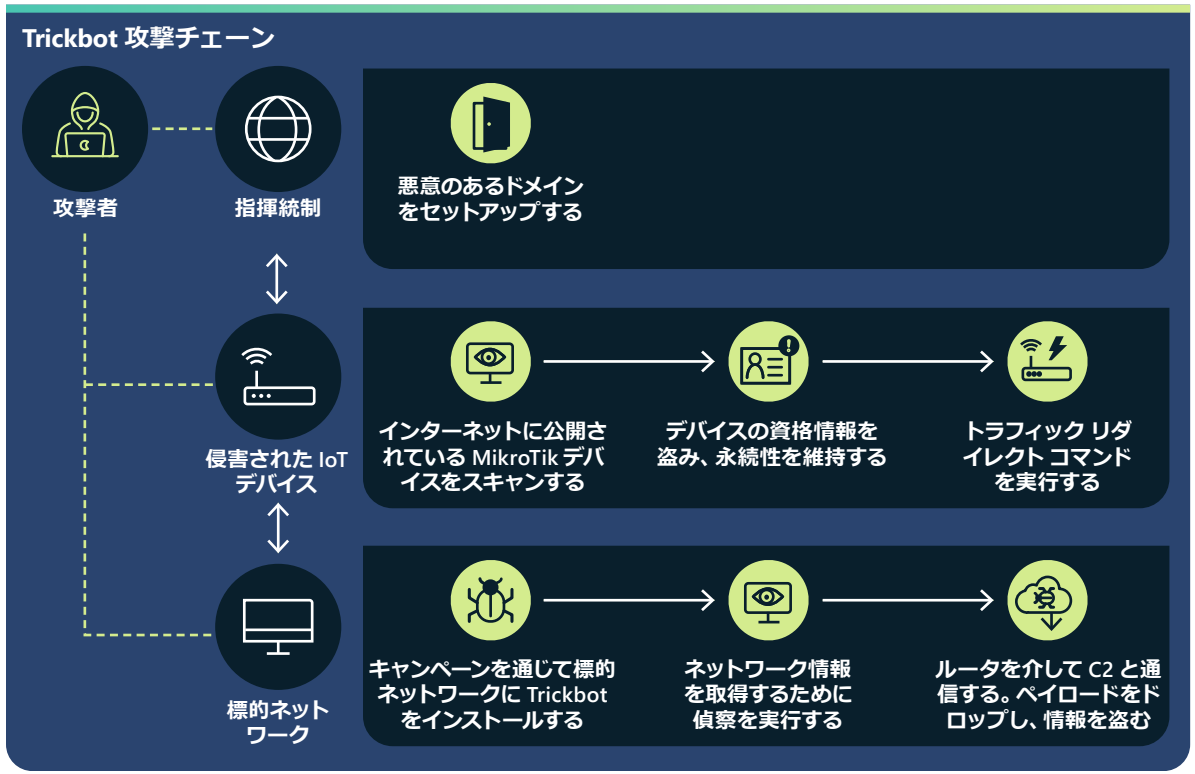
ルーターは、インターネットに接続された家庭や組織に広く普及しているため、特に脆弱な攻撃ベクトルとなります。マイクロソフトは、世界中の個人および企業でよく利用されているルーターである MikroTik ルーターのアクティビティを追跡し、指揮統制 (C2)、ドメイン ネーム システム (DNS) 攻撃、暗号マイニング ハイジャックにどのように利用されているかを調べてきました。

具体的には、Trickbot オペレーターが侵害された MikroTik ルーターをどのように利用し、C2 インフラの一部として機能するように再構成しているかを特定しました。これらのデバイスは広く利用されているため、Trickbot による悪用の重大度が上昇し、独自のハードウェアとソフトウェアによって、脅威アクターが従来のセキュリティ対策を回避して、インフラを拡大し、より多くのデバイスとネットワークを侵害することが可能になっています。



インターネットに公開されたルーターは潜在的な脆弱性を悪用されるリスクがあります。

マイクロソフトは、セキュア シェル (SSH) コマンドを含むトラフィックを追跡および分析することにより、MikroTik ルーターを利用する攻撃者が、デバイスに対する正当な資格情報を取得した後 Trickbot インフラと通信するのを観察しました。そのような資格情報は、修正プログラムをすぐに入手できる既知の脆弱性を悪用し、既定のパスワードを使うことにより、ブルート フォース攻撃を通じて入手できます。デバイスにアクセスすると、攻撃者はルーター内の 2 つのポート間のトラフィックをリダイレクトする一意のコマンドを発行し、Trickbot の影響を受けたデバイスと C2 の間に通信回線を確立します。



MikroTik IoT デバイスを C2 のプロキシ サーバーとして使っていることを示す Trickbot 攻撃チェーン。

Trickbot だけでなく、MikroTik デバイスを攻撃するさまざまな方法に加えて、既知の共通脆弱性識別子 (CVE) についての知識を、MikroTik デバイス用のオープン ソース ツールに集約しました。このツールからは、それらのデバイスへの攻撃に関連するフォレンジック アーティファクトを取り出すことができます。[31]

マルウェア C2 のリバース プロキシとして機能するデバイスは、Trickbot および MikroTik ルーターに固有のものではありません。マイクロソフトの RiskIQ チームとの共同作業では、関係する C2 をもう一度トレースし、SSL 証明書を観察することによって、同じように影響を受けた Ubiquiti および LigoWave デバイスを特定しました。[32] これは、IoT デバイスが国家レベルの組織的攻撃のアクティブなコンポーネントになっていることと、広範囲に及ぶボットネットを使ったサイバー犯罪者の標的としてよく利用されていることを示す強力な証拠です。

IoT デバイスを悪用する仮想通貨犯罪者

既知の脆弱性の数が年々増加しているため、ゲートウェイ デバイスは脅威アクターにとってますます重要な標的となっています。それらのデバイスは、暗号通貨マイニングや他の種類の悪質なアクティビティに利用されています。

仮想通貨が普及するにつれて、多くの個人や組織が、ルーターなどのデバイスからブロックチェーン上のコインをマイニングするため、コンピューティング能力とネットワーク リソースに投資してきました。しかし、仮想通貨マイニングには多くの時間とリソースが必要で、成功する可能性は低くなっています。コインをマイニングする可能性を高めるため、マイナーたちは、分散型の共同ネットワークにプールし、接続されているリソースでマイニングに成功したコインの割合に比例したハッシュを受け取っています。

この 1 年間、マイクロソフトは、ルーターを悪用して仮想通貨マイニングの試みをリダイレクトする攻撃が増加しているのを観察しました。サイバー犯罪者は、マイニング プールに接続されたルーターを侵害し、標的デバイスの DNS 設定を改変する DNS 汚染攻撃を通じて、関連する IP アドレスにマイニング トラフィックをリダイレクトします。影響を受けたルーターは、間違った IP アドレスを特定のドメイン名に登録し、マイニング リソース (つまり、ハッシュ) を脅威アクターが使用するプールに送信します。それらのプールは、犯罪行為に関連する匿名のコインをマイニングしたり、マイニングされたコインの割合を獲得するためマイナーによって生成された正当なハッシュを使用したりすることによって、報酬を得る可能性があります。

2021 年に見つかった既知の脆弱性の半数以上には修正プログラムがないため、デバイスの所有者と管理者にとって、企業およびプライベート ネットワーク上のルーターを更新してセキュリティで保護することが大きな課題となっています。

ゲートウェイ デバイスの DNS 汚染によって、合法的なマイニング アクティブが侵害され、リソースが犯罪者のマイニング アクティビティにリダイレクトされます。

犯罪インフラとしての仮想マシン

クラウドへの広範な移行に伴い、フィッシングやマルウェア資格情報盗聴ツールの配布によって得られた、何も気づいていない被害者の個人資産をサイバー犯罪者が利用するようになっています。多くのサイバー犯罪者は、自身の悪意のあるインフラを、クラウドベースの仮想マシン (VM)、コンテナ、マイクロサービスにセットアップすることを選択しています。

サイバー犯罪者がアクセス権を取得すると、スクリプトや自動化プロセスを通じて一連の仮想マシンなどのインフラをセットアップする一連のイベントを発生させることができます。そのようなスクリプト化された自動化プロセスは、大規模なメール スパム攻撃、フィッシング攻撃、悪質なコンテンツをホストする Web ページなど、悪意のあるアクティビティを開始するために使用されます。さらに、暗号通貨マイニングを実行する大規模な仮想環境がセットアップされることもあり、月末には数十万ドルもの請求書が最終的な被害者に送られることになります。

サイバー犯罪者は、悪意のあるアクティビティが検出されて停止させるまでの生存期間は限られていることを理解しています。そのため、サイバー犯罪者はスケールアップし、不測の事態を念頭に置き、先を見越して活動するようになっています。それらのサイバー犯罪者は侵害されたアカウントを事前に準備し、環境を監視することがわかりました。アカウント (数十万の仮想マシンを使ってセットアップ) が検出されると、次のアカウント (スクリプトによってすぐにアクティブ化できるように準備されている) に移動するため、悪意のあるアクティビティはほとんど中断することなく続きます。

クラウド インフラと同様、オンプレミス インフラはオンプレミス ユーザーが知らない仮想ローカル環境でも攻撃に利用できます。そのためには、最初のアクセス ポイント開いたままアクセス可能な状態に維持するする必要があります。オンプレミスの個人資産も、クラウド インフラの延長チェーンを開始し、アクセス元を難読化して不審なインフラ作成の検出を回避するため、サイバー犯罪者によって悪用されてきました。

実用的なインサイト

1. 優れたサイバー衛生を実装し、ソーシャル エンジニアリングを回避するためのガイダンスによって社員にサイバーセキュリティ トレーニングを実施します。
2. 大規模な検出を通じて通常の自動化ユーザー アクティビティ異常チェックを実施し、そのような種類の攻撃を軽減します。
3. 企業およびプライベート ネットワーク上のルーターを更新し、セキュリティで保護します。

ハクティビズムは今後も続くのか

ハクティビズムは新たな現象ではありませんが、ウクライナの戦争では、政敵、組織、さらには国家の評判や資産を傷つけるため、サイバー ツールを展開するよう政府に指示されたハッカーなど、ボランティア ハッカーの急増が見られました。

2022 年 2 月、ウクライナ政府は、30 万人の強力な「IT 軍」の一部としてロシアに対するサイバー攻撃を実施するよう世界中の民間人に呼びかけました。[33] 同時に、Anonymous、Ghostsec、Against the West、Belarusian Cyber Partisans、RaidForum2 などのハクティビスト グループを設立し、ウクライナを支援する攻撃を実施しました。(一部の Conti ランサムウェア ギャングを含む) 他のグループは、ロシアの側につきました。[34]

その後の数か月間、Anonymous の活動が非常に目立ちました。そのグループ (またはそのアフィリエイトの 1 つ) の名前を代表して行動するハッカーたちは、数千ものロシアおよびベラルーシの Web サイトを無効にして、数百ギガバイトの盗んだデータを漏えいさせ、ロシアのテレビ チャンネルをハッキングしてウクライナ寄りのコンテンツを流すだけでなく、降伏したロシアの戦車のためにビットコインを支払うことも求めました。

市民ハッカーの台頭

ソーシャル メディア プラットフォームにより、何千人もの自称市民ハッカーをすばやく組織して動員することが可能になり、DDoS 攻撃など、簡単に実行可能な攻撃を実行する指示が与えられました。まとめ役は、Twitter、電報、プライベート フォーラムを利用してハッカーを結集させ、活動を整理し、ハッキングの説明書を広めました。

しかし、それらのハッカーのほとんどは、指示があったとしてもスキルが限られている可能性があります。その結果、2 つの未来が考えられます。基本的な技術能力を持つ数百あるいは数千人の個人が攻撃テンプレートを使用し、標的に対して組織的または個人的なハクティビスト攻撃を実行する未来か、ウクライナでの戦闘が終わった後、少なくとも行動を呼び起こす次の政治的または社会的問題が起きるまでは、ハクティビズムが置き去りにされる未来です。

ハッカーの政治問題化

この政治的動員によってもたらされるより大きなリスクは、テクノロジに精通したハッカーが展開され、自ら始めるものであれ政府の命令によるものであれ、自国の優先事項を後押しするため、外国政府の標的に対するサイバー攻撃を継続的に実行するかもしれないという点です。

イラン、中国、ロシアは既に、国家のハッキング グループの人材を募集するための理由付けとしてハクティビズムを利用しています。たとえば、2022 年 4 月、ロシア寄りのハッキング グループである Killnet は、チェコが直接戦争に関与していないにもかかわらず、チェコの鉄道、地方空港、チェコの民間サービス サーバーに対する DDoS 攻撃を開始しました。[35] 同時に、一部の政府は従来のサイバー スパイ行為や妨害工作の代わりとしてハクティビズムを利用している可能性があります。例として、イスラエルに対するイランの活動などが挙げられます。

ハクティビズムに関連する DDoS 攻撃が増加しているため、テクノロジ業界には、Web サイトへの通常のトラフィック フローと異常なトラフィック フローの違いをすばやく見分けることが求められています。マイクロソフトとそのパートナーは、悪意のある DDoS トラフィックを区別し、生成元までトレースするツール コレクションを開発しました。さらに、マイクロソフトの Azure プラットフォームは、異常なレベルのアウトバウンド トラフィックを生成しているコンピューターをプラットフォームで特定し、それらをシャットダウンすることができます。

プロテストウェアの登場

プロテストウェアは、ロシアとウクライナの戦争に対する感情的な反応の直接の結果として登場しました。一部のオープン ソース ソフトウェア開発者は、次々に明らかになる地政学的な状況について発言したり行動を起こしたりする手段として、ソフトウェアの人気を利用しました。これには、デスクトップやブラウザーで開いて平和的なメッセージを広める無害なテキスト ファイルも含まれていましたが、IP アドレスの地理的位置情報に基づいた標的型攻撃や、ハード ドライブのワイプなどの破壊的なアクションも含まれていました。今後、他の出来事が世界規模で明らかになると、再びプロテストウェアが現れることが予想されます。これらの事例では一般に、尊敬されているオープン ソース管理者が自身のオープン ソース コンポーネントを使って個人的な表明を行っているにすぎないため、今のところこの種の変更がソース ファイルで発生するのを阻止する保護措置は取られておらず、ユーザーは潜在的な影響を常に認識している必要があります。

ソーシャル メディア プラットフォームにより、何千人もの自称市民ハッカーを組織して動員することが可能になり、DDoS 攻撃など、簡単に実行可能な攻撃を実行する指示が与えられました。

実用的なインサイト

1. この新しい脅威に対する包括的な対応を設計するには、テクノロジ業界が連携する必要があります。
2. マイクロソフトを含む大手テクノロジ企業は、DDoS 攻撃に関連する悪意のあるトラフィックを特定し、関係するコンピューターを無効化するためのツールを用意しています。
3. オープン ソース ユーザーは、地政学的な対立が発生したときに監視の強化を維持する必要があります。

巻末注

1. https://www.reuters.com/business/energy/shell-re-routes-oil-supplies-after-cyberattack-german-logistics-firm-2022-02-01/
2. https://www.bleepingcomputer.com/news/security/greeces-public-postal-service-offline-due-to-ransomware-attack/
3. https://www.bleepingcomputer.com/news/security/costa-rica-s-public-health-agency-hit-by-hive-ransomware/; https://www.reuters.com/world/americas/cyber-attack-costa-rica-grows-more-agencies-hit-president-says-2022-05-16/
4. https://www.bleepingcomputer.com/news/security/spicejet-airline-passengers-stranded-after-ransomware-attack/
5. https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/
6. エンドポイントで検出および対応。https://www.microsoft.com/en-us/security/business/threat-protection/
7. https://www.washingtonpost.com/national-security/cyber-command-revil-ransomware/2021/11/03/528e03e6-3517-11ec-9bc4-86107e7b0ab1_story.html
8. https://www.bbc.com/news/technology-59998925
9. 綿密に審査されたフォーラムは、新しいメンバーを追加する際に既存のメンバーの保証を必要とするオンライン ディスカッション フォーラムです。
10. https://www.statista.com/statistics/800426/worldwide-blockchain-solutions-spending/; https://www.blockchain.com/charts/my-wallet-n-users; https://coinmarketcap.com
11. https://blogs.microsoft.com/on-the-issues/2022/04/13/zloader-botnet-disrupted-malware-ukraine/
12. https://www.coindesk.com/business/2021/12/13/crypto-exchange-ascendex-hacked-losses-estimated-at-77m/ ; https://www.zdnet.com/article/after-77-million-hack-crypto-platform-ascendex-to-reimburse-customers/
13. https://etherscan.io/address/0x73326b6764187b7176ed3c00109ddc1e6264eb8b
14. https://finance.yahoo.com/news/ethereum-worth-over-1-5m-160249300.html
15. https://news.bitcoin.com/decentralized-finance-crypto-exchange-uniswap-starts-blocking-addresses-linked-to-blocked-activities/
16. データ ソース : Defender for Office (悪意のあるメール / 侵害された ID アクティビティ)、Azure Active Directory Identity Protection (侵害された ID イベント / アラート)、Defender for Cloud Apps (侵害された ID データ アクセス イベント)、M365D (製品間の相関関係)。
17. データ ソース : Defender for Endpoint (攻撃行動アラート / イベント)、Office Defender (悪意のあるメール)、M365D (製品間の相関関係)。
18. https://www.ic3.gov/Media/Y2022/PSA220504
19. ドメイン ベースのメッセージ認証、レポート作成、適合 : メール ドメイン所有者がドメインを不正利用から保護できるようにする、メール認証、ポリシー、レポート作成プロトコル。
20. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
21. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/learn-about-spoof-intelligence?view=o365-worldwide
22. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/impersonation-insight?view=o365-worldwide
23. https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview
24. https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-defender-office-365
25. https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview
26. Microsoft Corporation v. John Does 1-27, et. al., No. 1:10CV156, (E.D.Va.2010 年 2 月 22 日)。
27. 「Bowden, Mark. Worm: The First Digital World War. Grove/Atlantic, Inc., Sep 27, 2011」を参照
28. 具体的には、連邦民事訴訟法の規定 65 によると、1) 救済措置が与えられなければ当事者が直ちに回復不能な損害を被る、および 2) 当事者が時宜を得た方法で相手側に通知を行うとしている場合、当事者はそのような救済策を求めることができます。さらに、この法律では、釣り合いテスト (被告の通知する権利と、公衆に対する損害量の釣り合いを取る) を適用することが義務付けられています。
29. Microsoft Corporation v. John Does 1-11, et. al., No. 2:11cv222, (W.D. Wa. 2011 年 2 月 9 日)。
30. Microsoft Corp. v. Does, No. 1:20-cv-01171 (AJT/IDD), 2021 U.S. Dist. LEXIS 258143, at *1 (E.D.Va.2021 年 8 月 12 日)。
31. https://github.com/microsoft/routeros-scanner
32. RiskIQ: Ubiquiti Devices Compromised and Used as Malware C2 Reverse Proxies | RiskIQ Community Edition
33. https://www.theguardian.com/world/2022/mar/18/amateur-hackers-warned-against-joining-ukraines-it-army
34. https://therecord.media/russia-or-ukraine-hacking-groups-take-sides/
35. https://www.expats.cz/czech-news/article/pro-russian-hackers-target-czech-websites-in-a-series-of-attacks

国家レベルの脅威

国家レベルのアクターは、検出を回避し、戦略的な優先事項に促進するため、ますます高度なサイバー攻撃を始めています。

国家レベルの脅威の 概要

国家レベルのアクターは、検出を回避し、戦略的な優先事項に促進するため、ますます高度なサイバー攻撃を始めています。ウクライナのハイブリッド戦争におけるサイバー兵器展開の到来は、新しい対立の時代の幕開けです。

さらに、ロシアはプロパガンダを使用してロシア、ウクライナ、そして世界中の人々の意見に影響を与えることにより、情報の影響力を戦争に活かしていきました。この初めての本格的でハイブリッドな争いは、他の重要な教訓を教えてくれます。まず、デジタル オペレーションとデータのセキュリティは、サイバースペースでも物理空間でも、クラウドに移行することによって十分に保護することができます。ロシアによる初期の攻撃では、ワイパー マルウェアを使ってオンプレミス サービスが標的となり、最初に発射されたミサイルの 1 つは物理データ センターを標的としていました。

ウクライナは、ウクライナ国外のデータ センターにホストされているハイパースケール クラウドにワークロードとデータをすばやく移行することで対応しました。第 2 に、クラウド内のデータと高度な AI および ML サービスを活用したサイバー脅威インテリジェンスとエンドポイント保護の進歩により、ウクライナはロシアのサイバー攻撃から防御することができました。

他の場所では、国家レベルのアクターが活動範囲を拡大し、自動化、クラウド インフラ、リモート アクセス テクノロジの進歩を利用して、より広範な標的を攻撃しています。最終的な標的へのアクセスを可能にする企業の IT サプライ チェーンには、攻撃が頻繁に行われました。攻撃者は修正プログラムが適用されていない脆弱性をすばやく悪用して、高度な手法とブルートフォース手法の両方を使って資格情報を盗み、オープンソースや合法的なソフトウェアを使って活動をあいまいにしたため、サイバーセキュリティ管理手順がさらに重要になりました。さらに、イランは、定番の攻撃方法であるランサムウェアなどの破壊的なサイバー兵器を使用する点でロシアに加わっています。

このような動向が見られるため、人権を優先して、オンラインでの向こう見ずな行動から人々を保護する一貫したグローバル フレームワークを早急に採用する必要があります。すべての国が、責任ある国家の行動に関する決められた規範とルールを実装するよう尽力する必要があります。

ウクライナ防衛：サイバー戦争から得られた初期の教訓 ― Microsoft On the Issues

特に IT 業界、金融サービス、交通システム、通信インフラなど、重要インフラが標的となることが増えました。

詳しくは 35 ページをご覧ください

IT サプライ チェーンは、標的にアクセスするためのゲートウェイとして使用されています。

NOBELIUM

詳しくは 36 ページをご覧ください

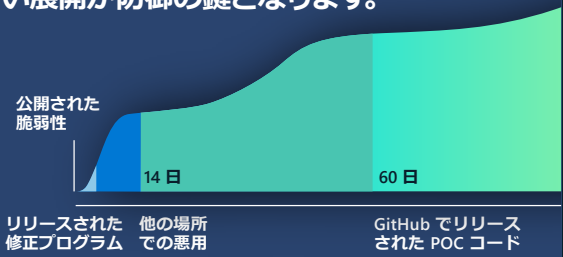
中国は、東南アジアの特に小規模な国においてグローバルな標的を拡大し、インテリジェンスと競争優位性を獲得しています。

詳しくは 44 ページをご覧ください

イランは、権力移行後に攻撃性をますます強めて、ランサムウェア攻撃を地域の敵対国だけでなく米国と EU の標的に拡大し、米国の重要インフラを標的にしました。

詳しくは 46 ページをご覧ください

修正プログラムが適用されていない脆弱性の特定とすばやい悪用が主な戦略となりました。セキュリティ更新プログラムのすばやい展開が防御の鍵となります。



詳しくは 39 ページをご覧ください

北朝鮮は、防衛を構築して、経済を強化し、国内の安定を確保するという政府の目標を達成するため、防衛および航空宇宙企業、仮想通貨、報道機関、脱北者、援助組織を標的としました。

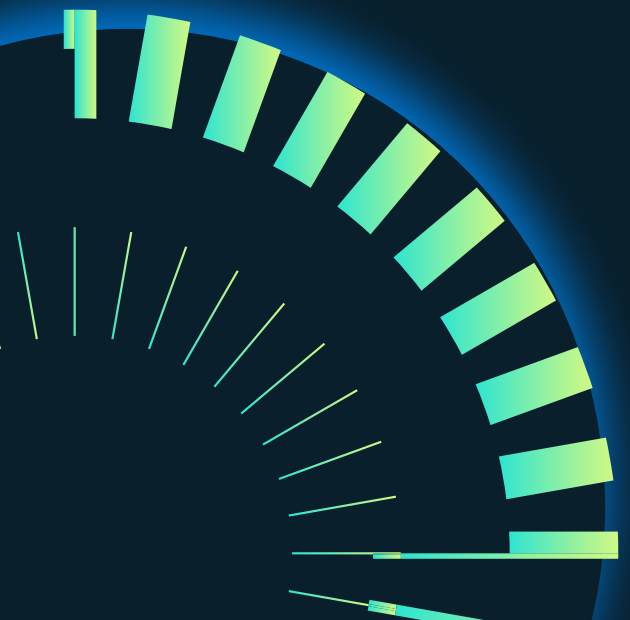
詳しくは 49 ページをご覧ください

民間企業からなるサイバー傭兵業界は成長を続けており、クライアント（多くの場合は政府）がネットワークやデバイスに侵入するための高度なツール、手法、サービスを開発および販売しているため、サイバースペースの安定性を脅かしています。

詳しくは 52 ページをご覧ください

イントロダクション

2020 年と 2021 年に攻撃が注目を浴びた後、国家レベルの脅威アクターは、高度な脅威から防御するため各組織が実装した新しいセキュリティ保護に対応し、大きなリソースを費やしました。



多くの企業組織と同様、攻撃者たちは、自動化、クラウド インフラ、リモート アクセス テクノロジの進歩を利用して攻撃をより広範な標的に拡張し始めました。このような戦術調整により、企業のサプライ チェーンに対する新しいアプローチと大規模な攻撃が生じました。アクターが、修正プログラムが適用されていない脆弱性をすばやく悪用するための新たな方法を生み出して、企業ネットワークを侵害するための手法を拡大し、オープンソースまたは合法的なソフトウェアを使って活動を難読化したことにより、IT セキュリティ衛生の重要性はさらに高まりました。新しい攻撃手法により、標的のネットワークにアクセスするための検出がより困難な新しいベクトルが生まれました。さらに、戦争中の物理な攻撃がエスカレートするにつれて、軍事活動においてサイバー攻撃が重要な役割を果たすようになりました。

ウクライナにおける紛争は、サイバー攻撃が進化し、地上における武力紛争と並行して世界にどのような影響を与えるかについて、痛烈すぎる例を教えてくれました。電力システム、通信システム、メディア、その他の重要インフラはいずれも、物理的な攻撃とサイバー攻撃両方の標的となりました。スパイ活動と情報流出キャンペーンの一環としてよく見られるネットワーク侵害の試みは、重要なインフラ システムに対する破壊型ワイパー マルウェア攻撃に対するハイブリッド戦争に重点を置いていました。それらのシステムのセキュリティをクラウドに接続することにより、起きるかもしれない壊滅的な攻撃を早期に検出し、阻止することができました。[1]

大規模なサイバー問題としては初めて、機械学習を利用した行動検知で既知の攻撃パターンを使用し、基盤となるマルウェアに関する事前の知識がなくても (人間が脅威を認識する前であっても) さらなる攻撃を特定し、阻止することができました。さらに、マイクロソフトは、そのようなシステムを保護する防御者との間で脅威インテリジェンスをリアルタイムで共有し、アクティブな攻撃を予測して防御するための重要情報を得ることの価値も確認しました。

世界中にいる国家レベルの脅威アクターは、新たな方法で活動を拡大し続けています。中国、北朝鮮、イラン、ロシアはすべて、マイクロソフトのお客様に対して攻撃を行っています。アクターが複数の組織へのアクセス ポイントとなる上流サービスに重点を移したため、IT サービスのサプライ チェーンが標的となることが多くなりました。アクターは、企業のサプライ チェーンにおける信頼関係を引き続き悪用すると予想されます。そのため、認証ルールの全面的な適用、修正プログラムのこまめな適用、リモート アクセス インフラのアカウント構成、パートナー関係の頻繁な監査により信頼性を検証することの重要性が高まっています。

ランサムウェアや犯罪者など同じように、国家レベルのアクターは、構成が不適切であるか修正プログラムが適用されていないエンタープライズ システム (VPN/VPS インフラ、オンプレミス サーバー、サードパーティ ソフトウェア) を標的にする方針に転換し、環境寄生型攻撃を行うことにより、発覚の増加に対応しています。多くは、悪意のあるアクティビティを難読化するため、コモディティ マルウェアとオープン ソース レッド チーム ツールの使用を拡大しています。

その結果、重点的な修正プログラム適用、改ざん防止機能の有効化、RiskIQ などの攻撃対象領域管理ツールによる攻撃対象領域の客観的な確認を通じて IT セキュリティ衛生の強固なベースラインを維持し、企業全体で多要素認証を有効にすることが、多くの行動なアクターからプロアクティブに防御するための基盤となっています。

国家レベルのアクターは、攻撃の戦術としてランサムウェアの使用も増やしており、犯罪者エコシステムによって作成されたランサムウェア マルウェアを攻撃に再利用することがよくあります。イランと北朝鮮のアクターはどちらも、コモディティ ランサムウェア ツールを利用して標的システムに損害を与えてきました。多くの場合は、近隣の対立国にある重要インフラが含まれます。最後の点として、脆弱性の高いサードパーティ ソリューションの悪用を拡大するためのツール、手法、サービスを開発して販売するサイバー傭兵の脅威が高まっています。国家レベルのアクターによる攻撃の高度化と俊敏性は、年々進化し続けています。組織は、そのようなアクターの変化についての情報を入手すると同時に、防御を進化させる必要があります。

John Lambert
コーポレート バイス プレジデント兼ディスティングイッシュド エンジニア、Microsoft Threat Intelligence Center

国家データの背景

国家レベルの脅威とは、自国の国益を追及するという明白な意図を持って特定の国から発生するサイバー脅威活動です。国家レベルのアクターは、知的財産の盗難、スパイ活動、監視、資格情報の盗難、破壊的な攻撃など、マイクロソフトのお客様が直面しているものの中で最も高度かつ執拗な脅威となっています。

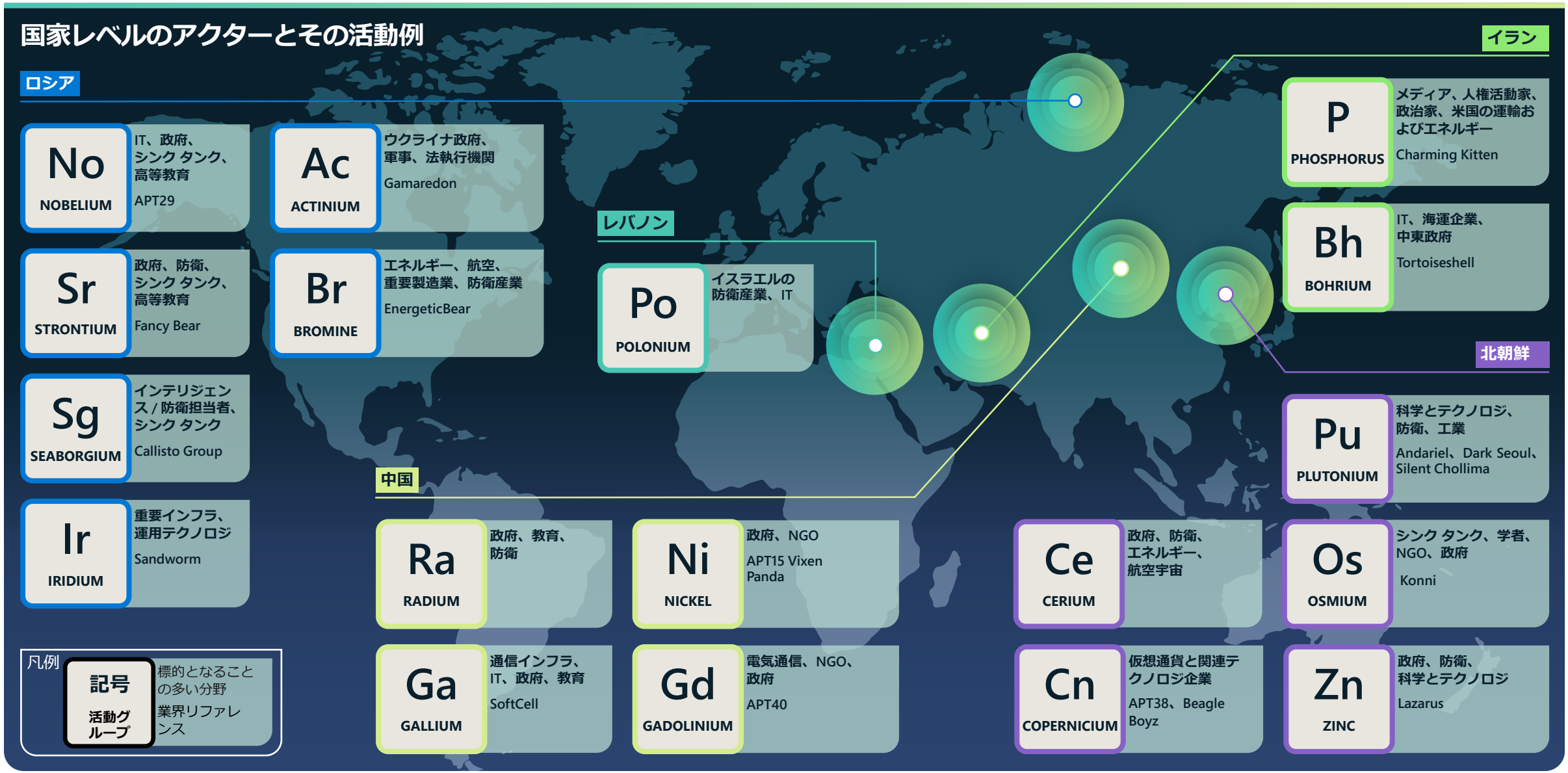
マイクロソフトは、このような脅威を発見して、理解し、対抗するため、重要なリソースに投資しています。組織または個人のアカウント所有者が、実際の国レベルの活動の標的となるか侵害された場合、活動の調査に必要な情報を含む、Nation State Notification (NSN) の形で直接お客様にアラートを送信します。2018 年に開始して以来、2022 年 6 月までに 67,000 件を超える NSN を送信してきました。

この章では、マイクロソフトの NSN アラート データについて説明し、測定可能な活動のビューを提供します。図に示されている国レベルの活動のレベルは、お客様の組織の少なくとも 1 つのアカウントを標的または侵害している国レベルのアクターが検出された場合にマイクロソフトがお客様に発行した NSN の数に基づいています。

このレポートに含まれている脅威グループが存在する 4 つの主要な国は、ロシア、中国、イラン、北朝鮮です。これは、過去 1 年間にマイクロソフトのお客様を標的としたアクターが最も多く見られる国を表しています。このレポートには、レバノンやサイバー傭兵の脅威グループ、請け負いの民間企業の攻撃アクターに関する観察も含まれています。

マイクロソフトは、次のページにいくつか例が示されているように、化学元素名 (NOBELIUM など) によって国家グループを識別しています。DEV-#### 表記は、脅威活動の未知のクラスター、新規クラスター、発展中のクラスターに与えられる一時的な名前として使用しています。これにより、活動の背後にいるアクターの出所や身元について信頼性の高い情報が見つかるまで、一意の情報セットとして追跡することができます。

条件を満たすと、DEV は名前のあるアクターに切り替えられるか、既存のアクターと結合されます。この章では、攻撃の標的、手法、動機の分析をより細かく理解するため、国レベルのグループと DEV グループの例を挙げています。それらのグループの多くは、サイバー犯罪者と同じツールを使っていますが、オーダーメイドのマルウェア、ゼロデイ脆弱性を検出して利用する能力、法的な処罰を受けない、といった形で独特な脅威となっています。


国家レベルのアクターとその活動例
ロシア
No
NOBELIUM
IT、政府、シンク タンク、高等教育
APT29
Ac
ACTINIUM
ウクライナ政府、軍事、法執行機関
Gamaredon
Sr
STRONTIUM
政府、防衛、シンク タンク、高等教育
Fancy Bear
Br
BROMINE
エネルギー、航空、重要製造業、防衛産業
EnergeticBear
Sg
SEABORGIUM
インテリジェンス / 防衛担当者、シンク タンク
Callisto Group
Ir
IRIDIUM
重要インフラ、運用テクノロジ
Sandworm
レバノン
Po
POLONIUM
イスラエルの防衛産業、IT
イラン
P
PHOSPHORUS
メディア、人権活動家、政治家、米国の運輸およびエネルギー
Charming Kitten
Bh
BOHRIUM
IT、海運企業、中東政府
Tortoiseshell
北朝鮮
Pu
PLUTONIUM
科学とテクノロジ、防衛、工業
Andariel、Dark Seoul、Silent Chollima
中国
Ra
RADIUM
政府、教育、防衛
Ni
NICKEL
政府、NGO
APT15 Vixen Panda
Ce
CERIUM
政府、防衛、エネルギー、航空宇宙
Os
OSMIUM
シンク タンク、学者、NGO、政府
Konni
Ga
GALLIUM
通信インフラ、IT、政府、教育
SoftCell
Gd
GADOLINIUM
電気通信、NGO、政府
APT40
Cn
COPERNICIUM
仮想通貨と関連テクノロジ企業
APT38、Beagle Boyz
Zn
ZINC
政府、防衛、科学とテクノロジ
Lazarus
凡例
記号
活動グループ
標的となることの多い分野
業界リファレンス

進化する脅威の状況

国家レベルのアクターの活動を追跡し、お客様が標的にされたり侵害されたりした場合はお知らせするというマイクロソフトの使命は、お客様を攻撃から保護するという使命に根ざしています。

この通知は、観察された攻撃がマイクロソフトのセキュリティ製品保護によって適切に阻止されたかどうかや、未知のセキュリティの弱点があるため攻撃が有効であるかどうかをお客様に知らせる取り組みにおける重要な要素です。時間の経過に伴って通知を追跡することにより、マイクロソフトはアクターによる脅威の傾向の変化を見分け、製品保護の重点を、クラウド サービス全体でお客様に対する脅威をプロアクティブに軽減することに置くことができます。

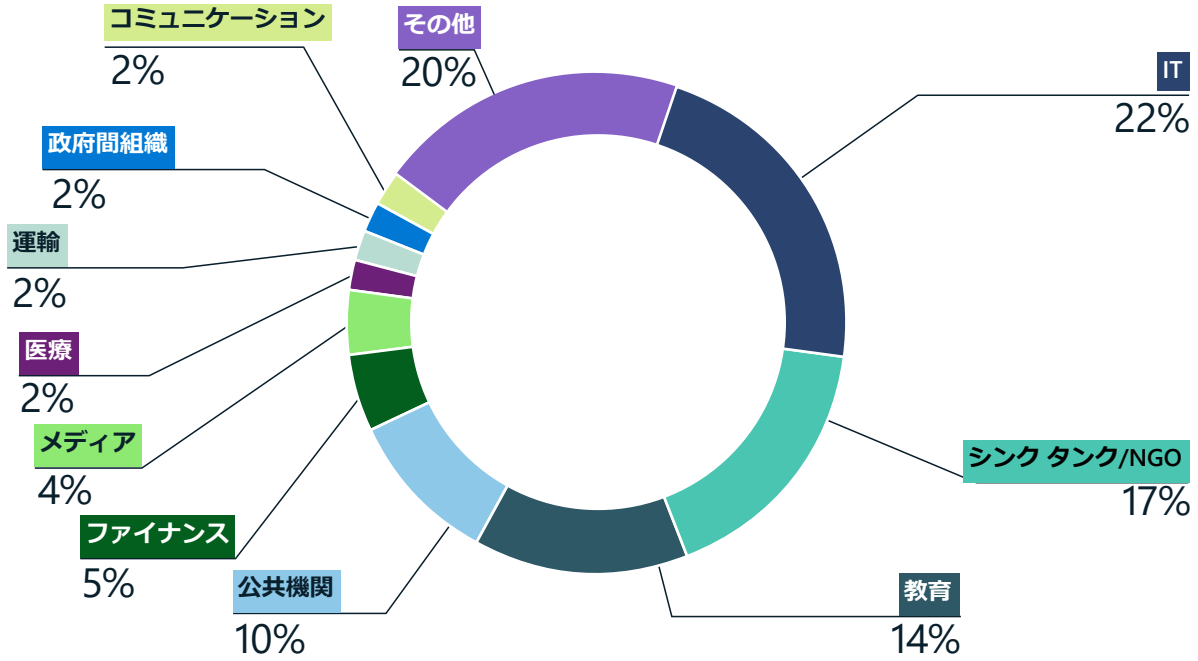
この追跡によって、観察された内容に関するデータとインサイトを共有することもできます。それらのアクターを追跡して攻撃を尾行するアナリストは、技術的な指標と地政学的な専門知識の両方を使ってアクターの動機を理解し、技術面でのコンテキストとグローバルなコンテキストを新しいインサイトにまとめる必要があります。このキュレーションにより、国家レベルのサイバー アクターにとっての優先事項と、それらのアクターを採用している国家の政治的、軍事的、経済的優先順位がアクターの動機にどのように反映されているかについて、独自の見解が得られます。

過去 1 年間の政治的な変化により、世界中の国家が支援する脅威グループにとっての優先順位とリスクの許容範囲が方向づけられました。地政学的な関係が崩れ、いくつかの国ではタカ派的な考え方がより支配力を強めているため、サイバー アクターはより大胆かつ攻撃的になっています。次に例を示します。

- ロシアは、地上での軍事行動を補完するため、ウクライナ政府と同国の重要インフラを執拗に攻撃しました。[2]
- イランは、港湾局など、米国の重要インフラへの進出を積極的に模索していました。
- 北朝鮮は、金融およびテクノロジ企業から暗号通貨を盗むというキャンペーンを継続しました。
- 中国は、グローバルなサイバー スパイ行為活動を拡大しました。

国家レベルのアクターは技術的に洗練されていて、幅広い戦術を採用できますが、多くの場合、その攻撃は優れたサイバー衛生によって軽減できます。これらのアクターの多くは、スピア フィッシング メールなどの比較的ローテクな手段に依存しており、カスタマイズされたエクスプロイトの開発や、標的型ソーシャル エンジニアリングを使って目的を達成することに投資する代わりに、高度なマルウェアを提供しています。

国家レベルのアクターの標的となる業界分野



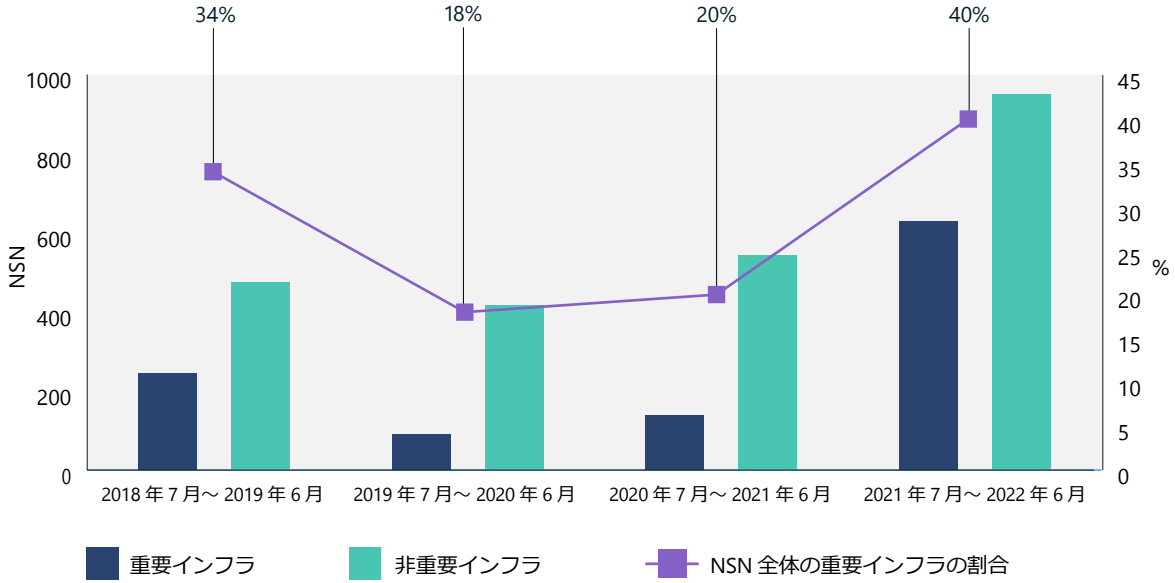
国家レベルのグループは、さまざまな分野を標的としてきました。ロシアとイランのアクターは、IT 業界を IT 企業の顧客にアクセスする手段として標的にしました。シンク タンク、非政府組織 (NGO)、大学、行政機関も、国家レベルのアクターの標的となることが多くありました。

国家レベルのアクターが組織や個人の特定のグループを標的にする目的はさまざまです。昨年、特に IT 企業を狙ったサプライ チェーン攻撃が増加しました。IT サービス プロバイダーを侵害することにより、脅威アクターは、多くの場合接続されたシステムを管理する会社との信頼関係を通じて元の標的に到達できるようになります。1 回の攻撃でその先にいる数百件の顧客を侵害することにより、大規模な攻撃を実行できる可能性もあります。IT 業界の後、最も頻繁に標的とされたのは、シンク タンク、大学に所属する学者、政府職員でした。これらは、地政学的な問題に関するインテリジェンスを収集するためのスパイ活動にとって理想的な「ソフト ターゲット」です。

進化する脅威の状況

(続き)

重要インフラの傾向

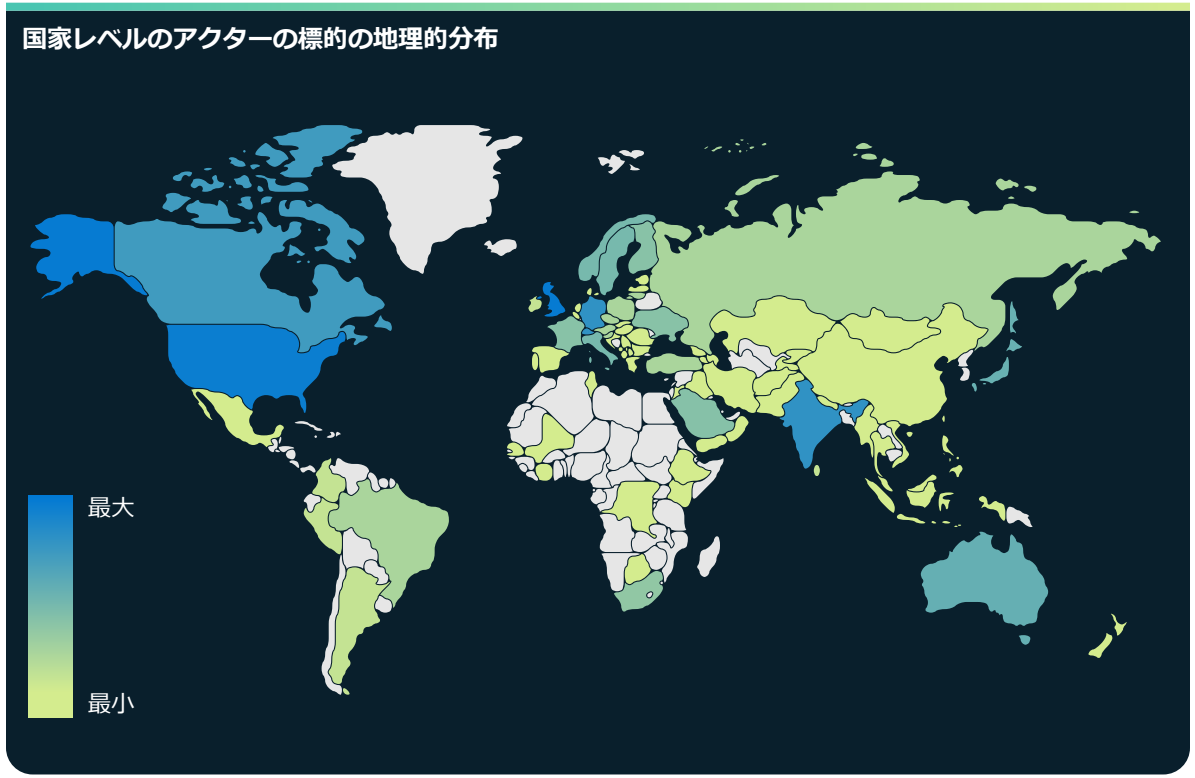


国家レベルのグループが標的とする重要インフラ[3] は過去 1 年間に増加しましたが、アクターたちは IT 業界、金融サービス、交通システム、通信インフラの企業に重点を置いていました。

「ウクライナ侵攻の前、各国政府はデータのセキュリティを確保するには国内にとどめる必要があると考えていました。侵入後、データをクラウドに移行して国外に移動することは、回復性の計画と優れたガバナンスの一部となりました。」

Cristin Flynn Goodwin、
アソシエイト法律顧問、カスタマー セキュリティ & トラスト担当

国家レベルのアクターの標的の地理的分布



国家レベルのグループによるサイバー攻撃の標的は、この 1 年間世界中に広がり、特に米国と英国の企業に集中しています。NSN のデータによると、イスラエル、UAE、カナダ、ドイツ、インド、スイス、日本の組織も頻繁に標的となっています。

実用的なインサイト

1. 価値が高いと見なされる可能性があるデータ ターゲット、リスクの高いテクノロジ、情報、およびビジネス オペレーションは国家レベルのグループの戦略的優先事項に合致する可能性があるため、それらを特定し、保護します。
2. クラウド保護を有効にし、ネットワークに対する既知の脅威と新しい脅威を大規模に識別し、軽減します。

デジタル エコシステムへのゲートウェイとしての IT サプライ チェーン

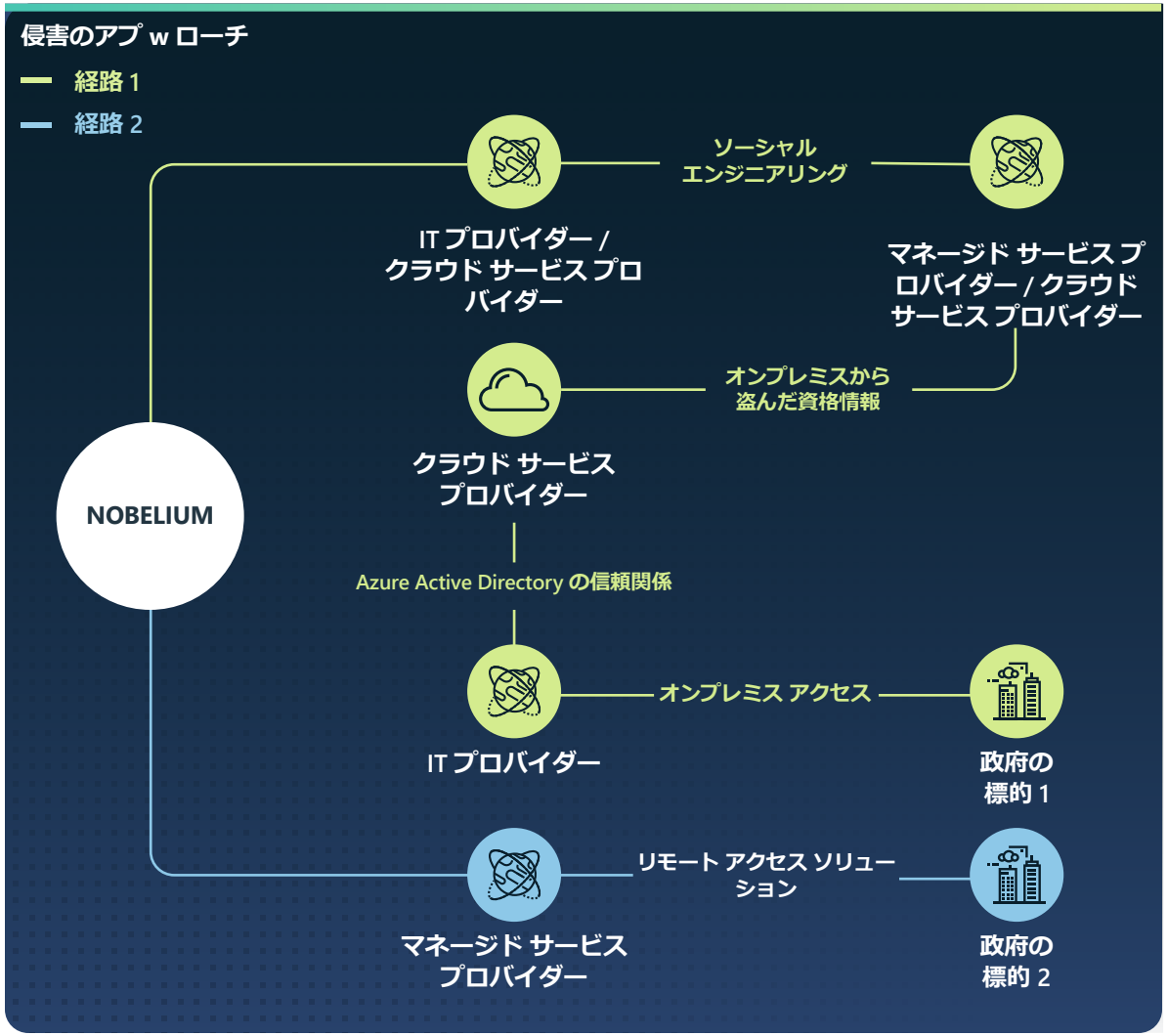
国家が IT サービス プロバイダーを標的にしているため、脅威アクターは、それらのサプライ チェーン プロバイダーに与えられた信頼とアクセス権を利用することで関心のある他の組織を悪用できる可能性があります。過去 1 年間、国家レベルのサイバー脅威グループが IT サービス プロバイダーを標的として、第三者の標的を攻撃し、政府、政策、重要インフラ分野のダウンストリーム クライアントにアクセスしました。

IT サービス プロバイダーは、国外のインテリジェンス サービスにとって興味深い数百もの直接クライアントあるいは数千もの間接クライアントにサービスを提供しているため、魅力的な中間標的となっています。それらの企業が持っている日常的なビジネス プラクティスと委任管理特権が悪用された場合、悪意のあるアクターは、アラートがトリガーされるまでの時間を稼ぎながら、IT サービス プロバイダーのクライアント ネットワークにアクセスして操作できるようになる可能性があります。

過去 1 年間、NOBELIUM はクラウド ソリューションやその他のマネージド サービス プロバイダーが持つ特権アカウントを侵害し、それを利用して、主に米国とヨーロッパの政府および政策顧客への標的型ダウンストリーム アクセスを試みました。

NOBELIUM は、「1 つの標的の侵害を多数の標的の侵害につなげる」アプローチを、認知された地政学的な敵対反対勢力に対してどのように適用できるかを実証しました。過去 1 年間、脅威アクターは、ロシア政府が実存的な脅威と認識している北大西洋条約機構 (NATO) の加盟国に基づいて、機密性の高い組織に第三者経由の侵入と直接侵入の両方を実施しました。2021 年 7 月から 2022 年 6 月上旬までの間、オンライン サービスのお客様に対するロシアの脅威活動に関するマイクロソフトのお客様への通知の 48% は、NATO 加盟国に拠点を置く IT 業界企業に送信されました。おそらく中間アクセス ポイントとして利用されたと思われます。全体として、同期間中のロシアの脅威活動に関する通知の 90% は、IT、シンク タンクと非政府組織 (NGO)、政府部門を中心とした、NATO 加盟国に拠点を置くお客様に送信されました。これは、標的への初期アクセスとして複数の手段を利用する戦略であることを示唆しています。

ソフトウェア サプライ チェーンの悪用から、クラウド ソリューションとマネージド サービス プロバイダーを標的としてダウンストリームの顧客にアクセスする IT サービス サプライ チェーンの悪用へと変化しました。



この図は、最終的な標的を侵害し、途中で他の被害者を巻き添えにする、NOBELIUM の複数ベクトル アプローチを示しています。上記の行為に加えて、NOBELIUM は関係するエンティティに対してパスワード スプレーおよびフィッシング攻撃を開始しました。考えられるもう 1 つの侵害ルートとして、少なくとも 1 人の政府職員の個人アカウントが標的となった可能性もあります。

デジタル エコシステムへのゲートウェイとしての IT サプライ チェーン

(続き)

Microsoft Threat Intelligence Center (MSTIC) は、年間を通じて、イランの国家レベルのアクターとイラン関連アクターが IT 企業を侵害した件数が増加していることを検出しました。多くの場合、アクターはサインイン資格情報を盗み、インテリジェンス収集から報復としての破壊的攻撃まで、幅広い目的のためにダウンストリーム クライアントにアクセスしていることが検出されました。

- 2021 年 7 月と 8 月、DEV-0228 はイスラエルのビジネス ソフトウェア プロバイダーを侵害した後、イスラエルの防衛、エネルギー、法律業界のダウンストリーム顧客を侵害しました。[4]
- マイクロソフトは、2021 年 8 月から 9 月にかけて、インドに拠点を置く IT 企業を標的にしたイランの国家レベルのアクターが急増したのを検出しました。このような変化の要因となる差し迫った地政学上の問題がなかったため、インド国外の子会社やクライアントへの間接アクセスを目的として標的にされたことを示唆しています。
- 2022 年 1 月、マイクロソフトの調査によるとイラン政府と協力関係にあるグループの DEV-0198 は、イスラエルのクラウド ソリューション プロバイダーを侵害しました。マイクロソフトは、プロバイダーを侵害して獲得した資格情報を使用し、イスラエルのロジスティクス企業で認証を行った可能性が高いと考えています。MSTIC は、その月の後半、同じアクターがそのロジスティクス企業に対して破壊的なサイバー攻撃を行おうとしているのを観察しました。
- 2022 年 4 月、マイクロソフトの調査によると IT サプライ チェーン技術に関してイランの国家レベルのグループと協力関係にある、レバノンに拠点を置くグループである POLONIUM は、イスラエルの別の IT 企業を侵害し、イスラエルの国防および法務組織にアクセスしました。[5]

過去 1 年間の活動は、NOBELIUM や DEV-0228 などの脅威アクターが、それらの組織自体よりも良い信頼関係の状況を把握していることを示しています。このような脅威が増加したことは、組織が自身のデジタル資産の境界とエントリ ポイントを把握し、強化する必要性を強調しています。さらに、IT サービス プロバイダーが自社のサイバーセキュリティの健全性を厳格に監視することの重要性も強調しています。たとえば、組織は多要素認証と条件付きアクセス ポリシーを実装して、悪意のあるアクターが特権アカウントを取得したり、ネットワーク全体に広がったりしにくくする必要があります。パートナー関係の徹底的な見直しと監査を実施すると、組織とアップストリーム プロバイダー間の不必要なアクセス許可を最小限に抑え、あまりよくわかっていない関係に対するアクセス権をすぐに削除することができます。これまでよりもアクティビティ ログを把握し、利用可能なアクティビティを確認することで、詳しい調査を行うきっかけとなる異常を発見しやすくなります。

> 国家は、第三者を標的とし、サプライ チェーン内の信頼とアクセスを利用することにより、機密性の高い組織を悪用できるようになります。

実用的なインサイト

1. アップストリームおよびダウンストリームのサービス プロバイダーとの関係と委任特権アクセスを見直しおよび監査し、不必要なアクセス許可を最小限に抑えます。あまりよくわかっていないパートナー関係やまだ監査されていないパートナー関係があれば、そのアクセス権を削除します。[6]
2. 単一要素認証で構成されたアカウントに重点を置いて、リモート アクセス インフラと仮想プライベート ネットワーク (VPN) のあらゆる認証アクティビティのログ記録を有効にしてレビューし、真正性を確認して異常なアクティビティを調査します。
3. すべてのアカウント (サービス アカウントを含む) で MFA を有効にし、すべてのリモート接続に MFA を適用します。
4. パスワードレス ソリューションを使ってアカウントを保護します。[7]

詳しい情報のリンク

- NOBELIUM はより広範な攻撃を可能にするため委任管理者特権を標的としている | Microsoft Threat Intelligence Center (MSTIC)
- イランによる IT 部門の標的が増加 | Microsoft Threat Intelligence Center (MSTIC)、Microsoft Digital Security Unit
- イスラエルの組織を標的とした POLONIUM アクティビティとインフラの公開 | Microsoft Threat Intelligence Center (MSTIC)

すばやい脆弱性の悪用

組織がサイバーセキュリティ対策を強化するにつれて、国家レベルのアクターは、攻撃を実行して検出を回避するための新しい独自の戦術を探すことで対応しています。これまで未知であった脆弱性 (ゼロデイ脆弱性と呼ばれます) の特定と悪用は、この取り組みにおける重要な戦術の 1 つ です。

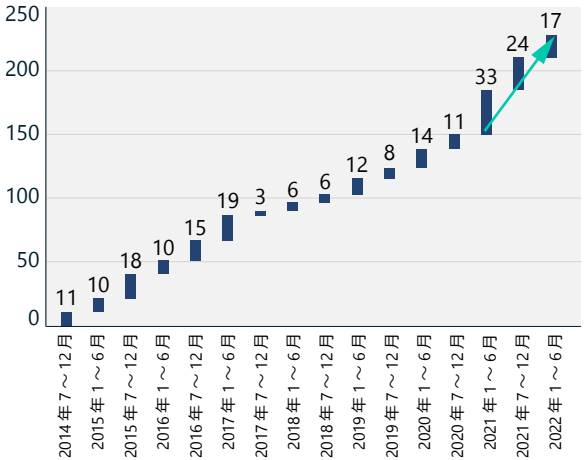
ゼロデイ脆弱性は、初期の悪用のために特に効果的な手段であり、いったん明らかになると、他の国家レベルのアクターや犯罪者によってすぐに脆弱性が再利用される可能性があります。過去 1 年間に公開されたゼロデイ脆弱性の数は、前年と同程度であり、史上最高レベルでした。

サイバー脅威アクター (国家レベルと犯罪者の両方) がそれらの脆弱性を利用する点でより巧みになるにつれて、脆弱性の発表からその脆弱性のコモディティ化までにかかる時間が短くなっていることがわかってきました。したがって、組織がすぐにエクスプロイトに修正プログラムを適用することが不可欠になります。同様に、新しい脆弱性を発見した組織や個人は責任を持って、調整された脆弱性開示の手順に沿って、影響を受けるベンダーにできる限り速やかに開示または報告することが重要です。

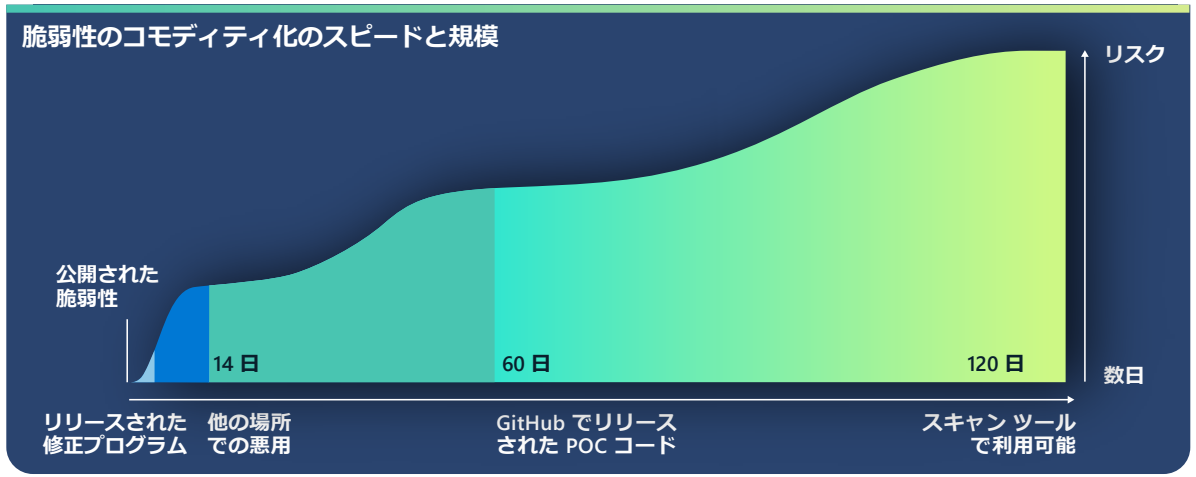
これにより、脆弱性を特定した後、タイムリーな方法で修正プログラムを開発して、それまで未知であった脅威からお客様を保護できるようになります。

多くの組織は、脆弱性管理がネットワーク セキュリティの肝要な部分となっていれば、ゼロデイ攻撃の被害を受ける可能性は低いと考えています。しかし、エクスプロイトのコモディティ化は、はるかに速いスピードで対処する必要があることを意味しています。ゼロデイ攻撃は多くの場合、他のアクターによって発見され、短期間で広く再利用されるため、修正プログラムが適用されていないシステムが危険にさらされます。ゼロデイ攻撃は検出が困難な場合がありますが、アクターの悪用後のアクションは多くの場合検出しやすく、修正プログラムがすべて適用されたソフトウェアからアクションが実行された場合は侵害の兆候を示す警告として機能します。

ゼロデイ脆弱性用にリリースされた修正プログラム



Common Vulnerabilities and Disclosures (CVE) のリストから公開されたゼロデイ攻撃の数。



脆弱性が公開された後、エクスプロイトが他の場所で利用できるようになるまで平均 14 日しかかかりません。このビューは、ゼロデイ脆弱性の悪用のタイムラインを分析したものであり、特定のエクスプロイトに対して脆弱かつインターネット上でアクティブになっているシステムの数について、最初の公開時点からの推移を示しています。

ゼロデイ脆弱性攻撃は、最初は限られた組織を標的にする傾向がありますが、すぐにより大きな脅威アクター エコシステムに採用されています。そのため、脅威アクターは、潜在的な標的が修正プログラムをインストールする前にできるだけ広い範囲でこの脆弱性を悪用すべく競争を始めます。

多くの国家レベルのアクターが未知の脆弱性からエクスプロイトを開発していることが観察されていますが、中国の国家レベルの脅威アクターは、ゼロデイ攻撃の発見と開発に特に習熟しています。中国の脆弱性報告規制は 2021 年 9 月に発効しましたが、脆弱性を製品またはサービスの所有者に知らせる前に、確認のため政府当局に脆弱性を報告することが世界で最初に義務付けられました。この新しい規制により、中国政府の分子が、報告された脆弱性情報を武器化するために備蓄できるようになる可能性があります。中国ベースのアクターがゼロデイを利用した件数が昨年増加したことは、中国のセキュリティ コミュニティで中国の脆弱性開示要件が発効した最初の 1 年間を反映したものであり、ゼロデイ攻撃を国家の優先事項として使用する大きな一歩を示していると考えられます。以下に記載されている脆弱性は、中国ベースの国家レベルのアクターが攻撃のためにまず開発および展開した後、より広範な脅威エコシステムの他のアクターに発見され、普及していきました。

すばやい脆弱性の悪用

(続き)

国家レベルの攻撃の標的となっていない組織でも、広範なアクター エコシステムによって悪用される前の限られた期間のうちに、影響を受けるシステムのゼロデイ脆弱性に修正プログラムを適用する必要があります。

新たに特定されたこれらの脆弱性の例は、脆弱性に修正プログラムを適用してから概念実証 (POC) コードがオンラインで利用可能になるまで平均 60 日かかることを示しています。また、多くの場合、他のアクターによって再利用されます。同様に、Metasploit などの自動化脆弱性スキャンおよびエクスプロイト ツールで脆弱性が利用できるようになるまで平均 120 日かかります。そのため、多くの場合、エクスプロイトが大規模に利用されることになります。これは、国家レベルの脅威アクターの標的となっていない組織でも、脆弱性が広範なアクター エコシステムによって悪用される前に、影響を受けるシステムのゼロデイ脆弱性に修正プログラムを適用する期間が限られていることを示しています。

CVE-2021-35211 SolarWinds Serv-U

2021 年 7 月、SolarWinds はマイクロソフトに言及しながら CVE -2021-35211 のセキュリティ アドバイザリをリリースししました。[8] そのとき、マイクロソフトは、国家と協力している脅威アクター DEV-0322 が SolarWinds Serv-U の脆弱性を積極的に悪用しているのを発見しました。マイクロソフトの RiskIQ チームは、6 月 15 日から 7 月 9 日までの間に、影響を受けたデバイスのインターネット接続バージョンをホストしている IP アドレスを 12,646 件観察しました。

CVE-2021-40539 Zoho ManageEngine ADSelfService Plus

2021 年 9 月、マイクロソフトの研究者は、中国関連のアクターが米国を拠点とする複数の企業で Zoho ManageEngine を悪用しているのを観察しました。この脆弱性は、9 月 6 日に CVE-2021-40539 Zoho ManageEngine ADSelfService Plus として公開されました。これは通常、組織がパスワードのリセットを処理するために使用しています。[9] DEV-0322 は 9 月後半にこの脆弱性を悪用し、ネットワークの足場を獲得する初期ベクトルとして使って、資格情報のダンプ、カスタム バイナリのインストール、永続性を維持するマルウェアのドロップなど、追加のアクションを実行しました。RiskIQ は、公開時点でこれらのシステムのインスタンスのうち 4,011 件がアクティブであり、インターネットに接続されているのを観察しました。

CVE-2021-44077 Zoho ManageEngine ServiceDesk Plus

2021 年 10 月下旬には、DEV-0322 が 2 つ目の Zoho ManageEngine 製品 ServiceDesk Plus (資産管理機能付き IT ヘルプ デスク ソフトウェア) に含まれる脆弱性 (CVE-2021-44077) を利用しているのを観察しました。DEV-0322 は、この脆弱性を利用して、医療、IT、高等教育、重要な製造業界の企業を標的にし、侵害しました。12 月 2 日、米国連邦捜査局 (FBI) と Cybersecurity and Infrastructure Security Agency (CISA) は、この脆弱性を利用している国家レベルの脅威アクターについて、共同アドバイザリの警告を発行しました。RiskIQ は、公開時点でこれらのシステムのインスタンスのうち 7,956 件がアクティブであり、インターネットに接続されているのを観察しました。

CVE-2021-42321 Microsoft Exchange

Exchange の脆弱性 CVE-2021-42321 に対するゼロデイ攻撃は、中国の成都で 2021 年 10 月 16 日と 17 日に開催された国際サイバーセキュリティ サミットおよびハッキング コンテスト Tianfu Cup で明らかになりました。マイクロソフトのセキュリティ研究者は、10 月 21 日 Exchange の脆弱性が他の場所で悪用されているのを観察しました。この脆弱性が明らかになってからわずか 3 日後のことです。RiskIQ は、公開時点でこれらのシステムのインスタンスのうち 61,559 件がアクティブであり、インターネットに接続されているのを観察しました。悪用アクティビティは、2021 年 11 月まで継続的に観察されました。

CVE-2022-26134 Confluence

中国関連のアクターは、6 月 2 日に脆弱性が公開される 4 日前、Confluence の脆弱性 (CVE-2022-26134) のゼロデイ攻撃コードを入手したと考えられるため、米国を拠点とするエンティティに利用したと考えられます。RiskIQ は、公開時点で脆弱性のある Confluence システムのインスタンスのうち 53,621 件がインターネット上でアクティブであることを観察しました。

脆弱性は、ますます短い期間で大規模に目を付けられ、悪用されています。

実用的なインサイト

1. ゼロデイ脆弱性の修正プログラムがリリースされたらすぐに優先して適用します。展開の修正プログラム管理サイクルを待つ必要はありません。
2. 企業ハードウェアおよびソフトウェア資産をすべて文書化してインベントリを作成することにより、リスクを見分け、修正プログラムに基づいて行動するタイミングをすばやく判断します。

ロシアの国家レベルのアクターによる戦時中のサイバー戦術がウクライナと他の国々を脅かしている

今年は、ロシアの国家レベルのアクターがサイバー作戦を開始し、ロシアによるウクライナ侵攻中の軍事行動を補完していますが、多くの場合、ウクライナ国外の標的に対して展開されているのと同じ戦術と手法が使用されています。世界中の組織が、ロシアと協力する脅威アクターからもたらされるデジタルの脅威に対して、サイバーセキュリティを強化するための対策を講じることが重要です。

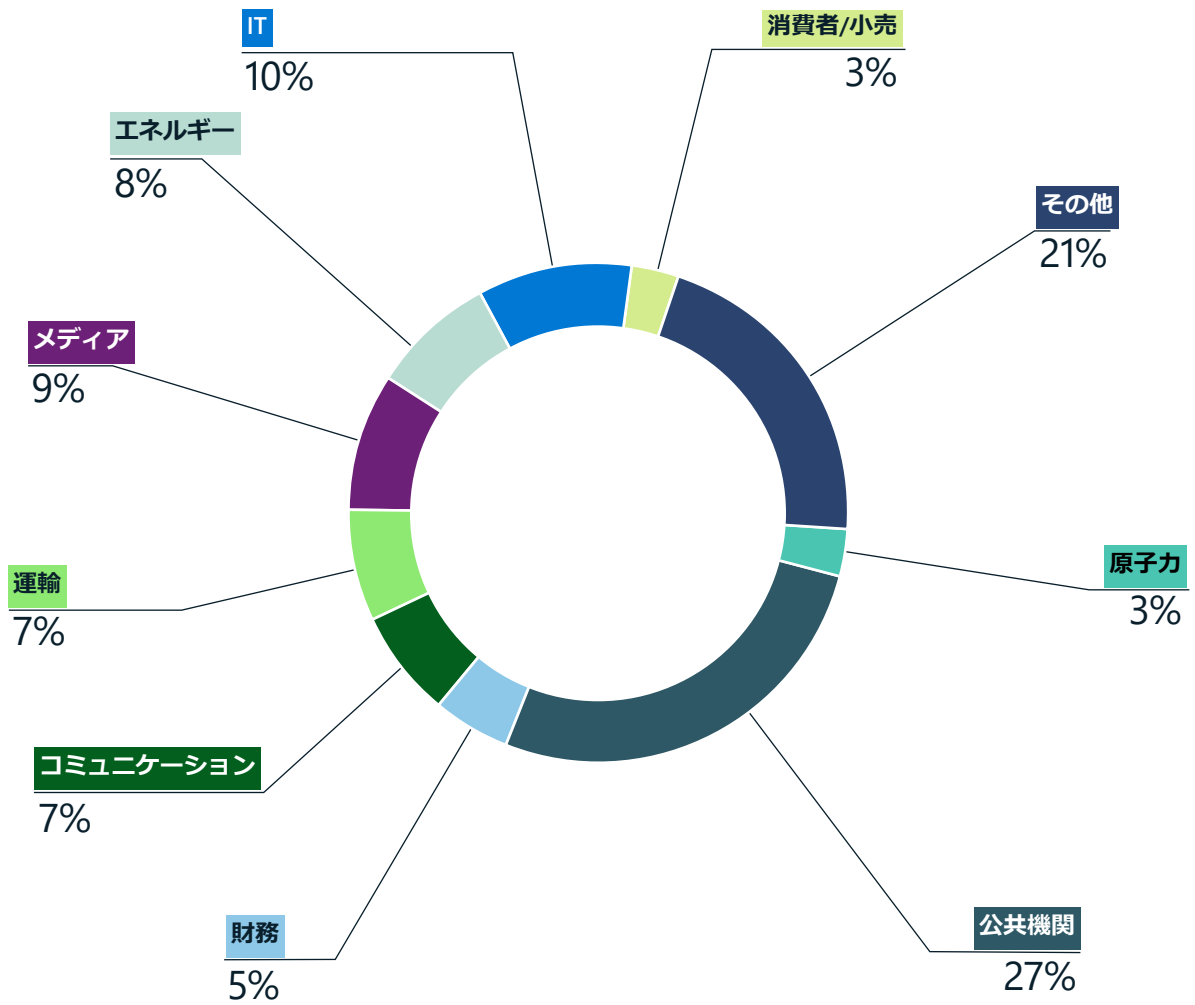
軍事紛争が長期化するにつれて現地の状況は変化を続けており、ロシアの国家レベルのサイバー オペレーターが軍事的な目的に沿って侵入の頻度や程度を高めた場合、ウクライナとその同盟国は自身を防御する準備をする必要があります。戦争の最初の 4 か月間、マイクロソフトは、ロシア軍に関係のある脅威アクターが、ほぼ 50 のウクライナの機関や企業に対して、破壊的なサイバー攻撃の波を複数開始し、他の多くの組織にスパイ行為を目的とした侵入を行ったことを観察しました。オンラインサービスの顧客に対する業務を除き、既知の標的に対するロシアの脅威活動の 64% が、2 月下旬から 6 月までの間にウクライナを拠点とする組織に向けられました。

各作戦では、ロシアの脅威アクターは、ウクライナ内外の標的に侵入する前に使用されていた戦術、手法、手順 (TTP) の多くを採用していました。これらのアクターは、データを破壊し、ウクライナの行政機関が紛争の初期にバランスを崩すことを意図していました。それ以降、ウクライナへの軍事および人道支援の輸送を妨げて、サービスとメディアの一般利用を妨害し、長期的なインテリジェンスまたは経済的価値に関する情報をロシアに盗み出そうとしてきました。

輸送を標的にすることは、ウクライナ国民が紛争を生き残るのにきわめて重要な領域を脅かすことを意味します。5 月にユニセフが委託した調査によると、紛争の影響を受けた都市部の回答者は、輸送と燃料、供給の中断、セキュリティ、食品、医療サービス、金融サービスを利用しにくくなることについて最も心配していました。[10] 6 月、ウクライナの国連危機調整官は、ウクライナの少なくとも 1,570 万人が人道支援を緊急に必要としており、その数は戦争が進むにつれて増加するだろうと述べました。[11]

ウクライナ国外では、2 月下旬から 6 月にかけて 42 か国の 128 の組織に対して、ロシアがネットワーク侵入を試みたことをマイクロソフトが検出しました。米国は、ロシアが最も多く標的とした国です。ウクライナに対する国際的な軍事および人道支援が経由しているポーランドも、この期間中に数多く標的となりました。ロシアと関連する脅威アクターは、4 月と 5 月に、バルト諸国の組織、デンマーク、ノルウェー、フィンランド、スウェーデンのコンピューター ネットワークも攻撃しました。

侵攻以来ウクライナで最も多く標的となった業界



ウクライナの連邦政府、州政府、地方自治体は、紛争が始まったときからロシアの国家レベルの脅威グループと国家関連の脅威グループが優先して攻撃する標的であり続けています。運輸、エネルギー、金融、メディアの各業界の組織が特に狙われていることは、ウクライナ国民が依存しているサービスにこれらのサイバー作戦がもたらすリスクを強調しています。

ロシアの国家レベルのアクターによる戦時中のサイバー戦術がウクライナと他の国々を脅かしている

(続き)

NATO 加盟国の外務省を標的とした同様の活動の増加が見られました。

ロシアの脅威グループは、過去 1 年間ウクライナ内外で重要インフラを侵害することに関心を示してきました。IRIDIUM は、マルウェア Industroyer2 を展開しましたが、ウクライナの何百万人もの人々を電力のない状態にする試みに失敗しました。ウクライナ国外では、2022 年初頭に BROMINE が製造業に携わる組織と、産業統制システムに侵入しました。

ロシアの国家レベルのアクターと関連アクターは今年、以下の TTP の多くを使って、ウクライナとその同盟国、インテリジェンスの価値を持つ他の標的に対するサイバー作戦を指揮しました。

悪意のある添付ファイルやリンクを使ったスピアフィッシング

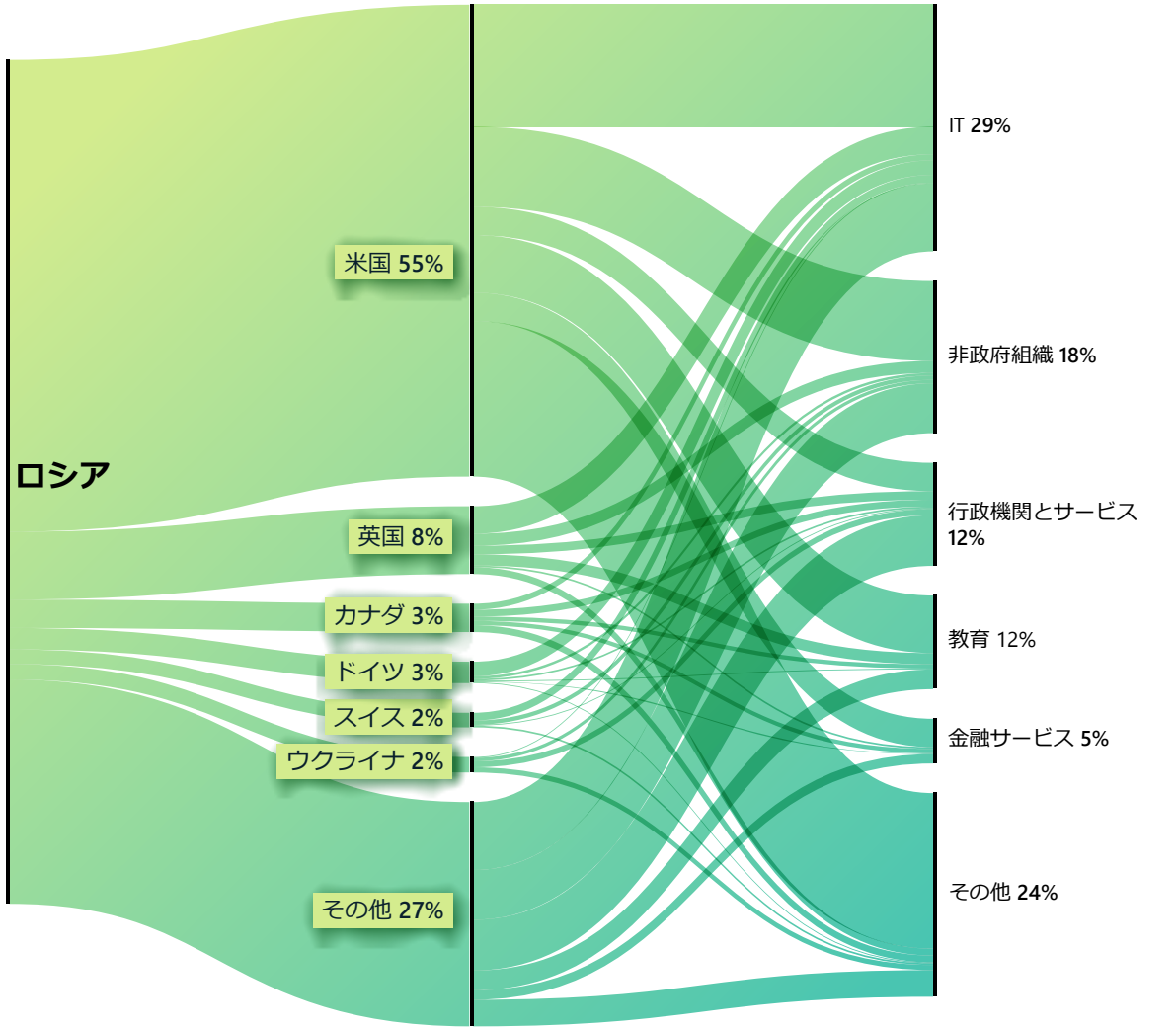
ACTINIUM、NOBELIUM、STRONTIUM、DEV-0257、SEABORGIUM、IRIDIUM など、ロシアの国家レベルのグループと関連グループはすべて、フィッシング キャンペーンを使って、ウクライナ内外の組織における目的のアカウントとネットワークへの初期アクセスを獲得しました。多くのキャンペーンで、標的となった組織や、同じ業界内の侵害されたアカウントやなりすましアカウントと、被害者を誘い込むための説得力のあるテーマが利用されました。NOBELIUM は、侵害された外交アカウントを使用して、世界中の外務省職員に外交連絡を装ったフィッシング メールを送信しました。STRONTIUM は、米国のシンク タンクの公開されたアカウント所有者の名前に基づいてなりすましアカウントを作成し、フィッシング メッセージを送信して、それらのシンク タンクのアカウントにアクセスしました。SEABORGIUM は、ウクライナ紛争の報告に関連するルアーを使ってフィッシングを行い、北欧諸国の国際事務シンク タンク アカウントへの初期アクセスを獲得しました。

IT サービスのサプライ チェーンを悪用してダウンストリームの顧客に影響を与える

2021 年の後半、ロシアの国家レベルのアクターは IT サービス プロバイダーを侵害して、アクセス権を使用し、1 月に DEV-0586 が Web サイトの改ざんと破壊的なマルウェア Whispergate の展開を実行できるようにしました。[12] DEV-0586 は、ウクライナ国防総省や通信および運輸業界の他の組織向けのリソース管理システムを構築した IT 企業のネットワークも侵害しました。これは、同グループがそれらの業界でサードパーティ攻撃オプションも模索していたことを示しています。

世界の他の国々、特に米国と西ヨーロッパでは、NOBELIUM が IT サービス プロバイダーを標的とし、2021 年から 2022 年の間に政府や他の機密ネットワークへのアクセス権を取得しています (この章の前半にあるサプライ チェーンの脆弱性についての説明を参照してください)。

ロシア : 標的とした主な国と業界



2022 年初頭以来、ウクライナを拠点とする組織に攻撃が集中していますが、北米と西ヨーロッパに拠点を置く企業も依然としてロシアのアクターが最も多く標的とするオンライン サービス顧客でした。IT 業界に対する NOBELIUM のキャンペーンでは、同業界が過去 1 年間最も多く標的となりました。

ロシアの国家レベルのアクターによる戦時中のサイバー戦術がウクライナと他の国々を脅かしている

(続き)

公開アプリケーションを悪用したネットワークへの初期アクセスの取得

2021 年後半以降、STRONTIUM は、Microsoft Exchange サーバーなどの公開サービスを悪用して情報を盗むため、自身の能力の育成と改良に取り組んでいました。STRONTIUM は、修正プログラムが適用されていない Exchange サーバーを悪用し、ウクライナ政府のアカウントだけでなく、米国、レバノン、ペルー、ルーマニアの軍事および防衛業界関連の組織や、アルメニア、ボスニア、コソボ、マレーシアに拠点を置く他の政府機関にもアクセスしました。さらに、ロシア軍に関連する 0586 は、Confluence サーバーの脆弱性を悪用し、ウクライナや他の東ヨーロッパ諸国の政府および IT 業界組織への初期アクセスを獲得しました。

ロシアの国家レベルの脅威アクターと関連脅威アクターは、同じ TTP の多くを使用して、戦争と平和の時代に関心を持つ組織を侵害しています。

管理者アカウントとプロトコルの使用、およびネットワーク探索と侵入拡大のためのネイティブ ユーティリティ

マイクロソフトは、ロシアの国家レベルのアクターが、ネットワークへの初期アクセス権を取得した後、できる限り長い間検出を回避する目的で、基本的なメンテナンス タスクを実行するために使用される正当なアカウントとソフトウェア ユーティリティを利用しているのを観察しました。自動化された監視やモニターやネットワーク防御者にすぐに気づかれずにネットワーク内で侵入を拡大するため、管理能力を持つ侵害した ID と、有効な管理プロトコル、ツール、手法に依存していました。

基本的なサイバー衛生とエンドポイント検出および対応ツールの採用により、平時も戦時中もこのような種類の作戦の悪影響を軽減することができます。

継続する紛争についての予測が困難なため、世界中の組織には、ロシアの国家レベルの脅威アクターや関連脅威アクターからもたらされるデジタル脅威に対抗してサイバーセキュリティを強化するための対策を講じることが求められています。

実用的なインサイト

1. MFA ID 保護ツールを実装して最小限の特権アクセスを適用し、最も機密性の高い特権アカウントおよびシステムを保護することにより、ユーザーの ID を保護して資格情報の盗難とアカウントの不正使用を最小限に抑えます。
2. 更新プログラムを適用し、すべてのシステムにできるだけ早く十分な保護を適用して、最新の状態に保ちます。
3. マルウェア対策、エンドポイント検出、ID 保護ソリューションを組織全体に展開します。多層防御のセキュリティ ソリューションと、トレーニングを受けた有能な担当者と組み合わせることで、ビジネスに影響を与える侵入を組織は特定、検出、防止できるようになります。
4. 重要なシステムをバックアップしてログを有効にすることにより、環境に対する脅威の通知を検出したり受け取ったりした場合に調査と復旧を実行できるようにします。インシデント対応計画を策定することを強くお勧めします。

詳しい情報のリンク

- ウクライナ防衛 : サイバー戦争から得られた初期の教訓 | Microsoft On the Issues
- ウクライナにおけるハイブリッド戦争 | Microsoft On the Issues
- ウクライナにおけるサイバー脅威活動 : 分析とリソース | Microsoft Security Response Center (MSRC)
- ウクライナを標的とするサイバー攻撃を阻止する | Microsoft On the Issues
- ウクライナ政府を標的としたマルウェア攻撃 | Microsoft On the Issues
- MagicWeb: あらゆるユーザーとして認証する NOBELIUM による侵害後のトリック | Microsoft Threat Intelligence Center (MSTIC)、Detection and Response Team (DART)、Microsoft 365 Defender Research Team

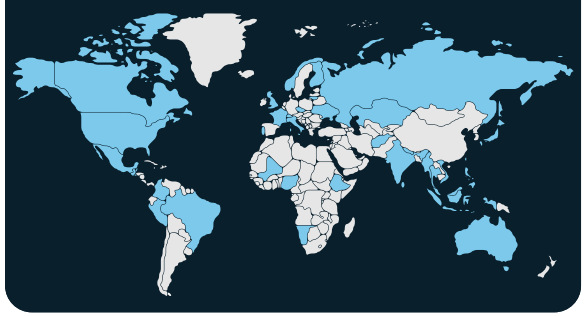
中国が競合優位性のためにグローバルな標的を拡大している

現在の複雑な地政学的環境では、サイバー作戦を実行している中国の国家レベルの脅威アクターと関連脅威アクターは多くの場合、中国の競争優位性を確立する目的の一環として、同国の軍事、経済、外交関係の戦略的目標をさらに強化することを目的としています。昨年、マイクロソフトは、世界中の国々を標的とした、中国の広範な脅威活動を観察しました。

2021 年半ば以降、中国は 2 年間で最も COVID-19 が急増している中、経済と金融の安定を確保するための作戦行動を取ってきました。[13] 中国は、ロシアとの「際限のない」パートナーシップのバランスを取ったり [14]、世界全体での地位を維持したりするのに苦労するなど [15]、地政学的出来事における自国の立場をうまく調整してきました。加えて、台湾 [16] と南シナ海に関する米国とその同盟国に対する中国のスタンスは、多くの国々との外交関係を緊張させ続けてきました。[17]

中国の国家レベルの脅威グループと関連脅威グループは、東南アジアを中心に、世界中の小規模な国々の標的を増やし、あらゆる最前線で競争優位性を獲得しました。

中国の国家レベルのグループと関連グループが標的とする国々

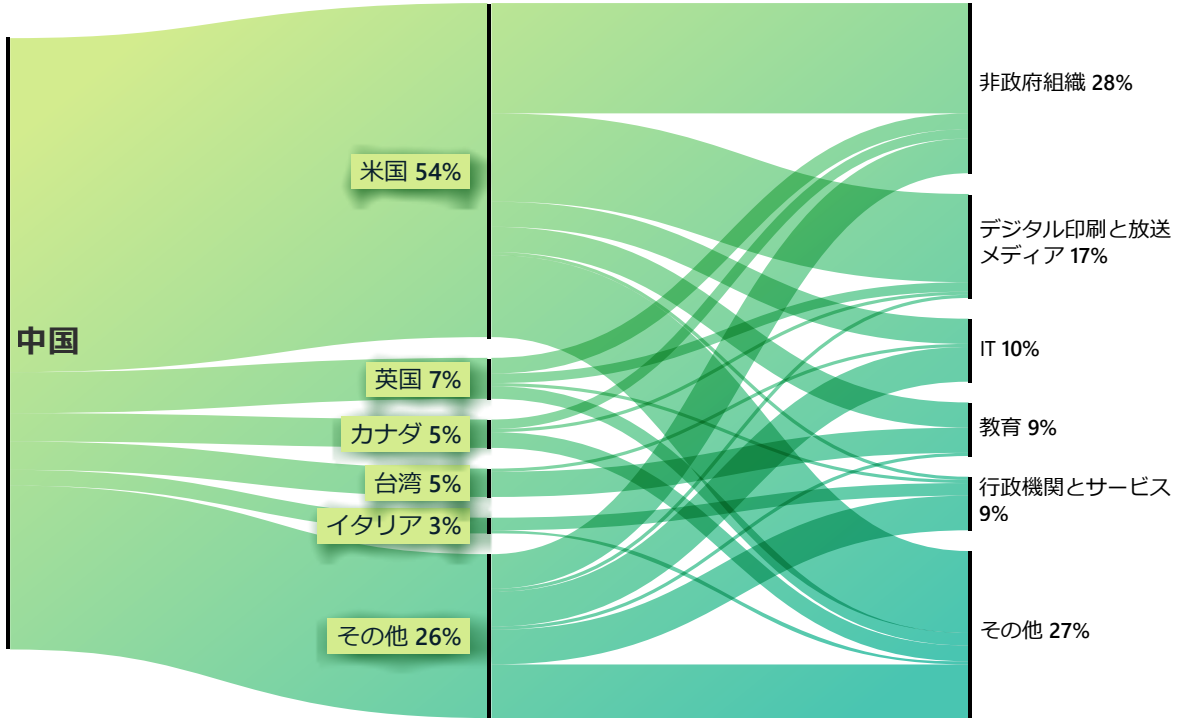


さらに中国は、既に確立された一帯一路政策 (BRI) を通じて世界中の経済への影響力を拡大し続けており、EU との包括的な投資フレームワークの復活を目指し [18]、地域的な包括的経済連携協定と呼ばれる新たな地域貿易協定をアジア太平洋の 15 か国と交渉しています。[19] マイクロソフトは、サイバー作戦が観察されており、幅広いエンティティが標的となっているため、中国はこれからも政治的、軍事的、経済的目標の達成を後押しするツールとしてサイバー コレクションを利用していくと予想しています。

サイバー攻撃は、経済的および軍事的な利益を後押しする可能性があります。

マイクロソフトは、中国の国家レベルの脅威グループと関連脅威グループが世界中の小規模な国々を幅広く標的としているのを観察しました。これは、中国がサイバー スパイ行為を世界の経済と軍事への影響力の要素として利用している可能性を示唆しています。

中国 : 標的とした主な国と業界



シンク タンク /NGO、メディア、IT、政府、教育の各分野は、中国ベースの脅威グループによる最も多くの標的となった分野であり、その目的は持続的なインテリジェンスの収集と偵察と考えられます。

標的の範囲は、アフリカ、カリブ海諸国、中東、オセアニア、南アジアの国々が含まれていますが、これに限りません。特に東南アジアの国々と太平洋諸島に重点が置かれていました。

中国の BRI 戦略に沿って、中国ベースの脅威グループはアフガニスタン、カザフスタン、モーリシャス、ナミビア、トリニダード・トバゴのエンティティを標的としました。[20] たとえば、トリニダード・トバゴは、2018 年に中国の BRI 戦略を支持した最初のカリブ海諸国であり、中国は同国を地域の重要なパートナーと見なしています。NICKEL は、2021 年以来トリニダード・トバゴを標的とした持続的なネットワーク作戦を行ってきました。たとえば、2022 年 3 月、NICKEL は行政機関を標的とした偵察活動を実施しました。これには、インテリジェンス収集の目的があると考えられます。

中国が競合優位性のためにグローバルな標的を拡大している

(続き)

一方、マイクロソフトは、中国の国家レベルの脅威グループと関連脅威グループが、東南アジアのエンティティに対するネットワーク作戦に重点を置き、太平洋島嶼国への拡大を目指しているのを観察しました。米国がこの地域に向けた新たな関心という問題に対処するため、中国が軍事と経済の優先事項を移したからです。2022 年 1 月、マイクロソフトは、RADIUM がベトナムのエネルギー企業およびエネルギー関連行政機関と、インドネシアの行政機関を標的としたのを観察しました。RADIUM の活動は、南シナ海における中国の戦略的目標に沿っていると考えられます。[21] 2 月下旬と 3 月上旬、GALLIUM は東南アジア地域の著名な政府間組織 (IGO) に加盟している 100 以上のアカウントを侵害しました。この地域の IGO を GALLIUM が標的としたタイミングは、米国と地域のリーダーたちの間で予定されていた会議の発表と一致していました。GALLIUM のアクターは、通信を監視し、イベントの前にインテリジェンスを収集する任務を負っていると考えられます。

中国が太平洋島嶼国での影響力を拡大したため、中国の脅威グループの活動が続いています。4 月、中国とソロモン諸島は、「平和と安全を促進する」ことを目的とした安全保障協定に調印しました。この協定により、中国は武装した警察と軍隊をソロモン諸島に配備できるようになる可能性があります。[22] 5 月、中国はフィジーで第 2 回中国太平洋島嶼国 (PIC) 外相会議を開催し、政治的、文化的、社会的、安全面、気候変動の関心事をさらに推し進め、パンデミックとも闘うため、「包括的な戦略的パートナーシップ」の推進を提案しました。[23] 5 月のほぼ同時期、マイクロソフトはソロモン諸島の政府システムで GADOLINIUM のマルウェアを特定しました。さらに、RADIUM はパプアニューギニアの通信会社のシステムでも悪意のあるコードを実行しました。マイクロソフトは、これらの活動は中国の全体的な地域戦略を後押しするインテリジェンスの収集を目的としている可能性が高いと考えています。

マイクロソフトは、NICKEL の作戦を阻止していますが、脅威グループは粘り強さを見せています。

2021 年 12 月、マイクロソフト デジタル犯罪対策ユニット (DCU) は、バージニア州東部地区の米国地方裁判所に、NICKEL によって制御されている 42 の指揮統制 (C2) ドメインを差し押さえる訴答状を提出しました。これらの C2 ドメインは、2019 年 9 月以来、中南米、カリブ海、ヨーロッパ、北米の政府、外交機関、NGO に対する作戦で使用されました。[24] これらの作戦を通じて、NICKEL は複数のエンティティに対する長期的なアクセスを確立し、2019 年の後半以降、犠牲者のデータを不正取得し続けてきました。

中国が多くの国との二国間経済関係 (BRI に関連する協定の場合もある) を確立し続けるにつれて、中国の世界的な影響が拡大し続けています。マイクロソフトは、中国の国家レベルの脅威アクターと関連脅威アクターが政府、外交、NGO の各分野で標的を狙い、新たなインサイトを得ると予想しています。これは、経済的なスパイ活動や、従来型のインテリジェンス収集が目的と考えられます。マイクロソフトが阻止してからも、NICKEL は複数の行政機関を標的にしています。失われたアクセスを取り戻そうとしていると思われます。2022 年 3 月下旬から 5 月までに、NICKEL は世界中の少なくとも 5 つの行政機関を再侵害しました。これは、同グループがそれらのエンティティへの追加のエントリ ポイントを持っていたか、新しい C2 ドメインを通じてアクセスを取り戻したことを示唆しています。世界中で同じ行政機関を繰り返し侵害することに見えている NICKEL の粘り強さは、そのタスクの重要性が高いレベルにあることを示しています。

中国の外交政策に対するスタンスは、強引さが増しています。マイクロソフトは、サイバーに対応した経済スパイとインテリジェンス収集が続くものと予想しています。

実用的なインサイト

1. サイバー防御を強化し、サイバー脅威をプロアクティブに軽減します。中国の脅威アクターが粘り強さを見せているため、組織は起こりうる侵入をタイムリーな方法で特定、保護、検出、対応する必要があります。
2. 脅威アクターは、持続性と防御の回避の一般的な方法としてスケジュールされたタスク[25]を悪用するため、よく使用されるその手法から保護するための追加のセキュリティ ガイドラインを環境で採用してください。[26]
3. 標的ネットワークへの初期ベクトルとして、Web シェルの使用が継続的に観察されています。[27] 組織は、リモート コマンドを実行するアクセス権を攻撃者に提供する可能性がある Web シェル攻撃に対抗できるよう、システムを強化する必要があります。[28]

詳しい情報のリンク

- NICKEL は中南米とヨーロッパ全体の行政機関を標的とする | Microsoft Threat Intelligence Center (MSTIC)、Microsoft Digital Security Unit (DSU)
- 最近のサイバー攻撃から人々を保護する | Microsoft On the Issues

権力移行後にイランは攻撃性をますます強めている

マイクロソフトは、イランの国家レベルのグループと関連アクターがイスラエルに対するサイバー攻撃のペースを高めて範囲を広げ、地域内の敵対国を超えてランサムウェア攻撃を米国と EU に拡大しただけでなく、今後実行するかもしれない破壊的サイバー攻撃の少なくとも準備として、米国の重要インフラを標的にしたことを観察しました。

イランの国家レベルのアクターによるサイバー攻撃の増加は、大統領の権力移行後に置きました。2021 年の夏、穏健派の Hassan Rouhani 氏に代わって強硬派の Ibrahim Raisi 氏が大統領に就任しました。最高指導者の支援を得ていて、イスラム革命防衛隊 (IRGC) と緊密な関係である Raisi 氏とは大きく異なり、前大統領である Rouhani 氏は、外交関係に対する考え方が原因で最高指導者や IRGC の最高幹部と対立することがよくありました。[29] イランとの核兵器取引を復活させる外交的交渉が再開されたにもかかわらず、Raisi 政権のタカ派的な考え方によって、イランのアクターがイスラエルと西側、特に米国に対して大胆な行動を取る意欲が高まっているように見えます。

イスラエルに対するイランのサイバー攻撃のペース向上と範囲拡大

Raisi 氏が外交政策チームを結成してから数週間以内に [30]、イランの国家レベルのアクターは、イスラエルに対する破壊的なサイバー攻撃を前年度よりも速いペースで再開しました。それらのランサムウェアおよびハック アンド リーク攻撃は、9 月から数週間ごとに実施され、少なくとも 3 つのイラン関連アクターが関与しました。これは、攻撃がイスラエルに対する報復の全国的キャンペーンの一部であった可能性があることを示唆しています。少なくとも 1 つのケースにおいて、2021 年後半のイスラエル組織に対するランサムウェア攻撃は、基礎となるデータ削除攻撃を隠蔽することが目的であったとマイクロソフトは考えています。マイクロソフトのマルウェア分析は、被害者に配信されたランサムウェアが、暗号化の後ワイパー マルウエアを実行するようにプログラムされていると判断しました。

2022 年までに、イランのサイバー攻撃は標的の選択と攻撃の形態の点でエスカレートしました。2 月、DEV-0198 はイスラエルの重要インフラに対する破壊的な攻撃を試みました。さらに、マイクロソフトは、6 月にイスラエルの緊急ロケット サイレンを作動させた高度なサイバー攻撃を、イラン関連アクターが担当した可能性が高いと考えています。おそらく、IP ネットワーク経由でオーディオを調整するソフトウェアを使用して行ったと考えられます。

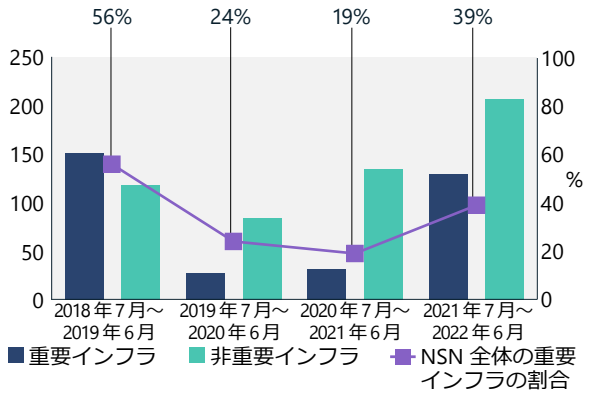
米国とイスラエルの重要インフラに対するイランの脅威が年間を通じて増加

マイクロソフトの調査によると、イランの国家レベルのアクターは IRGC (PHOSPHORUS および DEV-0198) と協力関係にあり、2021 年後半から 2022 年半ばまでに米国およびイスラエルの重要インフラを標的としました。イランでの破壊攻撃に関して IRGC 上級職員が米国とイスラエルを非難したのと同じ分野に対して報復する選択肢をテヘランに提供することが目的であったと考えられます。[31] この活動は、米国とイスラエルがイランの港湾、鉄道、給油所へのサイバー攻撃を実施したという、政権内の他の影響力のある人物から出た非難を表明した IRGC 将官 Gholamreza Jalali 氏 (消極的防衛組織の責任者) によって、2021 年 10 月下旬に発表された内容に関連しているとマイクロソフトは考えています。[32] Jalali 氏は、「USA」という文字を攻撃するミサイルが描かれた演壇で金曜日の祈祷舞台演説をしたとき、前もって準備された発言内容としてこの非難をもう一度表明しました。これは、彼の上官たちも同じ見解を持っていることを示唆しています。[33]

PHOSPHORUS は、2021 年 10 月に米国組織の広範なスキャンを開始し、修正プログラムが適用されていない Fortinet と ProxyShell の脆弱性を探しました。侵害されると、修正プログラムが適用されていないそれらのシステムは、米国および他の西側諸国の重要インフラに対するいくつかのケースで、ランサムウェア攻撃の実行に使われました。これらは、中東以外でイラン関連のランサムウェア攻撃が最初に確認されたケースです。10 月後半のイランの給油所に対するサイバー攻撃に続いて、マイクロソフトは米国企業に対するイランのランサムウェア攻撃が急増したのを観察しました。これは相関関係を示唆している可能性があります。

同時に、PHOSPHORUS は米国の重要インフラ企業を直接標的型攻撃に移行しました。多くの場合、玄関口となる主要な海港または空港、交通網、公共事業会社、石油およびガス会社などのスピア フィッシングを通じて行われます。この攻撃は多くの場合、スピア フィッシングを介して行われ、2022 年の半ばまで続きました。標的は、イランでの攻撃に関してテヘランが米国とイスラエルを非難した分野と直接関係があり、おそらくイランに報復の選択肢を提供したと考えられます。ほぼ同一の標的に対する侵害は、今後の攻撃を阻止する機会となりますが、罪を認めずに攻撃の原因を伝えることによってエスカレーションを回避することを狙っています。

イランによるインフラ標的攻撃の復活



イランによる重要インフラの標的攻撃は、2018 年の後半から 2019 年前半にかけて最も高いレベルまで増加しました。マイクロソフトは、米国大統領政策命令 21 (PPD-21) を利用して、企業が重要インフラの基準に適合しているかどうかを判断しました。(2021 年 7 月～2022 年 6 月)。

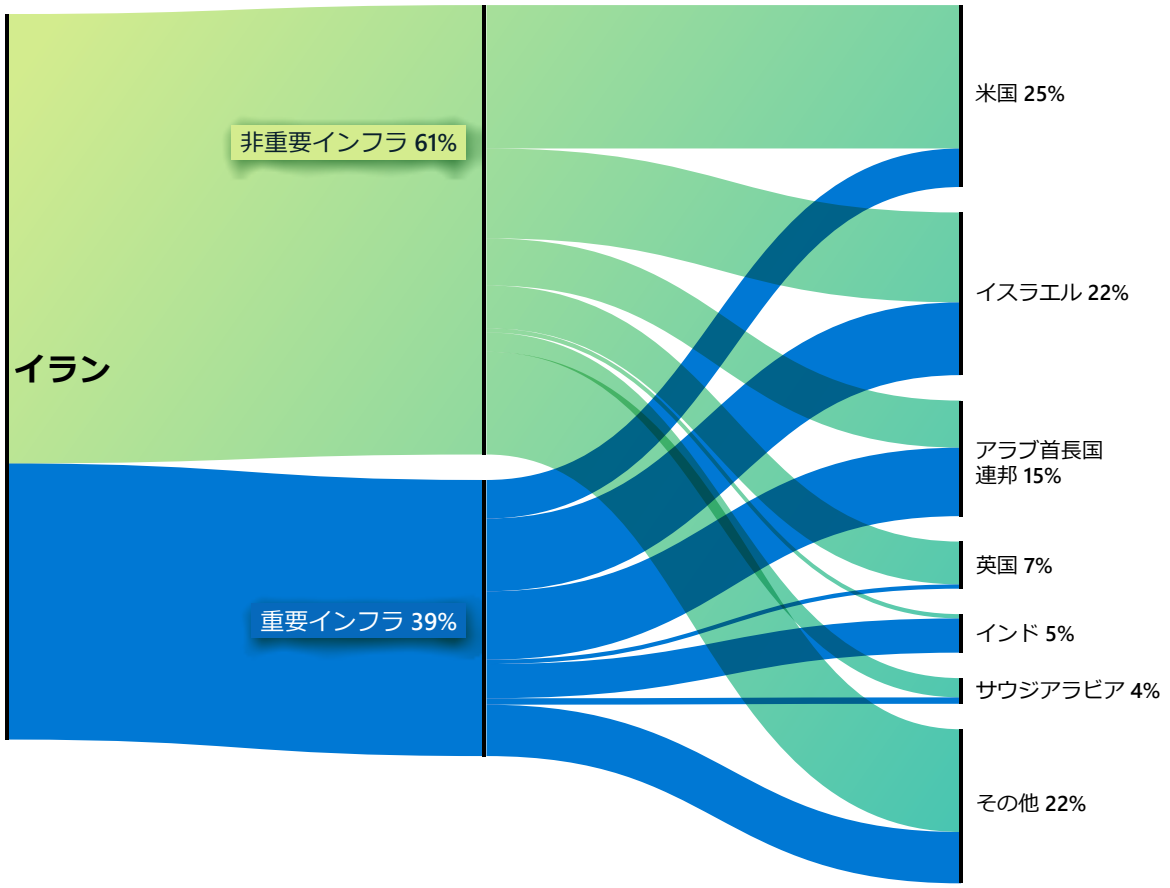
権力移行後にイランは攻撃性をますます強めている

(続き)

イスラエルでは、DEV-0198 がイスラエルの鉄道、ロジスティクス企業、ロジスティクス企業のソフトウェア プロバイダー、燃料企業 (特にガソリン スタンド) を標的としました。2022 年初頭、イスラエルの主要ロジスティクス会社のネットワークに対して破壊的な攻撃が行われました。これにより、同社のコンピューターがシャットダウンし、一部の業務に攻撃が混入しました。別のケースでは、盗難または再利用された資格情報を介して、イスラエルの主要輸送プロバイダーのネットワークにアクセスしようとするグループの試みが観察されました。一方、イランの別のアクターである DEV-0343 (国防総省、海上輸送機関、衛星画像企業を標的としていることが、IRGC との関連を示唆している) は、2021 年前半、イスラエルの輸送および港湾関連エンティティのアカウントを侵害しました。

イランの脅威グループは、特にイランの核取引の減少を復活させる外交努力として、米国とイスラエルの輸送およびエネルギー企業にとって脅威となり続ける可能性があります。ワシントン、テルアビブ、テヘランは、譲歩を引き出すための強硬な代替手段を模索しています。

イランによる重要インフラの標的化 (国別)



イランによる重要インフラの標的化は、イスラエル、アラブ首長国連邦、米国の組織で特によく見られます。

イランのアクターは、来年も米国とイスラエルの輸送およびエネルギー企業にとって脅威となる可能性が高いと考えられます。

イランのグループは、地域の敵対国を超えてランサムウェア攻撃を拡大しており、米国とイスラエルの重要インフラを標的としています。

実用的なインサイト

1. MFA などのパスワードレス ソリューションを有効にし、すべてのリモート接続でその使用を強制して、資格情報の侵害の可能性を下げることにより、組織全体のサイバー衛生を改善します。
2. すべての受信メール トラフィックの真正性を評価し、送信者アドレスが正当であることを確認します。
3. 早期かつ頻繁に修正プログラムを適用します。[34]
4. 組織とアップストリーム プロバイダー間の不必要なアクセス許可を最小限に抑えるため、サービス プロバイダーとのパートナー関係を 1 つ 1 つ見直して監査します。あまりよくわかっていないパートナー関係やまだ監査されていないパートナー関係があれば、そのアクセス権はすぐに削除することをお勧めします。[35]

詳しい情報のリンク

- イランによる IT 部門の標的が増加 | Microsoft Threat Intelligence Center (MSTIC)、Microsoft Digital Security Unit (DSU)
- 防衛、GIS、海事分野を標的としたイラン関連の DEV-0343 | Microsoft Threat Intelligence Center (MSTIC)、Microsoft Digital Security Unit (DSU)

イランに関連するレバノンを拠点とするグループがイスラエルを標的とする

マイクロソフトは、プラットフォーム、標的となる被害者、地理的地域に関係なく、サイバー脅威の活動を監視しています。お客様のために、世界中での脅威活動を検出して、明らかにすることに注力しています。

ロシア、中国、イラン、北朝鮮による脅威が観測された国家レベルのアクター活動の大半を占めていますが、NATO 加盟国や民主主義国家からの脅威についても追跡し、発表しています。昨年は、トルコに拠点を置くアクター (SILICON) とベトナムに拠点を置くアクター (BISMUTH) による活動を取り上げました。今年は、以前公開していたレバノンを拠点とするグループについてさらに詳しく説明しています。[36]

マイクロソフトは、以前は公開されていなかったレバノンを拠点とするグループを発見しました。このグループは、イランの諜報治安省 (MOIS) と関係があるアクターと協力していると、ある程度の確信を持って予想しています。テヘランからのそのような協力関係や方向性は、2020 年後半以降明らかになった、イラン政府がサイバー作戦を実施するために第三者を利用しているという事実と一致しています。これは、イランのもっともらしい反証を裏付けるためと考えられます。

観察された活動において、POLONIUM は、マイクロソフトによってその活動が阻止されて公になる前の 2022 年 2 月から 5 月の間、イスラエルを拠点とする 24 の組織と、レバノンで稼働している 1 つの IGO を標的にしたり、侵害したりしました。イスラエルの組織のほぼ半数は、イスラエルの防衛産業の一部であるか、イスラエルの防衛企業とのつながりを持っていました。これは、同グループが、インテリジェンスを収集したり、イスラエルに直接対抗したりする点で、イランと同様の利害関係を持っていたことを示しています。[37]

観察された被害者の重複と、ツールや手法の共通性に基づき、POLONIUM は MOIS グループと関連性があると考えられています。

- 被害者の重複 : マイクロソフトが MERCURY として追跡しているイランの国家レベルのグループ (イランの MOIS と関連がある) は以前、POLONIUM の複数の被害者を侵害していました。これは、ミッション要件の合致や、グループ間で被害者の「引き渡し」があった可能性を示唆しています。
- 共通のツールと手法 : MSTIC は、POLONIUM と同様に、DEV-0588 (CopyKittens とも呼ばれます) が作戦に同じ AirVPN を使用し、DEV-0133 (Lyceum とも呼ばれます[38]) が C2 と流出に OneDrive を使用していることを観察しました。POLONIUM は、イランの国家レベルのアクターと同様、クラウド サービス プロバイダーを使ってイスラエルの航空会社と法律事務所を侵害しました。[39]

POLONIUM は、C2 とデータ流出にクラウド サービス (特に OneDrive と DropBox) を使って一連のカスタム インプラントを展開しました。POLONIUM は多くの場合、標的専用の OneDrive アプリケーションを作成しました。検出を回避するためと考えられます。

2022 年 6 月の時点で、マイクロソフトは POLONIUM が作成した OneDrive アプリケーションを 20 件以上停止させて、影響を受けた組織に通知し、POLONIUM が開発したツールを隔離する一連のセキュリティ インテリジェンス更新プログラムを展開しました。

マイクロソフトは、POLONIUM が C2 としての OneDrive を不正利用しているのを検出し、無効化しました。

実用的なインサイト

1. ウイルス対策ツール[40] と更新し、クラウド保護[41] で関連するインジケーターの検出がオンになっていることを確認します。
2. サービス プロバイダーと関係のあるお客様の場合、すべてのパートナー関係の見直しと監査を実施し、組織とアップストリーム プロバイダーの間の不必要なアクセス許可を最小限に抑えてください。[42] よくわからないパートナー関係や監査されていないパートナー関係のアクセス権があれば、すぐに削除します。

詳しい情報のリンク

- イスラエルの組織を標的とした POLONIUM アクティビティとインフラの公開 | Microsoft Threat Intelligence Center (MSTIC)、Microsoft Digital Security Unit (DSU)
- 修正プログラムが適用されていないシステムで MERCURY が Log4j 2 の脆弱性を利用し、イスラエルの組織を標的とする | Microsoft Threat Intelligence Center (MSTIC)、Microsoft 365 Defender Research Team、Microsoft Defender 脅威インテリジェンス

政権の 3 つの主要目標を達成するために採用された北朝鮮のサイバー攻撃能力

過去 1 年間、北朝鮮のサイバー攻撃における優先順位は、同政府が表明した世界的な優先順位を反映していました。金正恩氏は、いくつかの主要な演説において、防衛力を構築して、低迷している同国の経済を強化し、国内の安定を確保するという 3 つの優先事項を強調しました。[43] 北朝鮮の国家レベルのアクターが取った行動は、これら 3 つの目標を達成するためにサイバー攻撃が利用されていることを明確に示しています。

北朝鮮の国家レベルのアクターは、さまざまな戦術を使って世界中の航空宇宙企業に侵入しようとしました。

北朝鮮の国家レベルの脅威グループ (主に CERIUM と ZINC) は、世界中の防衛および航空宇宙企業のネットワークへの侵入を試みるため、さまざまな戦術を利用しました。北朝鮮が 2022 年前半にこれまでで最も攻撃力の高いミサイル実験に着手した際、サイバースパイ行為を利用して、北朝鮮の研究者が国産防衛システムの開発において優位に立ち、敵対国の進歩に対抗できるようにしました。

COPERNICIUM は、世界中のさまざまな仮想通貨関連企業を標的にしており、多くの場合成功を収めているため、低迷する北朝鮮の経済に貢献しています。同グループが侵害後に資金を流出させることができたかどうかを確認することはできませんが、他の仮想通貨企業からの提案に偽装された悪意のあるドキュメントを送信することによって、COPERNICIUM が多数のコンピューターに感染したことが観察されました。

最後の点として、マイクロソフトが DEV-0215 として追跡しているグループは、北朝鮮の安定と忠誠心を守るため、北朝鮮の問題について報道するニュース組織を標的としました。これらの報道機関は、北朝鮮と脱北者コミュニティの両方に情報源を持っており、平壌は目前の脅威と見なしています。さらに、同グループは、北朝鮮に対して直接的な発言をする傾向があり、脱北者と積極的に連携している韓国語圏のキリスト教グループのネットワークにアクセスしました。

防衛および航空宇宙企業の標的化

CERIUM と ZINC が主導する北朝鮮の国家レベルのアクターは、防衛および航空宇宙企業への侵入を目的とした戦術の策定に大きな労力を注いでいます。CERIUM は、クライアントをダウンロードして弱点を探すことにより、韓国の仮想プライベート ネットワーク (VPN) を繰り返し調査しました。さらに、韓国の軍事および政府機関クライアントが使っている共通のアプリケーションもダウンロードしました。脆弱性を探すためと考えられます。同グループは、現在の出来事をしっかりと追いかけており、わなとして話題のトピックを使ってマルウェアの実行可能ファイルやリンクのクリックを誘い込む新しいルアー ドキュメントを作成しました。

ZINC と CERIUM はどちらも、キャンペーンにおいてソーシャル メディアとソーシャル エンジニアリングを使用していました。特に ZINC は、LinkedIn や他のソーシャル メディア サイトで偽のプロフィールを作成することに長けており、同グループのオペレーターが主要な防衛および航空宇宙企業の採用担当者のふりをしていました。それらのプロフィールを使って、ソーシャル メディアのダイレクト メッセージやメールを通じて潜在的な被害者にリンクや悪意のある添付ファイルを送信していました。

CERIUM は、企業の従業員に加えて、韓国軍の兵士を広く標的とすることで、韓国の士官学校と学界で働く兵士の両方に特別な関心を示しています。

仮想通貨を標的として損失のバランスを取る

北朝鮮の経済は、国連による制裁が 2016 年に課されて以来、洪水[44] や干ばつ[45] などの自然災害だけでなく、2020 年前半に COVID-19 パンデミックが始まってから国境がほぼ全面的に封鎖されて輸入できない状況が相まって、縮小が続いています。[46] 2022 年前半、北朝鮮は中国との貿易のため国境を短期間開きましたが、すぐに再度封鎖されました。[47] 5 月中旬、北朝鮮は COVID-19 の国内初の事例を報告しました。[48] それ以来、既に脆弱な北朝鮮の経済にマイナスの影響を与えたウイルスに対抗するため、大規模なロックダウンを行う中国流の「ゼロコロナ」政策が採用されました。

北朝鮮の国家レベルのグループである COPERNICIUM は、ネットワークに侵入できた企業から金銭を盗むことによって (通常は仮想通貨の形で)、損失の一部を相殺しようとしました。米国、カナダ、ヨーロッパ、アジア全域の仮想通貨関連企業にある多数のコンピューターが侵害されたことが観察されています。COPERNICIUM は、北朝鮮の強力な同盟国である中国 (本土と香港の両方) の仮想通貨関連企業に所属するコンピューターでさえ侵害しました。同グループは、標的を早期に偵察してアプローチする点でソーシャル メディアに大きく依存していました。アクターは、仮想通貨関連のビジネス開発者や役職者のふりをするため、プロフィールを作成しました。その後、業界の人々と親密な関係を築いてから悪意のあるリンクやファイルを送信しました。

政権の 3 つの主要目標を達成するために採用された北朝鮮のサイバー攻撃能力

(続き)

PLUTONIUM に関連するグループがランサムウェアを開発して展開する

マイクロソフトが DEV-0530 として追跡している北朝鮮のアクター グループは、ランサムウェアの開発を始め、2021 年 6 月の攻撃で使用しました。自身を H0lyGh0st と呼んでいるこのグループは、キャンペーン用と同じ名前でランサムウェア ペイロードを利用し、早ければ 2021 年 9 月に複数の国の小規模企業の侵害に成功しました。

マイクロソフトは、DEV-0530 が PLUTONIUM (DarkSeoul または Andariel とも呼ばれています) として追跡されている北朝鮮を拠点とする別のグループとのつながりを持っていると考えました。H0lyGh0st のランサムウェアの使用は DEV-0530 独自のものですが、MSTIC が 2 つのグループ間の通信を観察したところ、PLUTONIUM だけが独占的に作成したツールを DEV-0530 が使っていることがわかりました。

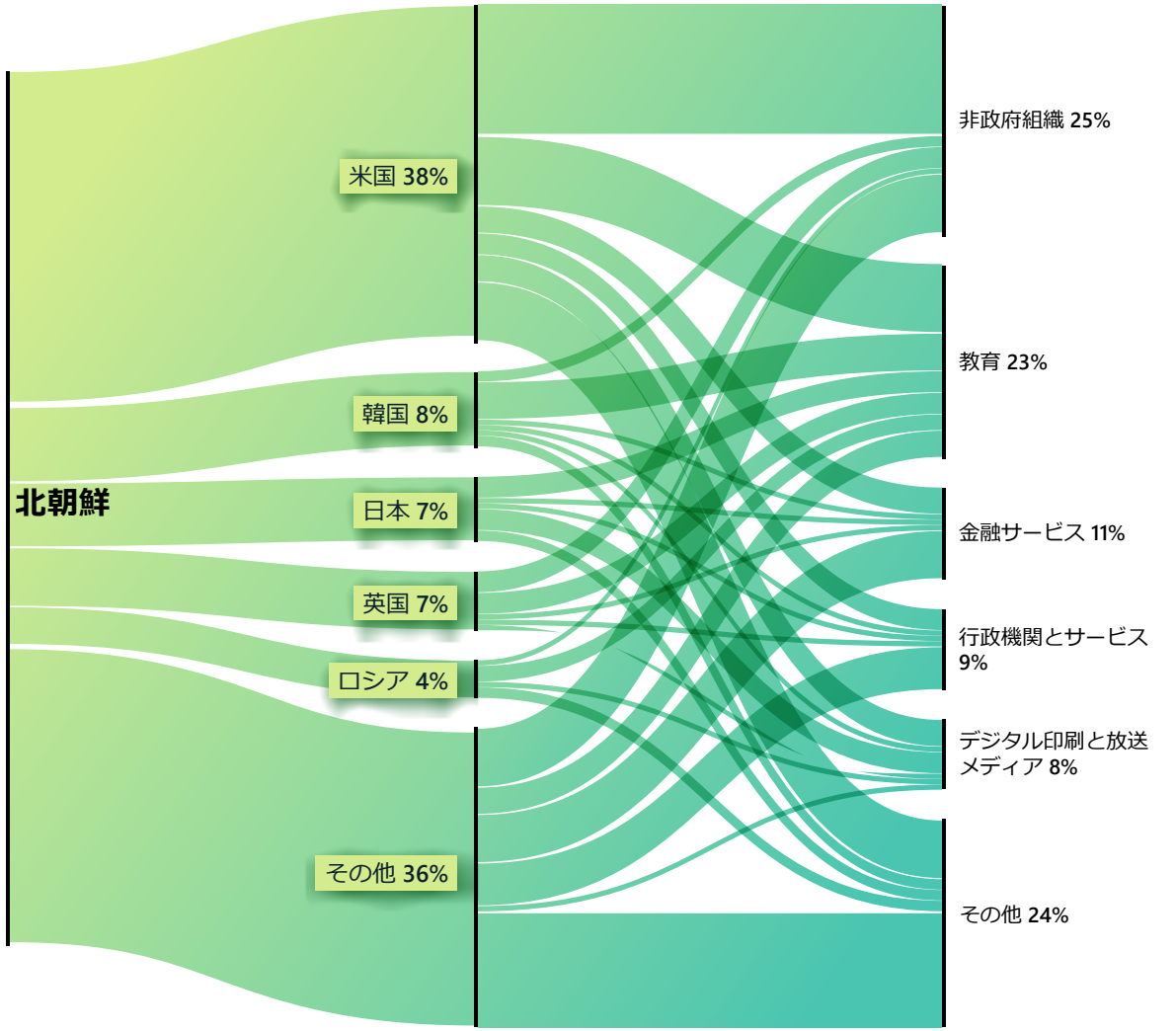
DEV-0530 の活動が政府によって支援されているかどうかははっきりしていません。ランサムウェア攻撃は、政府が仮想通貨企業からの盗難を支援しているのと同じ理由で政府が発注した可能性がありますが、DEV-0530 の背後にいるアクターが自分自身の金銭を稼ぐために独立して行動していた可能性もあります。北朝鮮のハッカーが独立して行動していたとしたら、政府が支援していた仮想通貨企業に対する盗難作戦と比べて活動が広まらなかった理由を説明できます。

北朝鮮の報道機関、脱北者、宗教団体、援助団体の標的化

昨年、最高指導者である金正恩氏は、公にはミサイルと核兵器よりも国内の安全保障と忠誠心に焦点を当てていました。この見方を国内の問題と照らし合わせると、少なくとも 2 つの北朝鮮の国家レベルのグループは、政権が国内の脅威として見ている側面に焦点を当てていました。

1 つ目は、北朝鮮のニュースをしっかりと追いかけているメディア組織を標的とした、マイクロソフトが DEV-0215 として追跡しているグループです。標的となっている理由の 1 つは、それらの報道機関が北朝鮮の脱北者、北朝鮮と緊密に関わっている中国国民、さらには国外とのさまざまな通信手段を利用している国内の北朝鮮国民からニュースを得ているためです。北朝鮮政府は、これらのグループを政府存続にとって目前の脅威と捉えています。特に北朝鮮国内にいる国民は、反逆者やスパイとみなされています。DEV-0215 は、情報漏えいのリスクがなくなるよう、それらの報道機関の情報源を特定しようとしていると考えられます。

北朝鮮 : 標的とした主な国と業界



北朝鮮は、米国、韓国、日本を主要な敵と見なしています。ロシアは長い間同盟関係にありますが、北朝鮮の脅威アクターはロシアのシンク タンク、学者、外交当局者を標的とし、世界情勢に対するロシアの見方についてのインテリジェンスを入手しています。

政権の 3 つの主要目標を達成するために採用された北朝鮮のサイバー攻撃能力

(続き)

さらに、DEV-0215 が韓国語圏のキリスト教コミュニティを標的としていた証拠も見られました。福音主義的な韓国のキリスト教会は、北朝鮮政府と、北朝鮮との関わりを支持する韓国政府両方に批判的になる傾向があります。それらの教会は、脱北者と接触しようとする可能性があり、北朝鮮との人道的な取り組みに従事している人もいます。北朝鮮が脅威として見ているのは、パンデミックの間に北朝鮮から出てくる脱北者の流れがほぼ止まった一方[49]、これらのキリスト教グループは、脱北者の脱出を支援する上で重要な役割を果たすことよくあるからです。DEV-0215 は、グループを標的にして脱北者の組織を支援している人を見つけるため、ルアーとしてキリスト教カンファレンスに関する偽の文書を韓国語話者向けに作成しました。

最後に、国家レベルのグループである OSMIUM は、過去に北朝鮮を支援したことのある組織も含め、国際支援団体に対して年間を通じて安定した関心を示しました。北朝鮮は一般に国外からの援助を敬遠していますが、特に COVID-19 の発生以来[50]、北朝鮮は援助の申し出を受け入れることを検討しています。ただし、国外の支援者を入国させることによる安全保障面での悪影響を警戒しています。北朝鮮は、世界中の援助団体のネットワークに侵入し、自国でそのような援助を受け入れるかどうかを判断する可能性があります。

実用的なインサイト

1. 北朝鮮の国家レベルのアクターは、熟練していて容赦なく独創的ですが、組織はそれらの攻撃から防御することができます。
2. 成功率の高い攻撃でも、2 要素認証の使用や、想環境内で不明なユーザーからの添付ファイルを開かないなど、基本的なサイバー衛生によって阻止できます。

詳しい情報のリンク

- 北朝鮮の脅威アクターが H0lyGh0st ランサムウェアを使って中小企業を標的とする | Microsoft Threat Intelligence Center (MSTIC)、Microsoft Digital Security Unit (DSU)

北朝鮮の専門家の間では、北朝鮮政府が本気で公式声明を出しているのか、効果があるように見せているのかについて、長い間議論されてきました。北朝鮮が発表した優先事項とサイバー攻撃が合致していることは、北朝鮮が目標について公表するときに語る内容が意味する信念を実証しています。

サイバー傭兵がサイバースペースの安定性を脅かす

クライアント (政府であることもよくあります) がネットワーク、コンピューター、電話、インターネット接続デバイスに侵入するためのツール、手法、サービスを開発および販売している民間企業の業界は増えています。国家レベルのアクターにとっての資産であるこれらのエンティティは多くの場合、抗議活動家、人権支持者、ジャーナリスト、市民活動支援者、その他の民間人を危険にさらしています。マイクロソフトは、サイバー傭兵や攻撃アクター企業と呼んでいます。

民間企業がサイバー兵器を作成して販売している世界は、消費者、あらゆる規模の企業、政府にとって危険な世界となります。これらの攻撃的なツールは、優れたガバナンスと民主主義の規範および価値に矛盾した方法で使用される可能性があります。マイクロソフトは、人権の保護は基本的な義務であると考えており、世界中の「サービスとしての監視」を抑制することにより真剣に受け止めています。

マイクロソフトは、民主主義政権か権威主義政権かを問わず、特定の国家レベルのアクターが「サービスとしての監視」テクノロジの開発または使用をアウトソーシングしていると推測しています。そのようにして説明責任と監督を回避し、ネイティブな開発が困難な機能を獲得しています。

> これらのサイバー兵器は、国家が単独では開発できない監視機能を提供しています。

サイバー傭兵が活動している市場は不透明です。それにもかかわらず、それらのグループがゼロデイ攻撃を使用して、サービスとしての監視を実現していることが観察され続けています。被害者とのやり取りがまったく必要なゼロクリック攻撃も利用されています。

マイクロソフトは最近、KNOTWEED (DSIRF と呼ばれるオーストリアを拠点とする PSOA) というヨーロッパの攻撃アクター企業について発表しました。複数のニュース報道が、同社を、Subzero というマルウェア ツールセットの開発および販売の試みと結びつけました。[51] 被害者には、オーストリア、英国、パナマなどの国の法律事務所、銀行、戦略的コンサルタント会社が含まれています。[52]

このような攻撃用監視機能は、防衛機関と情報局によって作成された極秘の機能ではなくなりましたが、企業や個人に商品として提供されるようになりました。サイバー兵器の規制制度を、輸出管理以外にも適用する必要があります。これらのサイバー兵器の影響は壊滅的なものになる可能性があります。

サイバー傭兵が製品やサービスの脆弱性を悪用すると、コンピューティング エコシステム全体が危険にさらされます。脆弱性が公に特定されると、企業にとって、広範な攻撃が起きる前に保護をリリースする点で時間との争いが始まります (脆弱性の悪用に関する前述の説明をつ参照してください)。これは、ソフトウェア サプライヤー (適切な修正プログラムを開発する必要がある) と製品の消費者 (直ちに修正プログラムを実装する必要がある) の両方にとって危険で困難なサイクルです。

サイバーセキュリティ テック アコード [53] (150 社以上のテクノロジ企業が集まった主要アライアンス) の創設メンバーであるマイクロソフトは、オンラインの攻撃活動に関与しないと約束しています。マイクロソフトはその約束と、この分野における人権に対する責任を守っています。また、技術面での混乱と法的課題に取り組むことで、サイバー傭兵のサービスによってもたらされる悪影響に光を当てており、悪用が発見された場合はお客様を保護し続けます。

> サイバー傭兵は、高度なマルウェアやさまざまな手法など、技術的に高度で広範に利用可能な「サービスとしての監視」機能を作成して提供しています。

政府の実用的なインサイト

1. 特に調達において、サービスとしての監視の透明性および監視要件を実装します。これには、米国がエンティティ リストに記載されている企業に関する商務省のリストで実施しているように、攻撃的なアクターを参入禁止にすることが含まれます。
2. この分野では、元従業員の雇用後の制限を確立します。
3. 「顧客を理解しつながりを強化する」義務を果たし、企業が人権に関する責任を果たすよう奨励することを目的とします。

詳しい情報のリンク

- KNOTWEED の解決 : ゼロデイ エクスプロイトを使ったヨーロッパの攻撃アクター企業 | Microsoft Threat Intelligence Center (MSTIC), Microsoft Security Response Center (MSRC), RiskIQ (Microsoft Defender 脅威インテリジェンス)
- サイバー兵器企業との闘いを続ける | Microsoft On the Issues

サイバースペースにおける平和と安全のためにサイバーセキュリティ規範を運用化する

人権を優先して、オンラインでの向こう見ずな行動から人々を保護する一貫したグローバル フレームワークを早急に必要です。ウクライナで進行中の戦争により、これまで以上にこのことが明確になりました。世界的な戦略的取り組みに加えて、各国政府は今すぐ行動して、ポジティブな影響を与えることができます。

5 年前、マイクロソフトは「デジタル ジュネーブ会議」を呼びかけ、オンラインの平和と安全を守るために業界間の責任と義務を推進しました。サイバースペースは、国家間の対立と競争が行われている、予想が困難な領域として明確に浮上しており、平穏な時期でも攻撃がより一般的になっています。

今日でもこのような枠組みがどうしても必要であることが、ロシアによる侵攻の一環として行われているウクライナに対するロシアのサイバー攻撃によって明らかになっています。この戦争では、以前の認識とは大きく異なる新たな最前線ができました。

サイバースペースを安定させるには、グローバル ガバナンス機関の強化と見直しを行い、目的に合った機関とする必要があります。サイバースペースは、他の分野とは根本的に異なります。国境がなく、人工的であり、大部分は民間企業が管理しています。これは、製品とサービスのセキュリティだけでなく、より広範なデジタル エコシステムに対する大きな責任を、テクノロジ業界が負っていることを意味します。あらゆる面で注目すべき進展が見られましたが、課題は劇的に増えています。

サイバースペースのセキュリティを守るための集団としての取り組みを倍加させなければなりません。オンラインで期待される権利と自由を奪い取ることはできません。この課題に対処するのは簡単ではありませんが、悪意のあるアクターは AI を使って、偽情報を利用し、できたばかりのメタバースを弱体化させる方法を見つけることにより、次に攻撃を行う方法と場所を計画しています。人権支持者、テクノロジ業界、権利を尊重する政府は、安心かつ安全なオンライン環境を作るための肯定的なビジョンに向けて協力しなければなりません。今後の道のりは長いものですが、サイバーセキュリティ エコシステムを改善するために政府が今すぐできることがあります。

- 特定に関する規範、法律、影響を引き合いに出します。過去 5 年間の主な改善点の 1 つは、政府によるサイバー攻撃の特定のスピードと調整です。これらの声明では、告発と処罰だけでなく、国際的な法律や規範が侵害されていることや、国際社会からの期待の認識を強化するためにどのように形の影響を被るかについて強調する必要があります。
- オンラインにおける国際法の解釈を明確化します。各国政府は、国際法がオンラインに適用されることに同意していますが、具体的なインスタンスにどう適用するかについては疑問が残ります。これは特にウクライナ侵攻の影響と大きく関連しています。政府は、国際法に基づく義務をどのように理解しているかを示すことによって、期待値を設定して、誤解を回避し、信頼を築くための長い道のりを踏み出すことができます。
- 他のステークホルダーに相談します。国際フォーラムでは、堅牢なマルチステークホルダーの関与を促す最善の方法を発見し続けています。各国政府は、どうしても必要な専門知識を持つ人たちとの会話からメリットが得られるように、マルチステークホルダー コミュニティ（特にテクノロジ業界）に相談することにより、情報に基づく対話を支援できます。
- サイバースペースでの責任ある国家の行動を支えるため、常任団体を設立します。オンラインでの責任ある国家の行動を推進するための国際外交フォーラムの仕事がこれほど重要になったことはありませんでした。サイバースペースを対立の領域として扱う恒久的な UN メカニズムが必要なことは明らかです。
- 進化し続ける脅威のための新しい規範を定義します。サイバースペースの脅威は、テクノロジのイノベーションとともに絶えず進化しています。国際的な規範はテクノロジ ニュートラルでなければなりませんが、脅威の状況の変化とテクノロジの使い方に基づいて更新と廃止が必要になります。現在でも、既存の国際的枠組みに素材するギャップが悪用されています。ソフトウェアの更新プロセスと同様、現在保護されていないデジタル エコシステムを支えるコア プロセスを国家が明示的に保護する必要があります。さらに、特定の領域には追加の保護が必要です。たとえば、パンデミックの最中にわかったように、医療を保護するための規範が不可欠です。

国家レベルのアクターと攻撃はボリュームと巧妙さを増しており、受け入れがたい状況になっています。

直ちに対処が必要です。サイバーセキュリティ エコシステムをすぐに改善するため、政府が今すぐできることがあります。たとえば、サイバースペースにおける国家の行動に関して合意された規範と規則を実践し、幅広いマルチステークホルダー コミュニティと協力して新たなギャップに対処することなどです。

国家レベルのサイバー攻撃の差し迫った課題に対処するには、多国間の機関を考え直す必要があります。

詳しい情報のリンク

- 見直しのタイミング：強力でグローバルなサイバーセキュリティ対応の必要性 | Microsoft On the Issues
- 医療を標的とするサイバー攻撃を阻止する | Microsoft On the Issues
- 国連におけるサイバー外交の新しい章が始まる | Microsoft On the Issues

巻末注

1. https://www.microsoft.com/en-us/cybersecurity/content-hub/cloud-security
2. https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/
3. この章で説明されている重要インフラは、大統領政策命令 21 (PPD-21)、重要インフラのセキュリティとレジリエンス (2013 年 2 月) によって定義されています。
4. https://www.microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/
5. https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/
6. https://www.microsoft.com/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/
7. https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-passwordless-authentication
8. https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35211
9. https://pitstop.manageengine.com/portal/en/community/topic/adselfservice-plus-6114-security-fix-release
10. https://reliefweb.int/report/ukraine/unicef-ukraine-humanitarian-situation-report-no-13-10-17-may-2022
11. https://news.un.org/en/story/2022/06/1119672
12. https://zetter.substack.com/p/dozens-of-computers-in-ukraine-wiped?s=r ; https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
13. https://www.cnn.com/2022/03/14/economy/china-jan-feb-economy-challenges-ahead-intl-hnk/index.html
14. https://www.wsj.com/articles/russias-vladimir-putin-meets-with-chinese-leader-xi-jinping-in-beijing-11643966743
15. https://www.washingtonpost.com/world/2022/04/01/china-eu-summit/
16. https://twitter.com/MoNDefense
17. https://news.usni.org/2022/01/24/2-u-s-aircraft-carriers-now-in-south-china-sea-as-chinese-air-force-flies-39-aircraft-near-taiwan
18. https://ec.europa.eu/trade/policy/in-focus/eu-china-agreement/; https://www.usnews.com/news/world/articles/2022-02-28/eu-plans-summit-with-china-on-april-1-to-address-tensions
19. https://www.wsj.com/articles/u-s-on-sidelines-as-china-and-other-asia-pacific-nations-launch-trade-pact-11641038401
20. https://greenfdc.org/chinas-two-sessions-2022-what-it-means-for-economy-climate-biodiversity-green-finance-and-the-belt-and-road-initiative-bri/
21. https://www.cfr.org/global-conflict-tracker/conflict/territorial-disputes-south-china-sea
22. https://www.theguardian.com/world/2022/apr/30/the-china-solomons-security-deal-has-been-signed-time-to-move-on-from-megaphone-diplomacy
23. https://www.fmprc.gov.cn/eng/zxxx_662805/202205/t20220531_10694928.html
24. https://blogs.microsoft.com/on-the-issues/2021/12/06/cyberattacks-nickel-dcu-china/; https://www.microsoft.com/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe/
25. https://www.microsoft.com/security/blog/2022/04/12/tarrask-malware-uses-scheduled-tasks-for-defense-evasion/
26. https://attack.mitre.org/techniques/T1053/
27. https://www.microsoft.com/security/blog/2022/07/26/malicious-iis-extensions-quietly-open-persistent-backdoors-into-servers/
28. https://www.microsoft.com/security/blog/2021/02/11/web-shell-attacks-continue-to-rise/
29. https://www.timesofisrael.com/in-rare-criticism-of-irgc-rouhani-slams-anti-israel-slogans-on-test-missiles/; https://www.theguardian.com/world/2017/may/05/iran-president-hassan-rouhani-nuclear-agreement-sabotaged; https://d2071andvip0wj.cloudfront.net/184-iran-s-priorities-in-a-turbulent-middle-east_1.pdf; https://www.aljazeera.com/news/2016/3/9/iran-launches-ballistic-missiles-during-military-drill; https://www.usatoday.com/story/news/world/2015/04/25/iran-yemen-weapons/26367493/; https://www.armscontrol.org/blog/ArmsControlNow/2016-03-14/The-Iranian-Ballistic-Missile-Launches-That-Didnt-Happen; https://www.reuters.com/world/middle-east/iran-parliament-approves-most-raisi-nominees-hardline-cabinet-2021-08-25/;
30. https://www.reuters.com/world/middle-east/iran-parliament-approves-most-raisi-nominees-hardline-cabinet-2021-08-25/; https://www.france24.com/en/live-news/20210825-iran-s-parliament-approves-president-s-cabinet-choices

巻末注 (続き)

31. https://www.janes.com/defence-news/news-detail/iranian-irgc-consolidates-primacy-inintelligence-operations; https://www.proofpoint.com/us/blog/threat-insight/badblood-ta453-targets-us-and-israeli-medical-research-personnel-credential; https://miburo.substack.com/p/iran-disinfo-privatized?s=r.
32. https://www.reuters.com/business/energy/iran-says-israel-us-likely-behind-cyberattack-gas-stations-2021-10-30/
33. https://www.tasnimnews.com/en/news/2021/11/05/2602361/us-military-action-off-the-table-iranian-general
34. 特に、ProxyShell の脆弱性に対する Exchange Server の修正プログラム (CVE-2021-26855、CVE-2021-26857、CVE-2021-26858、CVE-2021-27065、CVE-2021-34473)。さらに、Fortinet FortiOS SSL VPN アプライアンスには必ず脆弱性の修正プログラムを適用してください。
35. https://docs.microsoft.com/en-us/microsoft-365/commerce/manage-partners?view=o365-worldwide
36. https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/
37. https://www.microsoft.com/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/
38. https://www.secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign
39. https://www.microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/
40. https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/manage-updates-baselines-microsoft-defender-antivirus?view=o365-worldwide
41. https://docs.microsoft.com/microsoft-365/security/defender-endpoint/cloud-protection-microsoft-defender-antivirus
42. https://docs.microsoft.com/microsoft-365/commerce/manage-partners?view=o365-worldwide
43. https://www.marketwatch.com/story/kim-jong-un-calls-for-improved-living-conditions-in-north-korea-01633920099
https://www.bbc.com/news/world-asia-59845636
https://kcnawatch.org/newstream/1650963237-449932111/respected-comrade-kim-jong-un-makes-speech-at-military-parade-held-in-celebration-of-90th-founding-anniversary-of-kpra/
44. https://www.theguardian.com/world/2021/aug/06/north-korea-homes-wreckeddamaged-and-and-bridges-washed-away-in-floods
45. https://www.reuters.com/world/asia-pacific/nkorea-mobilises-office-workers-fight-drought-amid-food-shortages-2022-05-04/
46. https://www.washingtonpost.com/world/asia_pacific/north-korea-kim-pandemic/2021/09/08/31adfd74-ff53-11eb-87e0-7e07bd9ce270_story.html
47. https://news.yahoo.com/china-halts-freight-train-traffic-102451425.html
48. https://www.cnn.com/2022/05/11/asia/north-korea-covid-omicron-coronavirus-intl-hnk/index.html
49. https://www.csis.org/analysis/number-north-korean-defectors-drops-lowest-level-two-decades
50. https://www.aljazeera.com/economy/2022/5/20/north-korea-shuns-outside-help-as-covid-catastrophe-looms
51. Jan-Philipp Hein、「In the mystery of creepy spy software, the trail leads via Wirecard to the Kremlin」、FOCUS Online、(2022 年)、https://www.focus.de/politik/vorab-aus-dem-focus-volle-kontrolle-ueber-zielcomputer-das-raetsel-um-die-spionage-app-fuehrt-ueber-wirecard-zu-putin_id_24442733.html; Sugar Mizzy、「We unveil the “Subzero” state trojan from Austria」、Europe-cities (2021 年)、https://europe-cities.com/2021/12/17/we-unveil-the-subzero-state-trojan-from-austria/; Andre Meister、「We unveil the state Trojan “Subzero” from Austria」、Netzpolitik.org (2022 年)、https://netzpolitik.org/2021/dsirf-wir-enthuellen-den-staatstrojaner-subzero-aus-oesterreich。
52. テクニカル ブログに記載されているように、ある国で標的が特定されたことは、必ずしも DSIRF の顧客が同じ国を拠点としていることを意味するわけではありません。国をまたいだ標的化が一般的になっているためです。
53. ホーム | サイバーセキュリティ テック アコード (cybertechaccord.org)

デバイスとインフラ

デジタル トランスフォーメーションの加速により、デジタル インフラのセキュリティがこれまで以上に重要になっています。

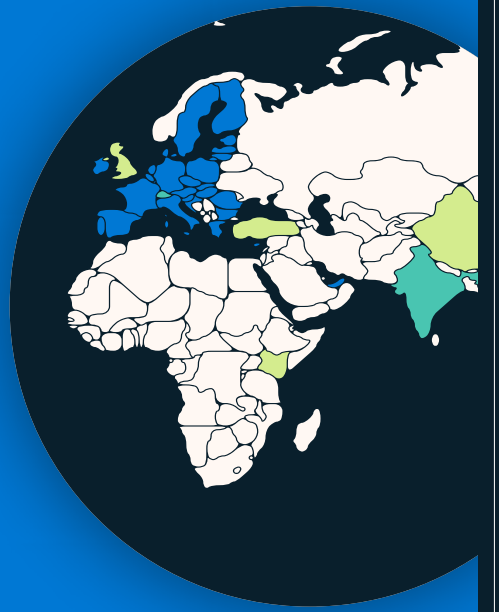
デバイスと

インフラの概要

パンデミックに加えて、デジタル トランスフォーメーションを加速させた 1 つの要素としてあらゆる種類のインターネット接続デバイスが急速に導入されたため、デジタル世界の攻撃対象領域が大幅に増加しました。

サイバー犯罪者と国家はすかさずそれを巧みに利用しています。近年、IT ハードウェアとソフトウェアのセキュリティは高まっていますが、モノのインターネット (IoT) のセキュリティと運用技術 (OT) デバイスのセキュリティは歩調が合っていません。脅威アクターは、それらのデバイスを悪用することにより、ネットワークへのアクセスを確立して侵入を拡大し、サプライ チェーン内での足場を確立したり、標的組織の OT 運用を中断したりしています。

世界中の政府は、IoT と OT のセキュリティを高めることで重要インフラの保護に移行しています。

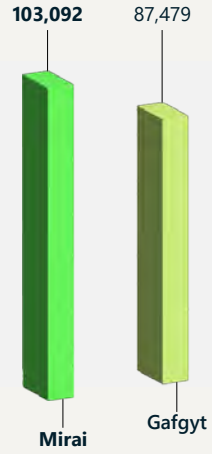


詳しくは 59 ページをご覧ください

広範な採用を確実に行うには、一貫性と相互運用性の高いセキュリティ ポリシーをグローバルに展開する必要があります。

詳しくは 59 ページをご覧ください

サービスとしてのマルウェアは、インフラ、ユーティリティ、企業ネットワークの公開 IoT と OT に対する大規模な運用に移行しました。



詳しくは 63 ページをご覧ください

リモート管理デバイスに対する攻撃は増えており、2022 年 5 月には 1 億件を超える攻撃が発生しました。過去 1 年間で 5 倍の増加です。

詳しくは 62 ページをご覧ください

攻撃者は、IoT デバイス ファームウェアの脆弱性を利用して企業ネットワークに侵入し、壊滅的な攻撃を仕掛けることが増えています。

詳しくは 65 ページをご覧ください

分析対象のファームウェア イメージの 32% には、少なくとも 10 の既知の重大な脆弱性が含まれていました。

詳しくは 66 ページをご覧ください

はじめに

デジタル トランスフォーメーションが加速した結果、重要インフラやサイバー物理システムに対するサイバーセキュリティのリスクが高まっています。

この数年間で、デジタル環境は前例のない変化を遂げました。組織は進化しており、インテリジェント クラウドとインテリジェント エッジの両方から、コンピューティング機能の進歩を活用しています。パンデミックによって、企業は生き残るためにデジタル化を余儀なくされ、世界中の業界でインターネット接続デバイスを採用するペースが速まっています。その結果、デジタル環境の攻撃対象領域が急激に増加しています。

この急速な移行は、セキュリティ コミュニティの対応能力を上回っていました。過去 1 年間、従来の IT 機器から、運用技術 (OT) コントローラー、単純なモノのインターネット (IoT) センサーにいたるまで、組織のあらゆる部分でデバイスを悪用する脅威が観察されてきました。近年 IT 機器のセキュリティは強化されていますが、IoT のセキュリティと OT デバイスのセキュリティは歩調が合っていません。脅威アクターは、それらのデバイスを悪用することにより、ネットワークへのアクセスを確立して侵入を拡大したり、組織の OT 運用を中断したりしています。電力網に対するへの攻撃、OT 運用を妨げるランサムウェア攻撃、持続性を高めるために利用される IoT ルーター、ファームウェアの脆弱性を標的とする攻撃が観察されています。

IoT と OT の脆弱性が広範囲に存在することはすべての組織にとって大きな課題となりますが、脅威アクターは重要なサービスを停止するこには大きな影響があることを学習したため、重要インフラがさらされているリスクが高まっています。Colonial Pipeline Company における 2021 年のランサムウェア攻撃は、犯罪者が身代金支払いの可能性を上げるためために重要なサービスをどのように中断させる可能性があるかを示しています。さらに、ウクライナに対するロシアのサイバー攻撃が示すように、国家によっては、重要インフラに対するサイバー攻撃を、軍事目標を達成するための許容可能な破壊行為と見ています。

しかし、今後の展望には希望があります。政策立案者とネットワーク防御者は、信頼できる IoT や OT デバイスなど、重要インフラのサイバーセキュリティを改善する役割を果たしています。政策立案者は、重要インフラとデバイスのサイバーセキュリティに対する社会的な信頼を築くため、法律や規制の策定を急いでいます。

マイクロソフトは世界中の政府と連携してサイバーセキュリティを強化する機会を捉えており、さらなる関与も喜んで受け入れます。しかし、一貫性のない要件、特注要件、あるいは複雑な要件が意図しない影響をもたらす可能性があることを懸念しています。たとえば、少数のセキュリティ リソースを重複する複数の認定に準拠するために流用することで、セキュリティが低下する場合があります。

セキュリティ運用の観点からは、ネットワーク防御者は、組織の IoT/OT セキュリティ対策を改善するために複数のアプローチを取っています。1 つのアプローチは、IoT および OT デバイスの継続的な監視を実装する方法です。もう 1 つは、「シフト レフト」です。これは、IoT および OT デバイス自体が持つ優れたサイバーセキュリティ対策を要求して実装することです。3 番目のアプローチは、IT と OT の両方のネットワークにまたがるセキュリティ監視ソリューションを実装する方法です。この包括的なアプローチには、OT と IT の間にある「サイロを壊す」など、重要な組織プロセスに貢献するという大きなメリットがあります。この結果、組織はビジネス目標を達成しながら、強化されたセキュリティ対策を実現できるようになります。

Michal Braverman-Blumenstyk
コーポレート バイス プレジデント、最高技術責任者、クラウドおよび AI セキュリティ

重要インフラのセキュリティとレジリエンスを高めるために行動している政府

世界中の政府は、重要インフラのサイバーセキュリティ リスクを管理するための政策を策定し、進化させています。その多くは、IoT および OT デバイスのセキュリティを高めるためのポリシーも制定しています。世界的な政策イニシアチブの波の高まりによって、サイバーセキュリティを強化する大きな機会が生まれているだけでなく、エコシステム全体のステークホルダーに大きな課題ももたらされています。

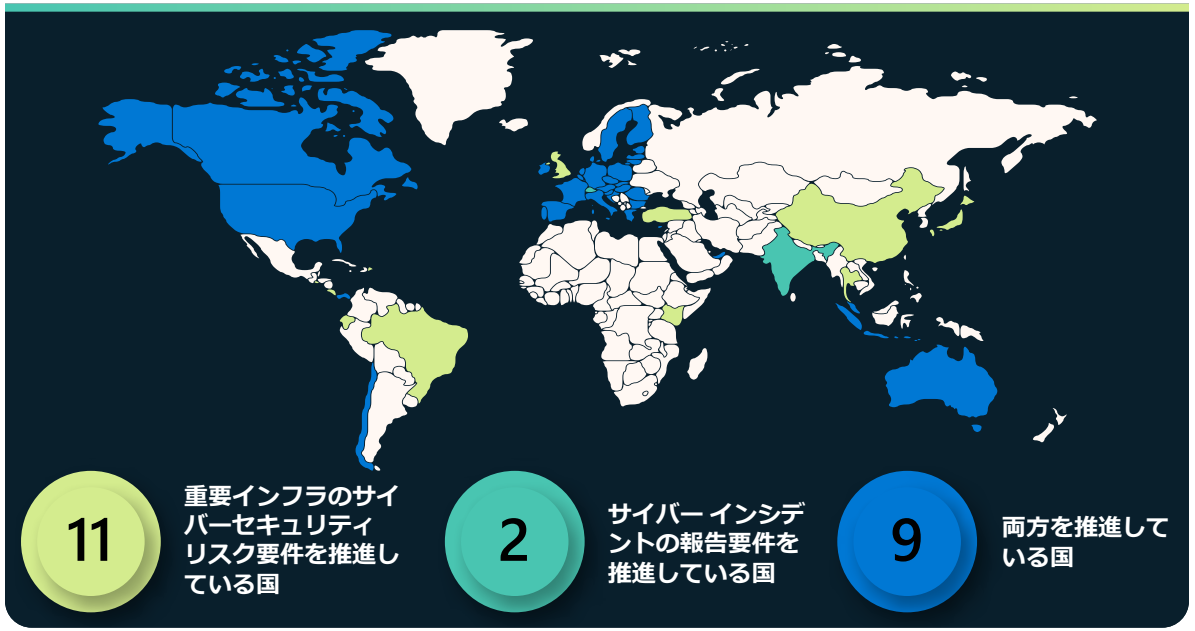
重要インフラのサイバーリスクを管理するための包括的なビジョンを策定することはとても重要ですが、特にテクノロジとグローバル サプライヤー間の相互接続の程度、テクノロジの利用範囲と関連するリスク、短期的戦略と長期的戦略の両方に投資する必要性を考えると、複雑なことでもあります。反復的な学習と改善を推し進め、分野を超えたグローバルな相互運用性をサポートするポリシーを効果的に調査することで、複雑さに対処し、よりセキュリティ意識の高いデジタル トランスフォーメーションを実現できます。しかし、法律へのアプローチが細分化されていると、規制要件が重複したり矛盾したりする可能性があります。これはリソースに影響を及ぼし、最終的にはセキュリティ目標を満たせない可能性があります。たとえば、組織はリソースをイノベーションとセキュリティから形式主義的なコンプライアンス行動に転用する可能性があります。

マイクロソフトは、効果的な重要インフラのサイバーセキュリティ政策を追跡して、課題と機会についての理解を深め、集合的なリスク対策を強化する取り組みを支援する点で、世界中の政府との連携を模索しています。

重要インフラのサイバーセキュリティ リスク管理における政策の策定

昨年、オーストラリア、チリ、欧州連合 (EU)、日本、シンガポール、イギリス (UK)、米国などの複数の管轄区域が、分野を超えたサイバーセキュリティ要件または特定の分野に特化したサイバーセキュリティ要件を策定、更新、または導入しました。[1] このような政府の多く (およびインド[2] やスイス[3] などの他の国々) は、重要インフラおよび重要なサービス プロバイダーに対するサイバーセキュリティ インシデント レポートの要件を既に発行しているか策定しています。[4]

昨年、オーストラリア、EU、インドネシア、米国では注目すべき政策の進展がいくつか見られました。オーストラリアは、分野を超えた重要インフラのサイバーセキュリティ リスクを管理するため、2 つの法律を制定しました。それらの法律は、とりわけ、新たな重要インフラ分野に言及し、リスク管理計画の策定とサイバーセキュリティ インシデント報告を義務付け、重大インフラ オペレーターがインシデントに適切な対応を取る意思がないか対応できないと判断した場合に政府が介入できるようにしています。



EU は、2016 年の NIS 指令の更新に着手しました。この指令は、経済と社会機能にとって重要であると見なされているテクノロジ サービスおよび製品を規制するための、EU 加盟国にとっての枠組みを提供していました。NIS 2 案には、重要なデジタル インフラの新しいカテゴリを作成して、サイバー インシデント レポートの要件を引き上げ、追加のサイバーセキュリティ リスク管理要件を課すという改訂が含まれています。さらに、EU は、デジタル運用レジリエンス法 (DORA) の更新案を策定し、金融サービス分野で使用される情報通信テクノロジに関する新しい要件を作成しました。

5 月、インドネシアは重要な情報インフラ (「IIV」) の保護に関する大統領規制を発令しました。これは、2024 年 5 月に発効し、特にエネルギー、運輸、金融、医療などの分野が対象となっています。この規制におけるインドネシアの目的は、IIV の導入の継続性を保護し、サイバー攻撃を防止して、サイバー インシデントに対応する備えを強化することです。IIV プロバイダーは、安全で信頼性の高い保護を実施して、効果的なサイバー リスク管理を実装し、対応する行政機関にサイバー リスクの結果を報告する責任を負うことになります。この規制には、24 時間以内にサイバー インシデントを報告するという要件も含まれています。

重要インフラのセキュリティとレジリエンスを高めるために行動している政府

(続き)

米国議会は、サイバーセキュリティおよびインフラ安全保障庁 (CISA) が重要インフラ事業者からのサイバーインシデント報告を要求する規制を発行することを承認した法律を可決し、米国運輸保安局 (TSA) は運輸部門で新しい分野固有のサイバーセキュリティ要件を発行しました。2021 年、TSA は、Colonial Pipeline Company におけるランサムウェア攻撃に応じて、有害液体および天然ガス パイプライン事業者に 2 つのセキュリティ指令を発布しました。

- 最初の指令では、事業者はサイバーセキュリティ コーディネーターを指名し、12 時間以内にサイバー インシデントを報告して、システムの脆弱性評価を実施することが求められていました。
- 2022 年に改訂された 2 つ目の指令では、ランサムウェア攻撃やその他の既知の脅威から IT および OT システムを保護するための具体的な緩和策を実施すること、30 日以内にサイバーセキュリティの不測の事態と対応計画を策定して実施すること、毎年のサイバーセキュリティ アーキテクチャ設計レビューを受けることが求められていました。

TSA は、パイプラインに関するその規制に基づいて、2021 年に 2 つの追加のセキュリティ指令を発布し、貨物鉄道、旅客鉄道運送会社、または鉄道輸送システムにサイバーセキュリティ要件を公布しました。この指令では、対象となる事業者がサイバーセキュリティ コーディネーターを指名すること、24 時間以内にサイバーセキュリティ インシデントを報告すること、サイバーセキュリティ インシデント対応計画を策定して実施すること、サイバーセキュリティの脆弱性評価を完了することが求められていました。TSA は同時に、航空安全プログラムも更新することも発表し、空港および航空会社の事業者が最初の 2 つの規定を守り、24 時間以内にコーディネーターを指名することと、インシデントを報告することが求められました。

IoT および OT デバイスのセキュリティに関する政策の策定

数十か国の政府は、IoT デバイスや OT デバイスを含む情報通信技術 (ICT) 製品およびサービスのサイバーセキュリティを推進するための要件の策定に積極的に取り組んでいます。ICT 製品およびサービスの文脈において最も懸念されるのは、ソフトウェア サプライ チェーンのセキュリティと IoT セキュリティです。

- 欧州委員会は、サイバー レジリエンス法を発案しました。これは、スタンドアロンのソフトウェアとコネクテッド デバイス、および関連サービスのサイバーセキュリティ要件を制定するものです。[5] ソフトウェアベンダーの関連プラクティスには、安全なソフトウェア開発ライフサイクル[6] の活用、ソフトウェア部品表の提供などが含まれています。[7] コネクテッド デバイスには新しいセキュリティ要件が適用され、すべての製造業者には、リリースされる製品の組織的な脆弱性開示[8] を管理する責任があります。

さらに、政策立案者は、IoT デバイスとネットワーク接続された OT デバイスの急増が続くことにも注目しています。

- 英国では、製品セキュリティおよび電気通信インフラス法案により、スマート テレビなどの消費者向け接続可能製品のメーカーに、サイバー犯罪者の標的となりやすい既定のパスワードの使用を停止すること、脆弱性開示ポリシーを確立すること (セキュリティ上の欠陥に関する通知を受け取る方法など)、セキュリティ更新プログラムが提供される最小期間について透明性を確保することが求められます。[9]
- EU では、無線機器指令への委任法など、複数の立法手段を通じて新たなセキュリティ基準や要件が執行されています。これらは、ワイヤレス デバイスに適用され、ネットワークのレジリエンスを高め、消費者のプライバシーを保護し、金融詐欺のリスクを軽減することを目指しています。[10] さらに、2019 年 EU サイバーセキュリティ法[12] が発効した結果、現在開発中のクラウド認証スキーム[11] を使用することが求められる場合があります。

一貫性の必要性

多くの場合、地域、業界、テクノロジ、運用リスク管理の各分野にわたるさまざまな活動が同時に進行するため、ガイダンスを利用したりコンプライアンスを実証したりしようとする組織では範囲、要件、複雑さの重複や矛盾が生じる可能性があります。IoT の定義が普遍的に受け入れられていない場合、IoT および OT デバイスの規制にとって範囲は特に大きな課題となります。上記の例は、「コネクテッド製品と関連サービス」、「消費者向け接続可能製品」、「ワイヤレス デバイス」に適用される可能性があります。同時に、多くの政府は、組織と製品が現在の要件、新しい要件、進化した要件を満たしているかどうかやどのように満たしているかをよく理解するため、より堅牢な評価体制を導入しようとしています。このような傾向が合わさると、複雑さが増します。幸い、EU のサイバー レジリエンス法の協議中に提起された質問により、新しい規制が既存のサイバーセキュリティ規制とどのように相互作用するかが検討され、サイバーセキュリティ要件の競合を回避する意思があることが示されました。

リスクベースかつ結果またはプロセス重視 (実装固有なものではなく) の反復的なアプローチは、サイバーセキュリティの向上と継続的な改善を促す可能性があります。同様に、複数の業界、地域、および政策分野で相互運用性を実現することに重点を置くことにより、相互接続されたグローバル サプライ チェーン全体でサイバーセキュリティを高めることができます。

重要インフラのセキュリティとレジリエンスを高めるために行動している政府

(続き)

地域、業界、トピックの分野をまたがる開発では、重要インフラのサイバーセキュリティ ポリシーの複雑さがますます増してしています。この活動は、大きな機会とも大きな課題ともなります。政府の進め方は、将来のデジタル トランスフォーメーションとエコシステム全体のセキュリティにとって非常に重要です。

ソフトウェア サプライ チェーンのセキュリティとゼロ トラスト アーキテクチャにおけるエコシステム全体への投資を加速

サイバーセキュリティの向上に関する米国大統領令 (EO) 14028 は、自社およびエコシステム全体のサプライ チェーン セキュリティに投資し、お客様がゼロ トラストの目標を達成できるようにする、マイクロソフトの継続的な取り組みを後押ししています。

約 15 年前にマイクロソフトのセキュリティ開発ライフサイクルが一般リリースされてから、マイクロソフトは、ソフトウェア サプライ チェーンを強化するには学習とベスト プラクティスの共有が必要であると長い間考えてきました。

さらに、National Cybersecurity Center of Excellence と緊密に連携して、オンプレミスとクラウドの両方のテクノロジに適用されるゼロ トラスト アーキテクチャへのアプローチを実証し、ハイブリッドおよびマルチクラウド環境に対するフィッシング対策認証を実施する機能など、新製品の機能を確立しています。

現在マイクロソフトは、EO の要件だけではなく、ソフトウェア サプライ チェーンのセキュリティ要件に準拠していることを実証し、ソフトウェア部品表 (SBOM) の情報を次の 2 つの方法で提供しています。

1. まず、Windows、Linux、Mac、iOS、および Android プラットフォーム上のビルドをサポートする CI/CD パイプラインと簡単に統合できるように構築された、オープン ソース バージョンの SBOM 生成ツールを共有しています。[13]
2. 第 2 に、Supply Chain Integrity, Transparency, and Trust (SCITT) の業界標準の策定に貢献しています。これにより、EO のソフトウェア サプライ チェーン ガイダンスの結果生じた要件など、各種要件への準拠を実証する成果物を含む、検証可能なサプライ チェーン情報の交換を自動化することができます。

実用的なインサイト

① 国家レベルのサイバー攻撃の差し迫った課題に対処するには、多国間の機関を考え直す必要があります。

② 地域、業界、トピックの領域にまたがって一貫性と相互運用性を備えたサイバーセキュリティ ポリシーを策定します。

詳しい情報のリンク

- サイバーセキュリティ大統領令を支持するサプライ チェーン セキュリティへの継続的な投資 | Microsoft Tech Community
- US Government sets forth Zero Trust architecture strategy and requirements | マイクロソフト セキュリティ ブログ
- サイバー大統領令 | Microsoft Federal
- Supply Chain Integrity, Transparency, and Trust | github.com
- Implementing a Zero Trust Architecture | NCCoE (nist.gov)

IoT と OT の露出：傾向と攻撃

ますます密接につながるデジタル環境では、デバイスのオンライン化が急速に進むため、大規模なシステムと通信して、データを収集し、以前は見えなかった空間が見えるようになります。その結果、組織や脅威アクターにとってもチャンスとなります。サイバー犯罪ビジネスは数十億ドル規模の業界であり、リスクともなります。

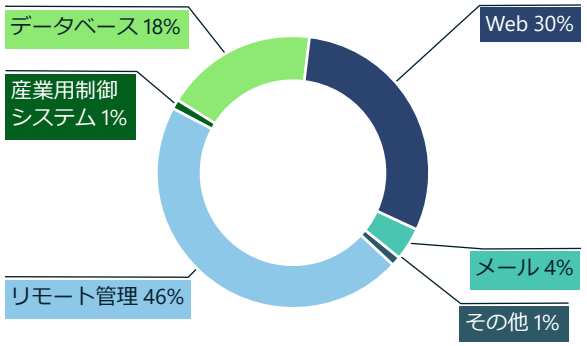
プリンターから Web カメラ、温度制御デバイス、ビル アクセス制御まで、IoT デバイスは、個人、組織、ネットワークに特有のセキュリティ リスクをもたらします。多くの組織の業務にとって非常に重要なものですが、責任とセキュリティ リスクがすぐに生じる可能性があります。ほぼすべての業界が IoT ソリューションを迅速に導入したため、攻撃ベクトルの数と組織の露出リスクが高まりました。

サービスとしてのマルウェアは、公共インフラや公益事業 (病院、石油ガス、送電網、運輸サービス、他の重要インフラなど) に加えて企業ネットワークに対する大規模な運用に移行しました。脅威アクターが運用環境と埋め込まれた IoT および OT デバイスの構成を調べて悪用するには、かなりの調査作業を行う必要があります。

IoT デバイスは、ネットワーク内のエントリ ポイントおよびピボット ポイントとして、独自のセキュリティ リスクをもたらします。何百万台もの IoT デバイスは、修正プログラムが適用されていないか、さらされています。

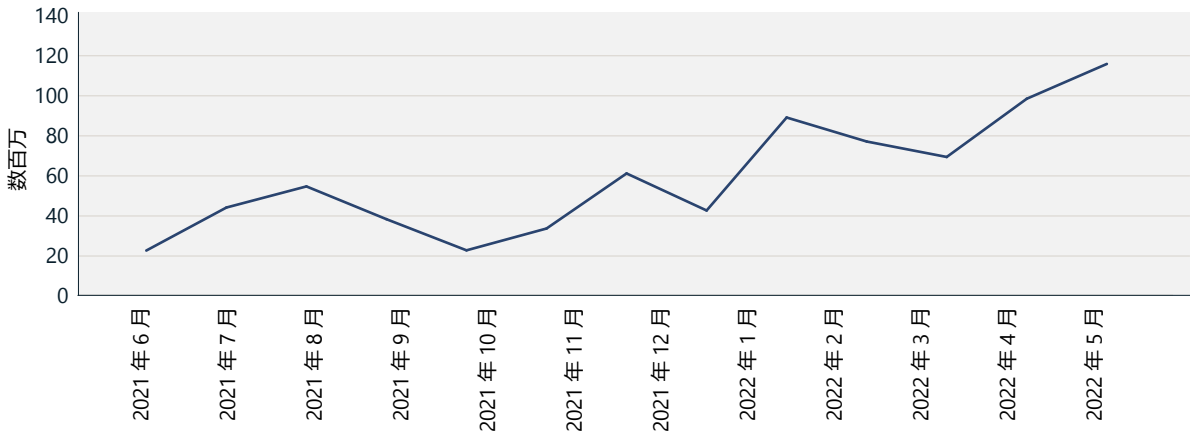
さらされたデバイスは、開いているネットワーク ポートでリッスンしているサービスを特定することにより、インターネット検索ツールを通じて検出できます。それらのポートは一般に、デバイスのリモート管理に使用されます。正しく保護されていない場合、権限のないユーザーがリモートでポートにアクセスできるため、企業ネットワークの別のレイヤーへのピボット ポイントとして、さらされた IoT デバイスを使用できます。カメラからルーター、サーモスタットまで、インターネットにさらされているデバイスの脆弱性を悪用しようとしている、さまざまな脅威アクターが観察されています。しかし、リスクが高いにもかかわらず、何百万台ものデバイスは修正プログラムが適用されていないか、さらされたままです。

IoT/OT における攻撃の種類の概要



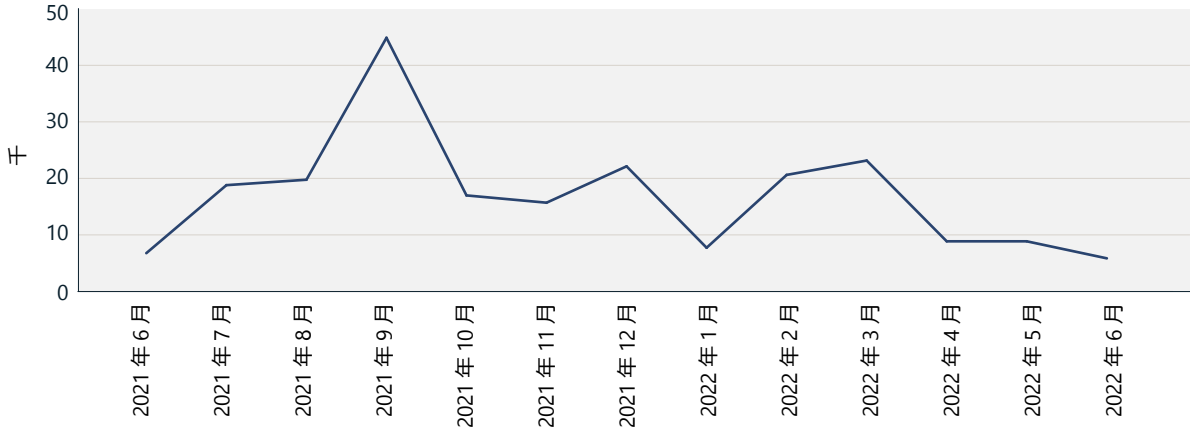
MSTIC センサー ネットワークを通じて観測された攻撃の種類。最も多く見られるのは、リモート管理デバイスに対する攻撃、Web 経由の攻撃、データベースへの攻撃 (ブルートフォースまたはエクスプロイト) でした。

リモート管理デバイスに対する攻撃



MSTIC センサー ネットワークから判明した、リモート管理ポートへの攻撃の増加。

IoT と OT に対する Web 攻撃



MSTIC センサー ネットワークから判明した、時間の経過に伴う Web 攻撃の量。Web に直接接続されているデバイスの数が減少するにつれて、攻撃者がそれらを調査する可能性は最終的に低くなります。

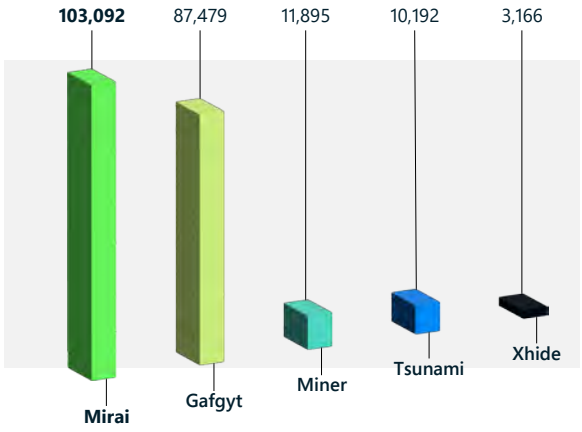
IoT と OT の露出：傾向と攻撃

(続き)

改良型マルウェア ユーティリティ

サイバー犯罪グループの進化に伴い、マルウェアの展開や標的の選択肢も進化しています。過去 1 年間で、Telnet などの一般的な IoT プロトコルに対する攻撃は大幅に低下 (場合によっては 60%) したことが観察されました。同時に、サイバー犯罪グループと国家レベルのアクターによってボットネットが転用されていました。「Mirai」などのマルウェアが残っていることは、それらの攻撃のモジュール性と既存の脅威の適応性を強調しています。

検出されたトップ IoT マルウェア



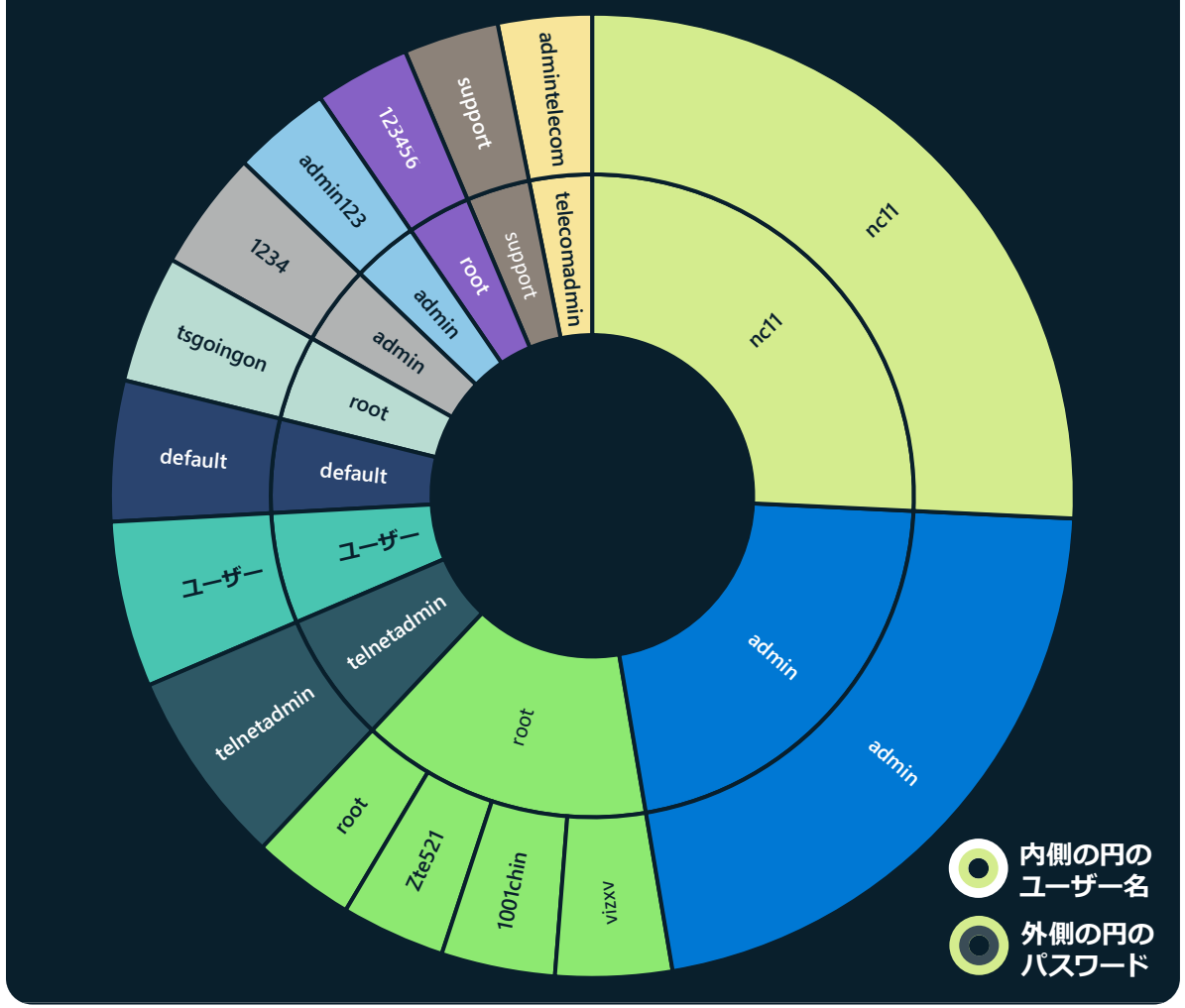
Mirai は進化し、インターネット プロトコル カメラ、防犯カメラのデジタル ビデオ レコーダー、ルーターなど、さまざまな IoT デバイスに感染するようになりました。攻撃ベクトルはレガシー セキュリティ コントロールを回避し、追加の脆弱性を利用して侵入を拡大するため、ネットワーク内のエンドポイントにとってリスクとなります。Mirai は何度も再設計され、その変異種はさまざまなアーキテクチャに適応し、既知の脆弱性とゼロデイ脆弱性の両方を利用して新しい攻撃ベクトルを侵害しています。

Mira の使用例は、過去 1 年間 32 ビットと 64 ビット両方の x86 CPU アーキテクチャで増加し、このマルウェアには国家レベルの犯罪グループによって急速に採用された新たな機能が与えられました。国家レベルの攻撃では、敵対国に対する分散型サービス拒否 (DDoS) 攻撃に既存のボットネットの新しい変異種が利用されるようになりました。

2022 年、IoT デバイスに対する攻撃からの収益が減少したことにより、いくつかの脅威アクター グループが、Log4j や Spring4Shell などの脆弱性を悪用して、サーバーなどのデバイスに悪意のあるペイロードを提供し、それらを感染させた後、DDoS 攻撃を行う大規模なボットネットとして利用しているのが観察されました。脆弱な IoT デバイスを標的とするよう設計されたマルウェアの改良型ユーティリティは、組織と国の両方にとって深刻な影響を及ぼします。侵入拡大によって、ネットワーク上の追加のペイロードや他のデバイスにバックドアを公開できるためです。

多くの産業制御システム プロトコルは監視されていないため、OT 固有の攻撃に対して脆弱です。これは、重要インフラのリスクが高まることを意味します。

45 日のセンサー信号において IoT/OT デバイスに見られるユーザー名 / パスワード ペアの相対的普及率



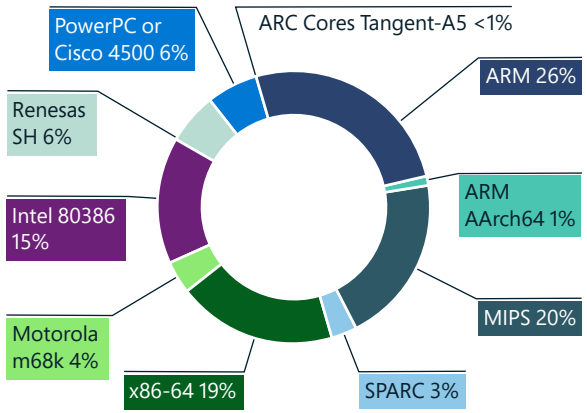
よくあるユーザー名とパスワードの組み合わせを使用すると、侵害のリスクが増加します。3,900 万を超える IoT および OT デバイスのサンプル サイズによると、同じユーザー名とパスワードを使用しているデバイスは 約 20% に相当します。

IoT と OT の露出：傾向と攻撃

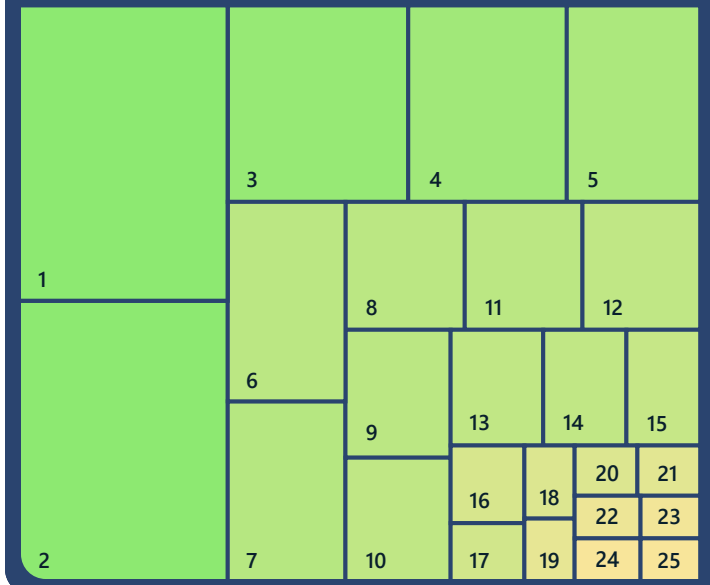
（続き）

脆弱な構成と既定の資格情報はやはりネットワークにリスクとなりますが、マイクロソフトは HTTP を利用している Web ベースのエクスプロイトを多く観察しています。レガシー ボットネットを使った Web ベース サービスに対する攻撃が増加しているのを観察しました。一方、インターネット上で開いている telnet ポートの数は減少したため、デバイスに対する歴史的なリスクとなったボットネットは関連性を失いつつあり、ネットワーク セキュリティにとってポジティブな兆候が見られます。開いている telnet ポートが減少したにもかかわらず、センサー ネットワークでは今でもボットネットが観察されています。

CPU アーキテクチャごとの IoT マルウェアの分布



産業制御システム プロトコルの普及率



1. EtherNet/IP
2. MODBUS
3. BACNet
4. Siemens S7
5. Profinet Real-Time
6. Profinet DCP
7. Siemens S7 Plus
8. CodeSys
9. Siemens WinCC Agent
10. EtherNet/IP O/O
11. Honeywell Control Data Access
12. MMS
13. IEC-60870
14. Honeywell FDA Diagnostics
15. Suitelink
16. DeltaV
17. GSM
18. DNP3
19. AMS
20. SRTP
21. TwinCat
22. Emerson Roc
23. Bently Nevada
24. Mitsubishi MELSEC
25. TriStation Tricon

マイクロソフトの観察によると、マルウェアの標的で最も多いのは ARM で実行されている IoT デバイスであり、MIPS、X86-64、Intel 80386 CPU が続きます。

産業制御システム プロトコルの脆弱性

マイクロソフトは、クラウドに接続されたセンサーから OT データを調べ、最も広く利用されている産業制御システム (ICS) プロトコルを明らかにしました。これらのプロトコルから、デバイスの性質と攻撃対象領域に関するインサイトが得られます。これは特に、重要インフラのセキュリティと関連性があります。主に次のようなことがわかりました。

1. ほとんどは独自プロトコルであるため、標準の IT 監視ツールには、これらのデバイスとプロトコルにおける十分なセキュリティ可視性が備わっていません。その結果、ネットワークは監視されないままのため、OT 固有の攻撃に対する脆弱性が高まります。
2. ベンダー固有のプロトコルにはさまざまな種類があります。これは、ベンダー固有のセキュリティ ソリューションがネットワーク全体を適切にカバーできないことを意味します。マイクロソフトは、ベンダーを問わないアプローチに優先順位を付け、さまざまなデバイスにセキュリティ カバレッジを提供しています。
3. 組織は、これらのプロトコルがネットワークからインターネットに直接公開されていないことを確認する必要があります。脆弱性が存在する可能性に加えて、これらのプロトコルは本来安全ではないため、このような露出は大きなセキュリティ リスクとなる可能性があります。

Mirai などのマルウェアは、新しい機能を開発することによって存続しています。サイバー犯罪グループと国家レベルのアクターによって採用されており、敵対国に対する DDoS 攻撃で既存のボットネットの新しい変異種が利用されています。

実用的なインサイト

1. 修正プログラムの適用、既定のパスワードの変更、既定の SSH ポートの変更よって、デバイスの堅牢性を高めます。
2. 不要なインターネット接続と開いているポートをなくし、ポートのブロック、リモート アクセスの拒否、VPN サービスの使用によりリモート アクセスを制限することにで、攻撃対象領域を減らします。
3. IoT/OT 対応のネットワーク検出および応答 (NDR) ソリューションとセキュリティ情報およびイベント管理 (SIEM)/ セキュリティ オーケストレーションおよび対応 (SOAR) ソリューションを使用して、よくわかっていないホストとの通信など、デバイスで異常な動作や許可されていない動作を監視します。
4. ネットワークを分割し、攻撃者が最初の侵入後に侵入を拡大して資産を侵害する可能性を減らします。IoT デバイスと OT ネットワークは、ファイアウォールを通じて、企業の IT ネットワークから分離する必要があります。
5. ICS プロトコルをインターネットに直接公開しないようにします。

サプライ チェーンとファームウェアのハッキング

ほぼすべてのインターネット接続デバイスにはファームウェアがあります。デバイスのハードウェアまたは回路基板に埋め込まれたソフトウェアです。過去数年間、壊滅的な攻撃を仕掛けるためファームウェアが標的になった事例が増えました。ファームウェアは今後も脅威アクターにとって重要な標的となると考えられるため、組織はファームウェアをハッキングから保護する必要があります。

ファームウェアは、ネットワークへの接続やデータの保存など、デバイスの主な機能を担当します。企業で使用されているルーター、カメラ、テレビ、その他のデバイス (IoT) のほか、重要インフラで使用されている産業制御機器 (OT) にもファームウェアが搭載されています。これまで、ファームウェアはセキュリティで保護されていないコードを使って記述されてきたため、デバイスを乗っ取ったり、悪意のあるコードをファームウェアに挿入したりするための悪用できる大きな脆弱性が生じていました。

サプライ チェーンの場合、このリスクはさらに高まります。ほとんどのデバイスは、多数のメーカーやオープン ソース ライブラリによるソフトウェアおよびハードウェア コンポーネントを使用して構築されています。多くの場合、デバイス オペレーターは、ネットワーク上のデバイスのサプライ チェーン リスクを評価する際、ハードウェアとソフトウェアの部品表 (H/SBOM) を把握していません。2020 年 6 月、多くのメーカーが利用しているネットワーク スタックに、消費者向け機器および産業機器の分野の数百万台もの IoT デバイスに影響を与える脆弱性が公開されました。[14] ネットワーク スタックは他のベンダーによってリブランディングされていることがあるため、デバイスに脆弱性が存在するという兆候はありませんでした。IoT/OT デバイスのこのようなソフトウェアとハードウェアのサプライ チェーンを標的にすることで組織を侵害している、悪意のあるアクターの脅威が増えています。

ファームウェア更新プロセスはデバイスによって大きく異なり、実行の複雑さとロジスティクス面の課題が更新頻度に影響を及ぼしています。デバイスが最新のファームウェアを実行しているかどうかを判断することは必ずしも可能ではないため、セキュリティ担当者が IoT および OT デバイスのセキュリティ対策を監視し、確実に行うことは困難です。さらに、デバイスによっては、ユーザーによる検証なしで更新できるようにするため、ファームウェアが暗号化されていません。これらの弱点によって、製造および流通チェーン全体でデバイスに対してサプライ チェーン攻撃が行われる可能性がさらに高まります。

これらの脅威に対処するため、マイクロソフトは、サプライ チェーンのさまざまな段階を通過するファームウェアのセキュリティと整合性を確保すること、attesting では、取り込み時または途中で改ざんされていないことを常に保証することに対して、多額の投資を行っています。この結果、マイクロソフトは各パイプライン セグメント間の信頼を検証し、お客様に出荷するすべてのコンポーネントに対して、認定済みかつ証明可能なエンド ツーエンドの保護チェーンを提供することができます。また、企業および OT ネットワーク上のすべてのデバイスで、チップからクラウドまでカバーしたこのようなセキュリティを実現するため、パートナーと協力しています。

「ICT インフラ サプライヤーは、単一の攻撃で広範なレプリケーションが可能になるため、標的となる事例が増えています。同時に、サプライ チェーンのセキュリティと回復性に関する法律、規制、お客様の要求は世界中で増加しており、多くの場合、要件とのずれがあります。

ソリューションはパートナーシップです。マイクロソフトは、サプライヤーや世界中の政府とともに、サプライ チェーン エコシステム全体にわたるセキュリティに取り組んでおり、お客様や規制当局からの要求を上回っています。これを実現するため、サプライ チェーン全体に柔軟に展開されるセキュリティと運用上の回復性に対する包括的なアプローチを推進しています。

設計からデバイス運用までファームウェアの整合性を推進することが、マイクロソフトの共同アプローチの鍵となります。サプライヤーの SDL プロセスを確保し、信頼できるイノベーションのハードウェア ルートを展開することは、マイクロソフトがサプライ チェーンの整合性を「搭載する」方法の例です。

マイクロソフトのコミュニティでは、新しい改ざん防止技術と暗号メカニズムに関する共同研究開発を活用し、継続的な監視と異常検出が組み合わされています。同時に、マイクロソフトは、サプライ チェーンの攻撃対象領域としての魅力を最小限に抑えるよう取り組んでいます。」

Edna Conway、
バイス プレジデント、セキュリティ & リスク担当責任者、クラウド インフラ

脚光を浴びるファームウェアの脆弱性

攻撃者は、IoT デバイス ファームウェアの脆弱性を利用して企業ネットワークに侵入することが増えています。XDR エージェントを使用して弱点を特定する従来の IT エンドポイントとは異なり、IoT/OT デバイス内の脆弱性の特定ははるかに困難です。

マイクロソフトが実施した最近の調査によると、Ponemon Institute は、企業内の IoT/OT デバイスのチャンスとセキュリティ上の課題の両方を強調しています。[15] 回答者の 68% は IoT/OT の導入が戦略的なデジタル トランスフォーメーションにとって重要であると考えていますが、60% は IoT/OT のセキュリティが IT/OT インフラにおける最もセキュリティの低い側面の 1 つであると認識しています。

IoT デバイス ファームウェアの脆弱性を使ってネットワークに侵入した攻撃者の例として、Trickbot トロイの木馬があります。これは、Mikrotik ルーター [16] の既定のパスワードと脆弱性を利用して、企業の防御システムを迂回していました。IoT デバイス ファームウェアの基本的な課題は、セキュリティ対策とデバイスの脆弱性を把握しにくいという点です。

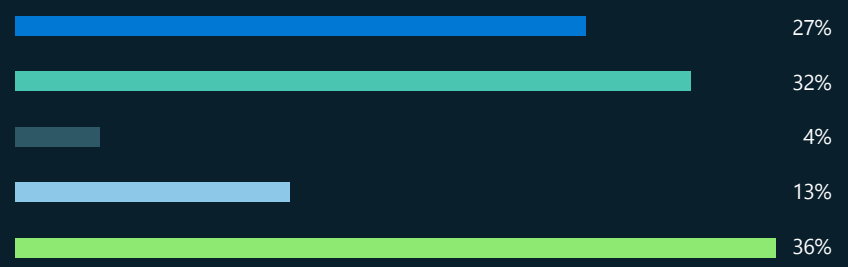
セキュリティで保護されたデバイスを構築するためのソリューションはありますが、既に数十億台ものデバイスが市場に出ており、企業に展開されています。これらは、ブラウンフィールド デバイスと呼ばれます。2021 年、マイクロソフトは ReFirm Labs を買収してブラウンフィールド デバイスのセキュリティに光を当て、デバイス ビルダーが自社製品のセキュリティを高められるようにしました。ReFirm Labs は、デバイスのバイナリ ファームウェア イメージを分析し、潜在的なセキュリティの弱点に関する詳細なレポートを生成しています。[17] このテクノロジは、Microsoft Defender for IoT の将来のリリースに組み込まれる予定です。

過去 1 年間、マイクロソフトはお客様によってスキャンされた独自のファームウェアの集計結果を確認しました。検出された弱点はすべて悪用可能であるとは限りませんが、デバイスのファームウェア セキュリティの根本的な課題を強調しています。

IoT/OT デバイスに存在する弱点の種類は、従来の Windows または Linux エンドポイントでは決して許容できない点に注意してください。

- 弱いパスワード : スキャン対象のファームウェア イメージの 28% には弱いアルゴリズム (MD5/DES) を使って暗号化されたパスワードが含まれていました。これは攻撃者が簡単に突破できます。

分析対象のファームウェア イメージにおけるセキュリティの弱点



- 既知の脆弱性 : 他のシステムと同様、IoT/OT デバイスのファームウェアはオープン ソース ライブラリを広く利用していました。ただし、それらのコンポーネントの最新バージョンを搭載せずに出荷されることがよくあります。分析では、イメージの 32% に、重大 (9.0 以上) と評価されている既知の脆弱性 (CVE) が少なくとも 10 件含まれていました。4% には、6 年以上前の重大な脆弱性が少なくとも 10 件含まれていました。
- 期限切れの証明書 : 証明書は、接続と ID を認証したり、機密データを保護したりするために使用されますが、分析対象のイメージの 13% には、3 年以上前に有効期限が切れた証明書が少なくとも 10 件含まれていました。
- ソフトウェア コンポーネント : イメージの 36% には、パケット キャプチャ ツール (tcpdump、libpcap) など、IoT デバイスから除外するようマイクロソフトが推奨されているソフトウェア コンポーネントが含まれています。攻撃チェーンの一部としてネットワーク偵察に利用できるためです。

検出されたファームウェア攻撃

Viasat: ファームウェアの脆弱性を使って衛星通信を標的にする

2022 年 2 月、衛星ネットワークのインシデントが戦略的な通信ネットワークを切り離し、ヨーロッパ全体でその影響が感じられました。Viasat の KA-SAT システムは大量のトラフィックを受信し、多くのモデムが切断されて、ネットワークに対してサービス拒否攻撃が開始されました。固定ブロードバンドが切断されたため、オペレーターがリモートから何千もの風力タービンにアクセスできなくなり、影響を受けたモデムに悪意のあるワイパー マルウェアが展開されました。この混乱は、企業や組織が通信に使用している 3 万台以上の衛星端末に影響を及ぼしました。

Cyclops Blink: ファームウェア サプライ チェーン攻撃を使ってファイアウォール ゲートウェイを標的にする

脅威アクターにとって、指揮統制 (C2) および攻撃インフラの開発と拡張は、成功を収めるための重要な要素です。安定した C2 インフラの必要性が高まったため、ルーターは理想的な攻撃ベクトルとなりました。修正プログラムが頻繁に適用されておらず、包括的なセキュリティ ソリューションがないためです。

マイクロソフトは、ファームウェア分析テクノロジに関して政府や業界と連携し、デバイスのセキュリティに関する詳細な可視性を提供して、デバイス ビルダーとオペレーターのためのライフサイクル セキュリティを実現しています。

2019 年 6 月以降、国家と関連のある持続的標的型攻撃 (APT) グループが、モジュラー型マルウェア Cyclops Blink を使用し、悪意のあるファームウェアの更新プログラムを実行して大規模なボットネットとして利用することで、脆弱な WatchGuard ファイアウォール デバイスと ASUS ルーターを標的としました。このマルウェアは、特権のエスカレーションを可能にする既知の脆弱性を悪用することによってデバイスへの感染に成功し、脅威アクターがデバイスを管理できるようにします。感染すると、さらにモジュールをインストールして、ファームウェアの更新を回避することができます。侵害されたデバイスは、他の WatchGuard デバイスにホストされている C2 サーバーへの接続が監視されました。さまざまな TCP ポート上で C2 向けの SSL 証明書を多数発行すると、Cyclops Blink オペレーターは、悪意のあるファームウェアの更新を実行し、スキャンなど、従来のセキュリティ手法を回避することによって、ネットワークへの特権リモート アクセスを獲得しました。

マイクロソフトがサプライ チェーンのセキュリティを高めている方法

マイクロソフトは、それらの IoT および OT デバイスのセキュリティ面での課題に対処するため、政府や業界と連携しています (66 ページの説明を参照)。マイクロソフトの貢献内容には、ファームウェア分析テクノロジを利用して、デバイス オペレーターがネットワーク上のデバイスのセキュリティ対策を把握できるようにすることが含まれます。これにより、お客様は、追加の保護、アップグレード、または交換が必要なデバイスを特定して優先順位を付けられるようになります。その結果、デバイス ビルダーがデバイスのセキュリティに投資する需要が高まっています。同時に、セキュアなデバイスを設計し、セキュアな開発ライフサイクルを採用するための包括的なソリューションによって、ビルダーをサポートしています。

もう 1 つの重要な要素は、デバイス ファームウェアを更新してセキュリティ上の問題を検出して解決できるように、堅牢なインフラをビルダーとオペレーターに提供することです。マイクロソフトでは、IoT および OT デバイス セキュリティのライフサイクル全体に対処できるソリューションを提供するため、ファームウェア分析および Defender for IoT と Device Update for IoT Hub を統合しています。これらは、IoT および OT ソリューションに対するゼロ トラスト アプローチをサポートするデバイスを導入することで、お客様がインフラを保護するというマイクロソフトのビジョンを実現するための重要なステップです。[18]

攻撃者は、IoT デバイス ファームウェアの脆弱性を標的にして企業ネットワークに侵入することが増えています。

実用的なインサイト

1. ネットワーク上の IoT/OT デバイスをより細かく把握し、侵害された場合は企業に対するリスクの度合いによって優先順位を付けます。
2. ファームウェア スキャン ツールを使って潜在的なセキュリティの弱点を把握し、ベンダーと協力して、リスクの高いデバイスのリスクを軽減する方法を特定します。
3. ベンダーごとにセキュアな開発ライフサイクルのベスト プラクティスの導入を求めることにより、IoT/OT デバイスのセキュリティにプラスの影響を与えます。

詳しい情報のリンク

- 米国の情報通信技術業界を支える重要なサプライ チェーンの評価

偵察ベースの OT 攻撃

複雑なサプライ チェーンでは、特定の設計情報を使用して実際のシステムを計画します。その設計情報を構成する無数の資産のうち、最も機密性が高いものは、環境とその資産を定義するプロジェクト ファイルです。このファイルは、脅威アクターがアクセス権を取得し、環境に合わせて十分に調整された攻撃を展開するために必要とする、戦略上の重要な標的となります。

業務プロセスを中断するために産業システムを標的とするには、次の 2 つのステップが必要です。

1. まず、攻撃者は OT ネットワークにアクセスする必要があります。これは、ネットワークのエンタープライズ側にある IoT デバイス (Purdue モデル レベル 4) から入り、従来はファイアウォールとネットワーク機器で分離されていた IT-OT 境界を通過して、運用および制御レベルまで到達することにより行うことができます。
2. 次に、ネットワーク デバイスを特定する必要があります。産業システムは、環境に特化したカスタマイズされたアーキテクチャで標準のデバイスとコンポーネントを使用しています。これらの標準デバイスのいずれかに、プログラマブル ロジック コントローラー (PLC) があります。どのメーカーも、産業システムの重要なコンポーネントである PLC に対して独自のインターフェイスと機能を開発しており、それらのデバイスは、顧客の環境に特化したカスタム スキーマでさらに構成されています。

各 PLC の固有の構成は、プロジェクト ファイルに記述されています。これには、環境とその資産の定義、ラダー ロジックなどが含まれています。

攻撃された証拠を示すほとんどの環境では、攻撃前のタイムラインが攻撃自体の長さをはるかに上回っていることが分析に示されています。脅威アクターは多くの場合、環境とその資産をリモートでシミュレートすることに数か月を費やし、モデルを構築して標的型攻撃を準備するため何度も試行します。環境は絶えず変化し、新しいデバイスが統合されるので、プロジェクトおよび構成ファイルのデータを中心に脆弱性が発生します。プロジェクト ファイルを盗難すると、攻撃が数週間あるいは数か月分前進するため、攻撃者は標的環境をすばやく正確にモデル化できるようになり、悪意のあるアクティビティの検出が難しくなります。

Industroyer と Incontroller

国家が支援するアクターがモジュール型マルウェアと攻撃フレームワークを使用して組織、重要インフラ、政府を標的とする攻撃の増加が観察されています。ウクライナの重要な作戦を妨げる新たな試みは、標的環境に合わせて高度に調整された偵察ベースの OT 攻撃の脅威が増加していることを強調しています。国家レベルのサイバー アクターによって実施された拡張偵察および調査フェーズは、インフラを遠隔操作して、サイバー キネティック作戦と政治的戦略の融合における具体的な戦略的目標や運用目標を達成するため、サイバー戦争を利用する戦略であることを示しています。

偵察ベースの OT 攻撃

(続き)

2022 年初頭、適応性の高い 2 つの重大な OT 攻撃が特定されました。ウクライナの変電所と保護継電器に対するサイバーフィジカル攻撃は、2016 年の展開後にウクライナで停電を引き起こしたとされるマルウェア Industroyer の変異種を含む、カスタマイズされたマルウェアを使って実行されました。

Industroyer2 は、悪意のある OT 攻撃マルウェアが新しい標的に初めて再展開された例として知られています。Industroyer 用に開発された IEC104 プロトコル (電源システムの監視および制御のための標準プロトコル) プラグインが利用され、大部分は PLC と似ている遠隔端末装置 (モデル番号 ABB RTU540/560) が標的になりました。このマルウェアの記述者は、被害者の環境に関する情報を使って、事前に定義された出力にコマンドを繰り返し発行し、手動でオンにできないようにしました。その結果、停電がより長期間続き、より深刻な影響が生じました。

同時期に特定されたモジュール型攻撃フレームワークである Incontroller は、レガシー セキュリティ ソリューションを迂回して、OT デバイスへの侵入と攻撃のリードタイムを大幅に短縮するモジュール型ツールキットです。この汎用ツールキットには、さまざまな環境に合わせて高度にカスタマイズ可能なデータ収集、偵察、攻撃の機能が搭載されており、偵察の実行に必要な時間を短縮し、デバイスとその構成に関する情報を抽出して環境のシミュレーションをサポートすることで、OT 攻撃の調査フェーズに大きな影響を与えることができます。

Incontroller フレームワークは、Schneider Electric と Omron の PLC のプロトコルをサポートしており、ファームウェア バージョン、モデルの種類、コネクテッド デバイスなどの情報を収集します。このツールキットは、構成を変更したり、出力をオン / オフにしたりするためのコマンドを発行できます。環境にアクセスすると、フレームワークは、より多くのペイロードを提供するためデバイスにバックドアを埋め込み、脆弱性を発生させてアクセス ポイントを増やした後、ラダー ロジックをアップロードして、DoS 攻撃を開始できるようにします。このツールキットには汎用的な性質があるため、脅威アクターは、すべての PLC または場所に合わせて新しい攻撃を記述しなくても、環境をすばやく攻撃することができます。そのため、アクターは、業界の異なるさまざまな種類のコンピューターとの対話を容易に行うことができます。

実用的なインサイト

1. システム定義が含まれているファイルを、セキュアでないチャネル経由で転送したり、不必要な担当者に転送したりしないようにします。
2. そのようなファイルの転送を避けられない場合、必ずネットワーク上のアクティビティを監視し、資産がセキュアであることを確認してください。
3. EDR ソリューションを使って監視することで、エンジニアリング ステーションを保護します。
4. OT ネットワークのインシデント対応を積極的に実施します。
5. Defender for IoT などの継続的な監視を展開します。

巻末注

1. 参照先の例 : Revised Directive on Security of Network and Information Systems (NIS2) | Shaping Europe’s digital future (europa.eu)、https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2020:595:FIN&rid=1、Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (homeaffairs.gov.au)、Chile: Bill for cybersecurity and critical information infrastructure introduced in Senate | News post | DataGuidance、Japan passes economic security bill to guard sensitive technology | The Japan Times、Review of the Cybersecurity Act and Update to the Cybersecurity Code of Practice for CIIs (csa.gov.sg)、Proposal for legislation to improve the UK’s cyber resilience—GOV.UK (www.gov.uk)、Telecommunications (Security) Act 2021 (legislation.gov.uk)、Updating the NIST Cybersecurity Framework—Journey To CSF 2.0 | NIST
2. Cert-In—ホーム ページ
3. Initiation of consultation on introduction of cyberattack reporting obligation (admin.ch)
4. 参照先の例 : 無題 (house.gov)
5. Cyber Resilience Act | Shaping Europe’s digital future (europa.eu)
6. 参照先の例 : マイクロソフト セキュリティ開発ライフサイクル
7. 参照先の例 : Generating Software Bills of Materials (SBOMs) with SPDX at Microsoft—Engineering@Microsoft、他の参照先の例 : The Minimum Elements For a Software Bill of Materials (SBOM) | National Telecommunications and Information Administration (ntia.gov)
8. 参照先の例 : https://www.microsoft.com/en-us/msrc/cvd
9. The Product Security and Telecommunications Infrastructure (PSTI) Bill—製品セキュリティ ファクトシート—GOV.UK (www.gov.uk)
10. Commission strengthens cybersecurity of wireless devices and products (europa.eu)
11. Cloud Certification Scheme: Building Trusted Cloud Services Across Europe — ENISA (europa.eu)
12. Certification — ENISA (europa.eu)
13. https://github.com/microsoft/sbom-tool「GitHub-microsoft/sbom-tool: SBOM ツールは、非常にスケーラブルでエンタープライズ向けのツールで、あらゆる種類のアーティファクトに対応する SPDX 2.2 と互換性のある SBOM を作成できます。
14. https://www.zdnet.com/article/ripple20-vulnerabilities-will-haunt-the-iot-landscape-for-years- to-come
15. IoT/OT Innovation Critical but Comes with Significant Risks (2021 年 12 月): https://www.microsoft.com/security/blog/2021/12/08/new-research-shows-iot-and-ot-innovation-is-critical-to-business-but-comes-with-significant-risks/
16. Uncovering Trickbot’s use of IoT devices in C2 Infrastructure (2022 年 3 月): https://www.microsoft.com/security/blog/2022/03/16/uncovering-trickbots-use-of-iot-devices-in-command-and-control-infrastructure/
17. IoT Show on Channel 9 Episode on IoT Firmware Scanning (2022 年 5 月): https://docs.microsoft.com/en-us/shows/internet-of-things-show/iot-device-firmware-security-scanning-with-azure-defender-for-iot
18. How to apply a Zero Trust approach to your IoT solutions (2021 年 5 月): https://www.microsoft.com/security/blog/2021/05/05/how-to-apply-a-zero-trust-approach-to-your-iot-solutions/

サイバー影響工作

国外からの現在の影響工作は、新しい手法とテクノロジを利用し、信頼がより効率的かつ効果的に損なわれるようキャンペーンを設計しています。

サイバー影響工作の

概要

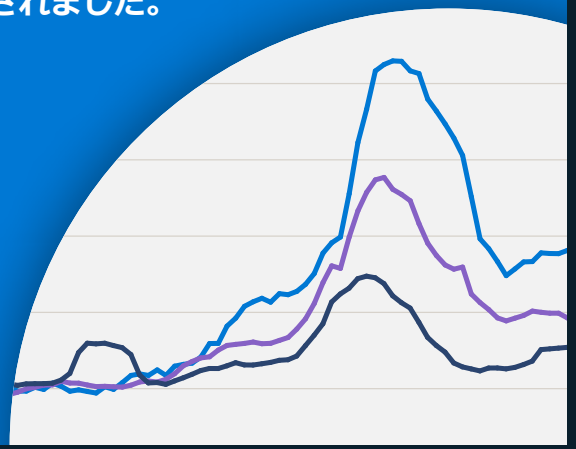
国外からの現在の影響工作は、新しい手法とテクノロジを利用し、信頼がより効率的かつ効果的に損なわれるようキャンペーンを設計しています。

国家は、プロパガンダを広めて国内外の世論に影響を与えるため、高度な影響工作をますます利用するようになっています。このような活動は、信頼の低下、対立の激化、民主的プロセスへの脅威につながります。熟練した高度で継続的なマニピュレーター (Advanced Persistent Manipulator) アクターは、インターネットやソーシャル メディアと共に従来のメディアを利用して、活動の範囲、規模、効率を大幅に強化し、グローバル情報エコシステムにきわめて大きな影響を及ぼしています。過去 1 年間、ロシアによるウクライナでのハイブリッド戦争の一環としてそのような工作が利用されてきましたが、ロシアに加えて中国やイランなどの他の国々は、グローバルな影響力を広げるため、次第にソーシャル メディアを利用したプロパガンダ工作に転換してきました。

政府や国家が世論を形成したり、敵対者の信用を失墜させたり、不和をそそのかしたりする目的でサイバー影響工作を利用しているため、サイバー影響工作はますます高度になっています。

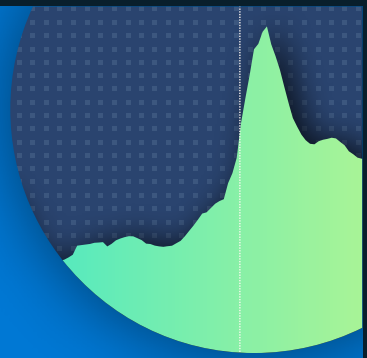
詳しくは 74 ページをご覧ください

ロシアのウクライナ侵攻では、影響力を最大限に高めるため、サイバー影響工作が従来型のサイバー攻撃やキネティック軍事作戦と実際に組み合わされました。



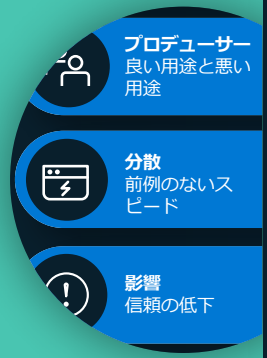
詳しくは 76 ページをご覧ください

ロシア、イラン、中国は、COVID-19 パンデミックの初期からプロパガンダと影響工作キャンペーンを利用してきました。多くの場合、広範な政治的目標を達成するための戦略デバイスとして利用しています。



詳しくは 76 ページをご覧ください

合成メディアは、かなりリアルな人工画像、動画、音声を簡単に作成して普及させることができるツールが急増したため、ますます広まっています。メディア資産の出所を認定するデジタル プロブナンス テクノロジは、誤用への対抗の点で期待されています。



詳しくは 80 ページをご覧ください

サイバー影響工作から保護するための包括的なアプローチ

マイクロソフトは、サイバー影響工作に対抗するため、既に成熟したサイバー脅威インテリジェンス インフラを構築しています。マイクロソフトの戦略は、国外の攻撃者によるプロパガンダ キャンペーンを検出、妨害、防御、阻止することです。

詳しくは 83 ページをご覧ください

はじめに

民主主義が繁栄するには信頼できる情報が必要です。マイクロソフトが重点を置いている重要な分野は、国家によって開発されて存続している影響工作です。このような活動は、信頼の低下、対立の激化、民主的プロセスへの脅威につながります。

国外からの影響工作は、情報エコシステムにとって常に脅威となってきました。しかし、インターネットとソーシャル メディアの時代において異なるのは、キャンペーンの範囲、規模、効率が大幅に高まり、グローバル情報エコシステムの健全性に膨大な影響を与える可能性があるという点です。

古くから「真実が靴を履いく頃、嘘は世界の半分を回っている」という格言がありますが、今これがデータで起きています。マサチューセッツ工科大学 (MIT) の調査[1] によると、嘘は真実よりもリツイートされる可能性が 70% 高く、6 倍の速さで最初の 1,500 人に到達します。プロパガンダ キャンペーンがインターネットとソーシャル メディアであふれ、従来のニュースに対する信頼が損われるにつれて、情報エコシステムはあいまいさ増しています。2021 年の調査[2] では、新聞、テレビ、ラジオの報道を信用していると回答したのは米国の成人のわずか 7% であり、34% は「まったく信用していない」と回答しています。

マイクロソフトは、国外のサイバー影響分野における主要なアクター、脅威、戦術を特定し、得られた教訓を共有することに取り組んでいます。今年 6 月、ウクライナから得られた教訓に関する包括的なレポートを発表しました。これには、ロシアのサイバー影響工作に関する詳細な調査結果が記載されています。[3]

さらに、マイクロソフトは、ディープ フェイクなどの高度なテクノロジがどのように兵器化され、ジャーナリストの信頼性を損なう可能性があるかについても調査しています。また、業界、政府、学界と連携し、合成メディアを検出して信頼を回復するためのより良い方法を開発しています。たとえば、偽物を特定できる人工知能 (AI) システムなどです。

従来のサイバー攻撃と影響工作の混合、民主的選挙における妨害など、情報エコシステムと国家のオンライン プロパガンダには急速に変化する性質があるため、民主主義に対するオンラインとオフラインの脅威の両方を軽減するための社会全体のアプローチが求められています。

マイクロソフトは、信頼できるニュースと情報が繁栄する、健全な情報エコシステムをサポートすることに注力しています。また、国家主導の影響工作の変化と拡大を続けるリスクに対抗するためのツールや脅威検出機能を開発しています。これを実現するため、マイクロソフトは最近 Miburo Solutions を買収しました。Global Disinformation Index and NewsGuard などのサードパーティ バリデーターと連携し、Coalition for Content Provenance and Authenticity (C2PA) などのパートナーシップもリードしています。民主的なプロセスや制度を弱体化させようとしている人たちと闘うには、協力がどうしても必要です。

Teresa Hutson

バイス プレジデント、テクノロジおよびコーポレート責任者

サイバー影響工作の動向

テクノロジが速いペースで進化しているため、サイバー影響工作はますます高度になっています。従来のサイバー攻撃で使用されているツールの重複と拡張が、サイバー影響工作にも見られています。さらに、国家間での連携と拡散が増えています。

マイクロソフトは今年、国外からの影響工作の分析に特化した企業である Miburo Solutions を買収することにより、国外からの影響工作への対抗策に投資しました。Miburo Solutions のアナリストをマイクロソフトの脅威コンテキスト アナリストと組み合わせることで、デジタル脅威分析センター (DTAC) を結成しました。DTAC は、国家レベルの脅威 (サイバー攻撃と影響工作の両方が含まれます) について分析および報告し、情報および脅威インテリジェンスと地政学的分析を組み合わせてインサイトを導き出し、効果的な対応と保護の方法を発表します。

世界中の 4 分の 3 を超える人々が、情報の兵器化について心配していると回答しており[4]、マイクロソフトのデータはそのような懸念に対応します。マイクロソフトとそのパートナーは、国家レベルのアクターが戦略的目標と政治的目標を達成するために影響工作をどのように利用しているかを追跡してきました。破壊的なサイバー攻撃やサイバー スパイ活動に加えて、権威主義的な政権は、世論を形成したり、敵対者の信用を失墜させたり、恐怖心をあおったり、不和をそそのかしたり、現実の歪曲を図ったりするために、サイバー影響工作を利用することが増えています。

このような国外からのサイバー影響工作には、通常、次の 3 つの段階があります。

事前配置

組織のコンピューター ネットワーク内にマルウェアを事前配置するのと同様、国外からのサイバー攻撃工作では、インターネット上のパブリック ドメインに虚偽の情報が事前配置されます。特に IT 管理者が最新のネットワーク アクティビティをスキャンしている場合、事前配置戦術は従来のサイバー活動に長く利用されてきました。ネットワーク上で長期間休止状態になっているマルウェアは、その後使用されたときの効果が高まります。インターネット上で注目されていない虚偽の情報は、その後の参照されたときに信頼が高いように見えます。

開始

多くの場合、アクターにとって目標を達成するのに最も適した時期に、政府が支援している機関や、影響を受けた報道機関 / ソーシャル メディア チャネルを通じて、情報を広めるための組織的なキャンペーンが開始されます。

拡散

最後に、国家が管理するメディアとプロキシによって、標的のオーディエンス内で情報が拡散されます。多くの場合、何も気づいていないテクノロジ イネーブラーが情報の到達範囲を広げます。たとえば、オンライン広告を使うと、財務活動や組織的なコンテンツ配信システムが検索エンジンをあふれさせることができます。

この 3 ステップのアプローチは、ウクライナでの生物兵器とバイオラボの噂に関するロシアの虚偽情報を裏付けるため、2021 年後半に利用されました。この情報は、まず 2021 年 11 月 29 日に、モスクワにいる米国人駐在員による英語のレギュラー番組の一部として YouTube にアップロードされました。そこでは、米国が資金提供したウクライナのバイオラボに生物兵器とのつながりがあるという主張がなされました。その情報は数か月間ほとんど気づかれませんでした。2022 年 2 月 24 日、ロシアの戦車が国境を越えたのと同時に、その情報が戦場に送られました。マイクロソフトのデータ分析チームは、2 月 24 日に同時にレポートを公開し、「昨年のレポート」を振り返って信ぴょう性を与えようとした、ロシアが管理するか影響力を持つ 10 のニュース サイトを特定しました。さらに、ロシア外務省当局は記者会見を実施し、情報環境における米国のバイオラボに関する虚偽の主張をさらに加えました。その後、ロシアが支援するチームが、ソーシャル メディアやインターネット サイトでその情報をより広範に拡散しようとしました。

世界中の権威主義的な政権が連携して、相互の利益のために情報エコシステムを汚染しています。たとえば、COVID-19 パンデミックの初期から、ロシア、イラン、中国は、民主主義を攻撃して地政学的な目標を達成するため、あからさまな宣伝方法、半分隠密な宣伝方法、隠密な宣言方法を組み合わせてプロパガンダと影響工作を利用しました (76 ページで詳しく説明します)。この 3 つの政権は、互いのメッセージングおよび情報エコシステムを利用し、望む情報を宣伝しています。この報道の多くは、政府内の人物が公式声明でふれ回っていた、米国とその同盟国に関する批判や陰謀説で構成されていましたが、自国のワクチンと COVID-19 への対応が米国や他の民主主義国家より優れているという宣伝も行っていました。国営報道機関は、互いに情報を拡散することによってエコシステムを作り、ある国営報道機関が生み出した民主主義国家に関するネガティブな報道 (あるいはロシア、イラン、中国についてのポジティブな報道) が他の報道機関によって補強されていました。

米国のバイオラボと生物兵器についての情報が、多数の国外からの影響工作の 3 つの大まかな段階 (事前配置、開始、拡散) によってどのように広がったを示す図。

サイバー影響工作の動向

(続き)

この課題を難しくしていることとして、民間企業のテクノロジ エンティティが知らずにそれらのキャンペーンに加担する可能性があります。イネーブラーには、インターネット ドメインを登録する企業、Web サイトをホストする企業、ソーシャル メディアや検索サイトで資料を宣伝する企業、トラフィックを送信する企業、デジタル広告を通じてそれらの活動に金銭を支払う企業が含まれます。組織は、権威主義的な政権がサイバー影響工作に利用しているツールと方法を認識し、キャンペーンを検出してその広がりを妨ぐことができる必要があります。さらに、消費者が国外からの影響工作を特定し、情報やコンテンツへの関与を制限する高度な能力を身に付けるための支援もますます必要になっています。

権威主義的なプロパガンダを含むサイバー影響工作は、信頼を失墜させて、二極分化を促し、民主主義のプロセスを脅かすため、世界中の民主主義国家にとって脅威となっています。

透明性を高め、それらの影響工作キャンペーンを明らかにして妨害するには、政府、民間企業、市民社会全体で協調を強め、情報共有を強化することが必要です。

世界中の 4 分の 3 以上の人々が情報の兵器化を心配しています。

COVID-19 とロシアのウクライナ侵攻における影響工作が脚光を浴びる

パンデミックとロシアによるウクライナ侵攻の間、情報環境を統制しようとしている国家は、権威主義的な政権がサイバー犯罪と情報操作をどのように融合させているかについて実例を示しています。

COVID-19 に関するプロパガンダ

ロシア、イラン、中国は、COVID-19 パンデミックの初期からプロパガンダと影響工作キャンペーンを利用してきました。COVID-19 により、次の 2 つの主要な方法でそれらのキャンペーンが明らかになりました。

1. パンデミック自体の表現。
2. より広範な政治的目標を達成するため、戦略的な道具として COVID-19 を利用したキャンペーン。

このような種類のキャンペーンの全体的な目的は、2 つの要素からなっています。1 つ目は、民主主義、民主的制度、および米国とその同盟国のイメージを世界の舞台で弱体化させることです。2 つ目は、国内外で自国政府の立場を強化することです。

その一例として、ロシアの既知のアカウントやメディア組織による英語の読者を対象としたメッセージと、ロシア政府が COVID-19 のワクチンと重症度に関して自国民にどのように伝えているかを比較できます。

RT.com で閲覧されたコロナウイルスに関する記事のトピック トップ 10 (2021 年 10 月～ 2022 年 4 月)

反ワクチンのプロパガンダがロシア語以外の読者を標的にしている

ロシア語 (以下では英語に翻訳されています)	英語
「ロックダウンとブースターは感染を防ぐ」	「ワクチントでは感染を抑制できず、新しい変異株には効果がない」
「ロシアの有名人が陽性になった」	「Pfizer ワクチンには危険な副作用がある」
「ロシアで症例と死者が増加している」	「政治的な動機で大量のワクチンが接種されている」
「スプートニク V ワクチンは非常に効果が高い」	「Pfizer と Moderna が無秩序な試験を実施している」
「公共交通機関ではワクチン証明が必要」	

ロシアの COVID-19 に関するメッセージは言語によって異なります。

別の例として、COVID-19 ウイルスの起源をあいまいにしようとしたキャンペーンがあります。パンデミックの開始以来、ロシア、イラン、中国の COVID-19 に関するプロパガンダは、これらの中心的なテーマを拡散するために、互いの報道を後押ししました。この報道の多くは、米国に関する批判や陰謀説を推し進める内容で構成されていました。国営報道機関は、互いに情報を定期的に拡散することによってエコシステムを開発し、ある国営報道機関が生み出した民主主義国家に関するネガティブな報道やロシア、イラン、中国についてのポジティブな報道が他の報道機関によって何度も補強されていました。

その一例は、COVID-19 が米国によって作られた生物兵器であるかもしれないという、ロシアとイランのメディアによる初期の示唆です。この主張は、COVID-19 が武器として作られたと信じていると主張した法律学の教授とのインタビューの後、パンデミックの早い段階で非主流派の陰謀 Web サイトに流れました。[6] 閲覧数が限られている数のいくつかの Web サイトでインタビューが公開された後、その情報は国営報道機関によって取り上げられました。イラン政府の支援を受けたイランの英語とフランス語の報道機関である PressTV は[7]、2020 年 2 月に「Francis Boyle 氏が信じているようにコロナウイルスは米国の生物兵器なのか」というタイトルで英語の情報を発表しました。この記事は、COVID-19 の大流行の背後に米国がいることを示唆し、「米国によるすべての戦争では、放射線兵器、化学兵器、生物兵器、および他の禁止されている兵器が使用されており、標的となる地域の人々に壊滅的な被害を及ぼしています。」と述べました。[8] ロシア国営報道機関と中国政府のアカウントは、それに同調しました。Russia Today (RT) (クレムリンのプロパガンダを広める役割があるとして知られている国営報道機関 [9]) は、COVID-19 は「イランと中国を対象とした米国の " 生物攻撃 " の産物」[10] かもしれないと主張する、イラン当局からの声明を宣伝する記事を少なくとも 1 件公開し、そのようなことを示唆するソーシャル メディアの投稿を行いました。たとえば、2020 年 2 月 27 日の RT によるツイートは「#coronaviru が生物兵器であることが明らかになっても驚かない人は手を挙げてください」というものでした。[11]

ウクライナでの戦争ー戦争の武器としてのプロパガンダ

ロシアのウクライナ侵攻は、影響力を最大限に高まるため、従来型のサイバー犯罪や地上の軍事作戦とサイバー影響工作がどのように組み合わされる可能性があるかという、明確な例を示しています。

マイクロソフトの脅威インテリジェンス アナリストは、ウクライナの侵攻に至るまでの間、ロシアと協力するアクターがウクライナに対して 237 件を超えるサイバー攻撃を開始したのを確認しました。これらのキャンペーンは、サービスと公共機関の機能低下、ウクライナ国民による信頼性の高い情報へのアクセス妨害、国のリーダーシップに対する疑念の植え付けを目的としていました。

COVID-19 とロシアのウクライナ侵攻における影響工作が脚光を浴びる

(続き)

2022 年 4 月にリリースされたマイクロソフトのレポートでは、キエフの情報環境を統制しようとする中、ロシアはキエフのテレビ塔に対してミサイル攻撃を開始したのと同じ日に、ウクライナの大手メディア企業に対して破壊的なマルウェアを立ち上げたことが紹介されています。[12]

サイバー攻撃と影響工作が同時に行われたことを示す別の例として、ロシアの脅威アクターが、マリウポリの住民からのものであると主張するメールをウクライナ国民に送信しました。そのメールは、戦争の激化がウクライナ政府によるものであると非難し、同胞に政府への抵抗を呼びかけました。それらのメールの宛先には、メールを受信している人の名前が具体的に記入されており、以前のスパイ関連のサイバー攻撃で情報が盗難された可能性を示しています。悪意のあるリンクは含まれていませんでした。これは、純粋な影響工作が目的であったことを示唆しています。

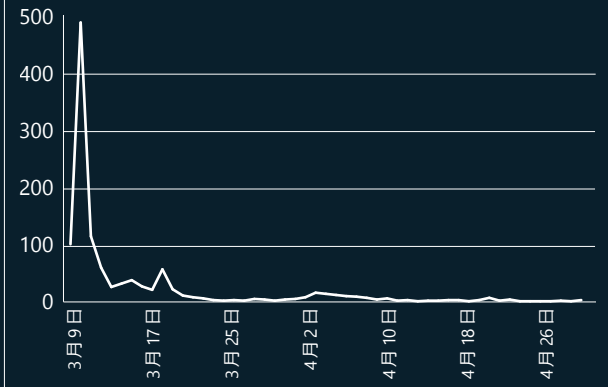
ハッキングした情報、流出した情報、または他の機密情報をうわさとして取り上げる方法は、ロシアのアクターが影響工作でよく利用する戦術です。ウクライナでの戦争の初期から、ロシア寄りのソーシャル メディア チャネルは、主張している内容はウクライナの情報源から流出したものか、他の機密情報であると宣伝しています。公共機関の信頼を低下させ、主流派の情報物語に疑念を投げかけるため、ロシア寄りのソーシャル メディア チャネルや報道機関では、より広範な影響工作戦略の一環として流出した情報や機密情報を使用しています。

この情報は、ウクライナと西側諸国を標的とするプロパガンダを作成して、デジタル セキュリティに対する信頼を下げ、ウクライナに対する西側諸国の支援を阻害するため、操作されることがあります。

ロシアは、現場での出来事の後に世論を形成したり、事実をあいまいにしたりするため、他の情報攻撃を利用してきました。たとえば、ロシアは 3 月 7 日、ウクライナのマリウポリにある産科病院が空になっており、軍事施設として使用されていたという情報を、国連 (UN) への届け出を通じて事前配置しました。3 月 9 日、ロシアはその病院を爆撃しました。爆撃のニュースが報道された後、ロシアの国連代表 Dmitry Polyanskiy 氏は、爆撃の報道が「フェイク ニュース」であるとツイートし、軍事施設として使用されているとするロシアの以前の主張を引用しました。それからロシアは、病院への攻撃後 2 週間、ロシアが管理する Web サイトでこの情報を広範囲に広めました。

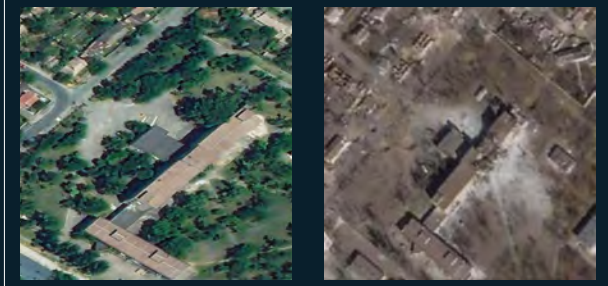
ドメインとトラフィック

(2022 年 3 月 9 日～ 2022 年 4 月 30 日)



プロパガンダ Web サイトは、産科病院についての情報を約 2 週間公開し、2022 年 4 月 1 日から短期間復活させました。出典 : Microsoft AI for Good Lab。

マリウポリにある産科病院の衛星画像 (2022 年 2 月と 3 月)



マイクロソフト独自の衛星画像解析により、産科病院が爆撃されたことが判明しました。最初の写真は 2022 年 2 月 24 日のもので、2 つ目の写真は 2022 年 3 月 24 日のものです。写真出典 : Planet Labs。

ロシアによる残虐行為の隠ぺいは、戦争の進行と同時に続きました。たとえば、2022 年 6 月下旬、ロシアの報道機関とインフルエンサーは、ショッピング モールの爆撃を正当かつ必要なものであったと発言し、モールとしては使用されておらず、ウクライナ国防軍の武器庫として使用されていたという誤った主張を行いました。[13] Telegram を利用しているクレムリン寄りの複数のブロガーが、「偽旗」情報を支持するコンテンツを投稿して拡散しました。映像に軍服を来た人物がいることと [14]、女性がいないことなど [15]、捏造の証拠を指摘したブロガーもいました。ロシアは、プロパガンダを伝える人とメディアのために構築されたシステムを利用して、キャンペーンを開始しました。このような情報をオンラインで拡散することにより、ロシアは国際的な舞台で非難をそらし、説明責任を回避できるようになります。

ロシアのような国家は、非公開の情報源から得られた情報を使って公共認識に影響を与えることの価値を理解しており、「ハック アンド リーク」キャンペーンを使って情報に反論し、不信感をまいています。

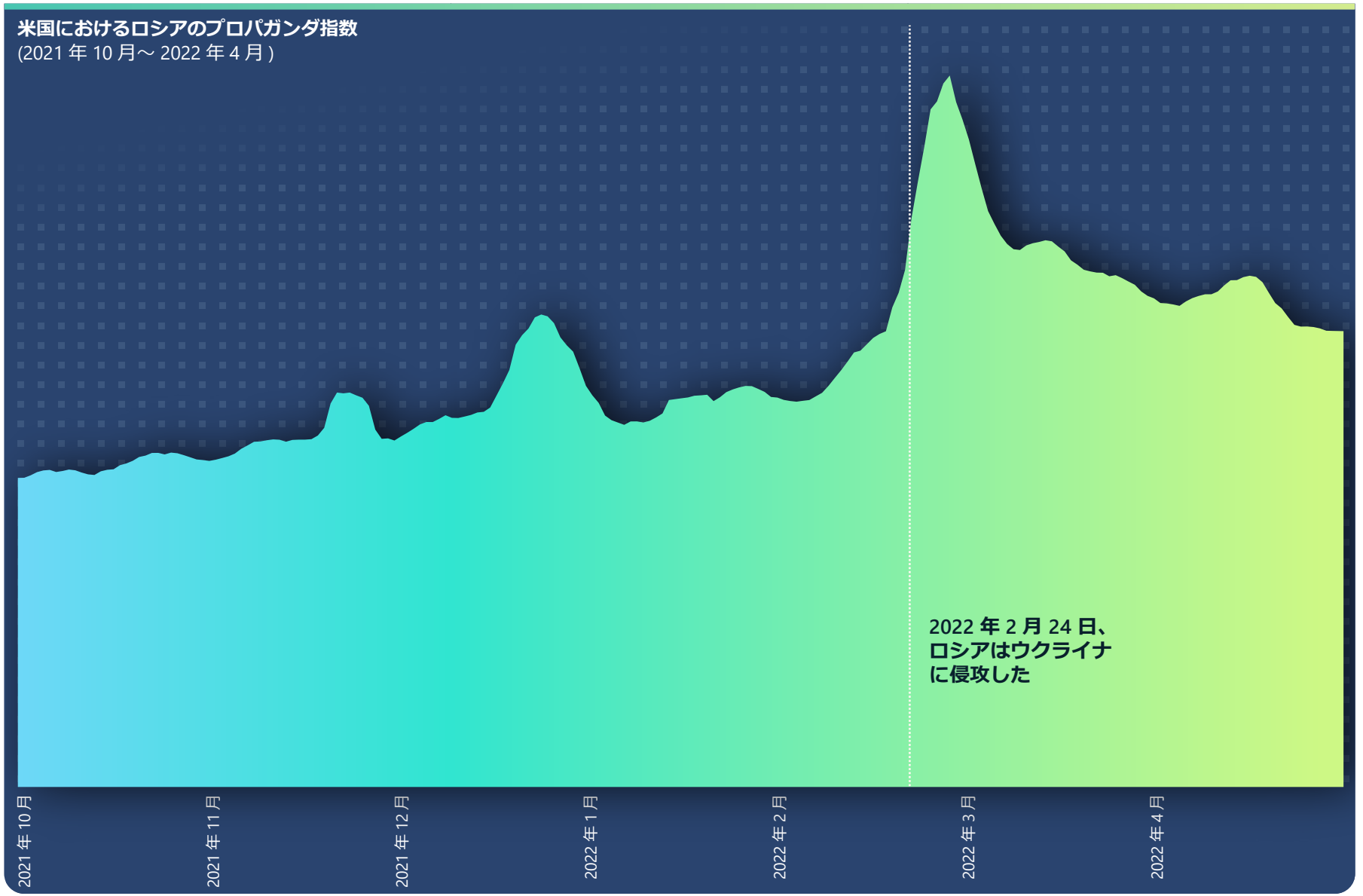
詳しい情報のリンク

- ウクライナ防衛 : サイバー戦争から得られた初期の教訓 | Microsoft On the Issues
- ウクライナにおけるロシアのサイバー攻撃活動の概要 | Microsoft Special Report
- ウクライナを標的とするサイバー攻撃を阻止する | Microsoft On the Issues

ロシアのプロパガンダ指数を追跡する

2022 年 1 月、ほぼ 1,000 件の米国 Web サイトがロシアのプロパガンダ Web サイトへのトラフィックを参照していました。米国のオーディエンスを標的とするロシアのプロパガンダ Web サイトの最も一般的なトピックは、ウクライナでの戦争、米国の国内政治 (トランプ氏支持かバイデン氏支持か)、COVID-19 およびワクチン関連の情報です。

ロシアのプロパガンダ指数 (RPI) は、ロシアの国家が管理する報道機関や拡散サイトからのニュースの流れを、インターネット全体のニュース トラフィックに対する割合として監視しています。RPI は、インターネット全体と各地域におけるロシアのプロパガンダ消費を、正確なタイムラインに沿ってグラフ化するために使用できます。ただし、マイクロソフトは、以前に特定された Web サイトに投稿されたロシアのプロパガンダのみ観察できる点に注意してください。当局のニュース Web サイト、未確認の Web サイト、ソーシャル ネットワーク グループなど、他の種類の Web サイトでのプロパガンダに関するインサイトはありません。



ロシアのプロパガンダ指数を追跡する

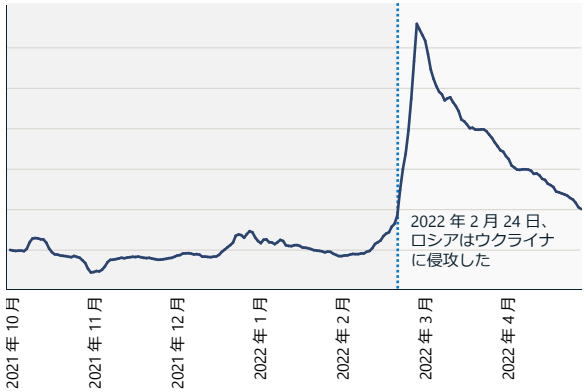
(続き)

ロシアのプロパガンダ指数 : ウクライナ

ウクライナ戦争が始まると、ロシアのプロパガンダが 216% 増加し、3 月 2 日にピークを迎えました。以下の図は、この急激な増加が侵攻と一致していることを示しています。2 つのグラフは、侵攻が始まって間もなくロシアのプロパガンダがどのように急増したかを示しています。

RPI、ウクライナ

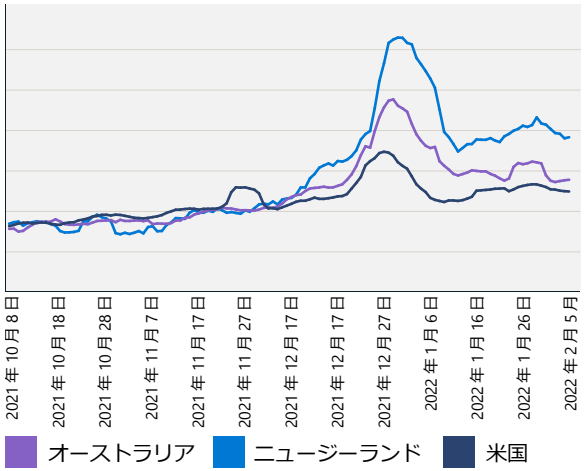
(2021 年 10 月 7 日～ 2022 年 4 月 30 日)



ロシアのプロパガンダ指数 : ニュージーランド、オーストラリア、米国

ニュージーランドにおける RPI の値は、COVID-19 のプロパガンダに関連し、2021 年後半に急増しました。ニュージーランドにおけるロシアのプロパガンダ消費の急増は、ウェリントンで 2022 年初頭に発生した抗議活動の前に生じました。2 回目の急増は、ロシアのウクライナ侵攻と明らかに関連性があり、オーストラリアと米国の RPI を上回っています。

RPI、ニュージーランド、オーストラリア、米国



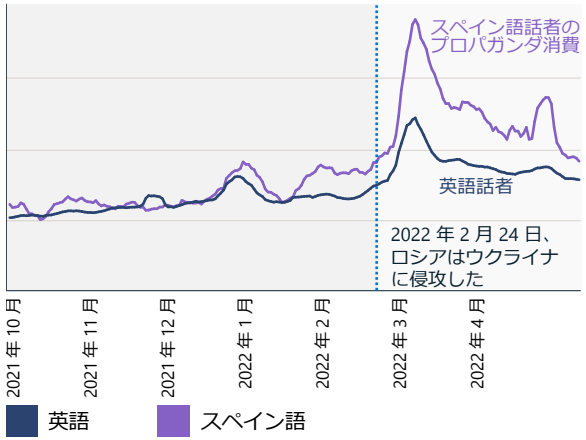
ニュージーランドにおけるロシアのプロパガンダ消費は、2021 年 12 月第 1 週までオーストラリアと似ています。12 月以降、ニュージーランドにおけるロシアのプロパガンダ消費は、オーストラリアと米国の消費より 30% 以上多くなっています。

米国におけるロシアのプロパガンダ指数 : 英語とスペイン語

RPI は、言語間のプロパガンダも追跡しています。RT や Sputnik News など、複数の報道機関は 20 以上の言語で利用できます。これには、英語、スペイン語、ドイツ語、フランス語、ギリシャ語、イタリア語、チェコ語、ポーランド語、セルビア語、ラトビア語、リトアニア語、モルダビア語、ベラルーシ語、アルメニア語、オセチア語、ジョージア語、アゼルバイジャン語、アラビア語、トルコ語、ペルシャ語が含まれます。

次のグラフは、米国でスペイン語のニュースの RPI が英語のニュースよりもはるかに高いことを示しています。

スペイン語話者の間におけるロシアのプロパガンダ消費は 2 倍多い



米国におけるロシアのプロパガンダ消費は、スペイン語話者の方が 2 倍多くなっています。

ロシアのプロパガンダは中南米で多い

スペイン語版 RT は、ページビューと Facebook フォロワーの数が最も多い国際報道機関です。

出典 : Microsoft AI for Good Research Lab

合成メディア

AI 対応のメディアの作成と操作にとって黄金時代が到来しました。マイクロソフトのアナリストは、これが 2 つの主なトレンド (とてもリアルな合成画像、動画、音声、テキストを人工的に作成するための使いやすいツールとサービスの普及、特定のオーディエンスに合わせて最適化されたコンテンツをすばやく広める機能) によってもたらされている点に注目しています。

これらの開発はいずれも、本質的には問題となりません。AI ベースのテクノロジを使用すれば、純粋に合成コンテンツを作成するのか、既存の素材を強化するのかにかかわらず、楽しくてエキサイティングなデジタル コンテンツを作成できます。これらのツールは、企業が広告やコミュニケーションのために使用したり、個人がフォロワー向けに魅力的なコンテンツを作成するために使用したりしています。しかし、合成メディアは、損害を与えることを目的として作成および配布された場合、個人、企業、公共機関、社会に深刻な被害を及ぼす可能性があります。マイクロソフトは、社内と広範なメディア エコシステムの両方においてこのような損害を抑えるため、テクノロジとプラクティスを積極的に開発してきました。

このセクションでは、有害な合成コンテンツを作成するための最新技術の現状、このコンテンツが広範に広まった場合に生じる被害、合成メディアを使ったサイバー脅威から防御するための技術的な軽減策に関する、マイクロソフトの分析から得られたインサイトについて説明します。

合成メディアの作成

大規模な映画スタジオにある膨大なコンピューティング リソースがなければできなかった技術が携帯電話アプリに組み込まれたため、合成テキストとメディアの分野は驚くほど速く進化しています。同時に、ツールは使いやすくなっており、フォレンジック メディアの専門家ですら欺くことができるレベルまでリアルなコンテンツを生成することができます。人物や内容を自由に合成して、ほぼ誰でも合成動画を作成できるところまで来ています。間もなく、オンラインで目にするコンテンツの大部分が、AI 技術を使って完全あるいは部分的に合成したものになる時代に突入と言っても過言ではありません。

> より高度で使いやすく、広範囲に入手可能なツールが登場したことで、合成コンテンツの作成は増加しており、まもなく現実との区別が付かなくなるでしょう。

高品質な無料 / 有料の画像、動画、オーディオ編集ツールが数多く存在します。これらのツールを使うと、誤解を招くテキストの追加、顔の入れ替え、コンテキストの削除や変更など、損害を与える可能性のある変更をデジタル コンテンツに対して簡単に加えることができます。そのような「チープ フェイク」は、悪質なコンテンツを広めるため、政治的イデオロギーを宣伝するため、評判を損なうために広く使用されています。よく知られている例として、米国下院議長 Nancy Pelosi 氏の 2019 年[16] の動画があります。このビデオでは、彼女のスピーチが不明瞭で、酔っているように見えます。効果を出すため動画はスロー再生されていたことがすぐにわかりましたが、元の動画とコンテキストが明らかになる前に「チープ フェイク」が広範囲に広がりました。

メディア コンテンツを改変するより高度なアプローチとして、高度な AI 技術を使って (a) 純粋に合成メディアを作成し、(b) 既存のメディアに高度な編集を加えるアプリケーションがあります。ディープフェイクという用語は、最先端の AI 技術を使って作成された合成メディアを指して使用されることがよくあります (名前は、ときどき使用されるディープ ニューラル ネットワークに由来します)。これらのテクノロジは、スタンドアロンのアプリ、ツール、サービスとして開発されており、既存の市販およびオープン ソースの編集ツールに統合されています。

このようなテクノロジが、個人や公共機関に損害を与えるため、悪意のあるアクターによって兵器化されています。ディープフェイク手法の例を次に示します。

- **顔の入れ替え (動画、画像)**—ビデオ内の顔を別の顔に置き換えます。この手法を使うと、個人、企業、または公共機関の脅迫を試みたり、個人を恥ずかしい場所や状況に置いたりすることができます。
- **操り (動画、画像)**—動画を使って静止画像や別の動画をアニメーション化します。これにより、個人が恥ずかしい発言や誤解を招く発言をしているように見えることがあります。
- **敵対的生成ネットワーク (動画、画像)**—写真のようにリアルな画像を生成するための手法ファミリー。
- **トランスフォーマー モデル (動画、画像、テキスト)**—テキストの説明からリッチな画像を作成します。

このように高度な AI ベースの手法は、現在のサイバー影響工作キャンペーンではまだ広く使用されていませんが、ツールが使いやすく、広範囲に入手できるようになるにつれて、問題が増加すると予想されます。

合成メディア操作の影響

情報操作を使って損害を与えたり、影響力を拡大したりする手法は新しいものではありません。しかし、情報が広がるスピードと、事実とフィクションをすぐに見分けることができないという現実は、Pelosi 氏の例に示されているように、フェイクや他の悪意のある合成メディアによる影響と損害がはるかに大きくなる可能性があることを意味します。

市場操作、決済詐欺、音声フィッシング、なりすまし、ブランド ダメージ、評判被害、ボットネットなど、考慮すべき損害のカテゴリがいくつかあります。これらのカテゴリの多くは、現実世界の事例として広く報告されており、事実とフィクションを切り離す私たちの能力が損なわれる可能性があります。

より長期的で狡猾な脅威は、見て聞いたものを信頼できなくなった場合に何が真実であるかを理解できなくなることです。このため、有名人でも一般人でも名誉を傷つけるような画像、音声、動画はフェイクとして無視することができます。これは、嘘つきの分け前 (The Liar’s Dividend) として知られる結果です。[17] 最近の調査[18] によると、テクノロジのこのような乱用は既に金融システムの攻撃に使用されていますが、他の多くの乱用シナリオも起きるものと思われます。

合成メディア

(続き)

合成メディアの検出

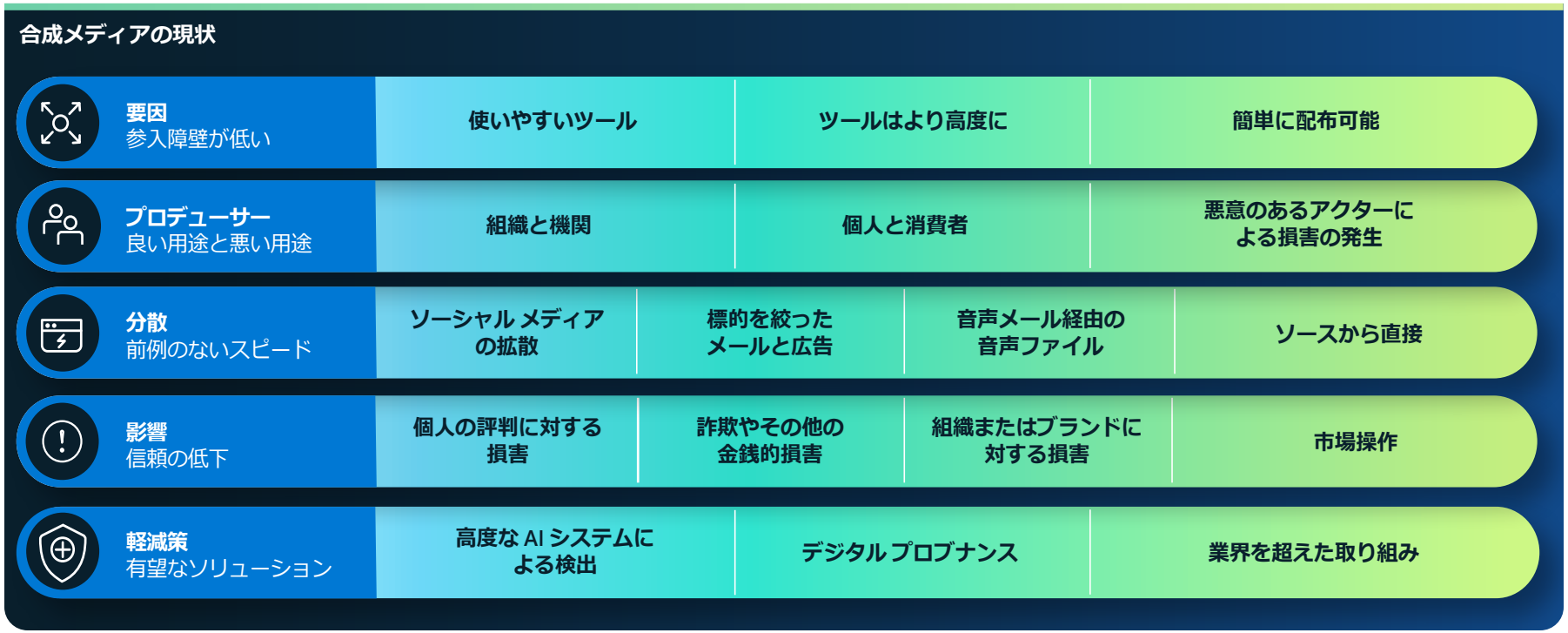
合成メディアを検出して軽減し、信頼を回復するためのより良い方法を生み出すため、業界、政府、学界にまたがった取り組みが進められています。いくつかの進捗があり、考慮すべきハードルもあります。

1 つのアプローチは、フェイクを見つけることができる AI ベースのシステムを構築することです。本質的には、攻撃的な AI システムに対抗するための「防御」AI システムです。これは、合成の音声および動画を作成する現在のシステムによって、トレーニングされたメディア フォレンジック アナリストや自動化ツールが特定できる隠し通すことのできない成果物が残る、アクティブな研究分野です。

残念ながら、現在のフェイクは弱点がありますが、正確な成果物は特定のツールまたはアルゴリズムに固有のものになる傾向があります。つまり、既知のフェイクに対するトレーニングは、ディープフェイク画像検出ツールを構築する 2020 年のオープン コンペティションで実証されたように、通常は他のアルゴリズムに一般化できないことを意味します。[19] より高度な検出ツールの開発への投資を増やすことは魅力的ですが、マイクロソフトは、次の 2 つの理由から、これにより意味のある改善がもたらされるかどうかについては懐疑的です。

まず、マイクロソフトには、実世界を反映した優れた物理モデルがあります。現在のフェイク クリエイターは近道をして検出可能な成果物を作成していますが、新しいモデルはこれまで以上にリアルになります。コンピューターでモデル化できないカメラによって撮影された現実世界の景色について、本質的に特別なことは何もありません。

次に、高度なフェイク作成アルゴリズムは、作成プロセスの一部に敵対的生成ネットワーク (GAN) と呼ばれる手法を使用しています。GAN は、Generator (生成者) を使って 2 つの AI システムを相互に実行し、フェイクと Discriminator (識別者) を作成することでフェイク画像を検出して Generator (生成者) をトレーニングします。より優れた検出ツールの開発に投資しても、Generator (生成者) がフェイクの品質を向上させることができるようになるにすぎません。



合成メディア

(続き)

デジタル資産の出所

フェイクを確実に検出できない場合、合成メディアの有害な利用から保護するために何ができるでしょうか。重要な新しいテクノロジとしてデジタル プロブナンスがあります。デジタル メディアの作成者が資産を認証できるようにし、そのデジタル資産が改ざんされているかどうかを消費者が識別できるようにするメカニズムです。コンテンツがインターネットを移動するスピードと、悪意のあるアクターがコンテンツを簡単に操作できることを考えると、デジタル プロブナンスは、現在のソーシャル メディア ネットワークのコンテキストにおいて特に重要です。

デジタル プロブナンス テクノロジは、最新バージョンの暗号ドキュメント署名であり、現在の Web を流れるオブジェクトのソース、編集履歴、メタデータをキャプチャすることを目的としています。この種のエンド ツー エンドのメディア改ざん防止証明書を実現するためのビジョンと技術的手法は、マイクロソフトの研究者と科学者の合同チームによって開発されました。マイクロソフトは、Project Origin (マイクロソフト、BBC、CBC/Radio-Canada、New York Times が設立) において、メディア プロブナンス テクノロジを実用化することを目的とした業界横断的なパートナーシップを共同でリードしており、Content Authenticity Initiative (Adobe が設立) に参加しています。さらに、マイクロソフトは、テクノロジおよびメディア サービスのパートナーと協力し、Coalition for Content Provenance and Authenticity (C2PA) を設立しました。C2PA は、画像、動画、音声、テキストなどのメディア資産を活用するため、最も先進的なデジタル プロブナンス仕様を最近発表した標準化組織です。

C2PA に対応したオブジェクトには、オブジェクトとメタデータを改ざんから保護するマニフェストが添付されており、それに付随する証明書が発行元を識別します。

合成メディアはもともと被害をもたらす目的で作られたわけではありませんが、個人や公共機関の信頼を低下させるために悪意のあるアクターによって兵器化されています。

デジタル プロブナンスは、メディア資産の出所を証明することによって、オンライン メディア コンテンツに対する人々の信頼を回復できる可能性がある有望な新しいテクノロジです。

C2PA 仕様に基づいて公開されたソリューションは、既存製品の新機能として、または新しいスタンドアロンのアプリおよびサービスとして登場しています。一般的に使用されているキャプチャ、編集、オーサリング ツールの大部分は、数年のうちに C2PA に対応すると予想されます。これは、企業がデジタル プロブナンスのニーズと用途を今すぐ判断し、既存のワークフローで使っているツールにこの追加の保護レイヤーを要求する機会を示しています。

実用的なインサイト

1. PR とコミュニケーションの対応をプロアクティブに検討することにより、誤情報の脅威から組織を保護するための予防的な対策を講じます。
2. 公式のコミュニケーションを保護するため、プロブナンス テクノロジを使用します。

詳しい情報のリンク

- 偽情報に対する有望な一歩 | Microsoft On the Issues
- 「A Milestone Reached」、2022 年 1 月 31 日
- Project Origin | Microsoft ALT Innovation
- Coalition for Content Provenance and Authenticity (C2PA)
- メディア認証におけるシステム Project Origin の使用に関する技術的な詳細について | Microsoft ALT Innovation

900%

2019 年以降、ディープフェイクが年々増加しています。[20]

サイバー影響工作から保護するための包括的なアプローチ

マイクロソフトは、既に成熟したサイバー脅威インテリジェンス インフラを基に、サイバー影響工作に関するより広範で包括的な見解を作成しています。

マイクロソフトは、工作活動によってもたらされる脅威に対抗するため、推奨される対応および軽減戦略の枠組みを使用しています。これは、4 つの主要な柱、つまり検出、妨害、防御、阻止に分けることができます。

さらに、マイクロソフトはこの分野での取り組みを進めるため、4 つの原則を採用しています。1 つ目は、表現の自由を尊重し、マイクロソフトのプラットフォーム、製品、サービスを通じて情報の作成、公開、検索を行うお客様の能力を維持するという約束です。2 つ目として、マイクロソフトのプラットフォームと製品が、国外からのサイバー影響工作に関するサイトとコンテンツの拡散に利用されないよう積極的に取り組んでいます。3 つ目として、国外からのサイバー影響工作に関するコンテンツやアクターから故意に利益を得ることはありません。最後の点として、社内データおよび信頼できるサードパーティのデータを製品に活用することにより、表示されるコンテンツに優先順位を付けて国外からのサイバー影響工作に対抗します。

検出

サイバー防衛と同様、国外からのサイバー影響工作に対抗するための第一歩は、検出する能力を育成することです。単一の企業や組織が個別に、必要な手順を進めることは期待できません。テクノロジ業界全体にわたる新しい広範なコラボレーションが重要になります。これにより、学術機関や非営利団体など、市民社会の役割に大きく依存しながら、サイバー影響工作の分析と報告を進めることができます。

この役割を認識しているプリンストン大学の Jake Shapiro 氏と Carnegie Endowment for International Peace の Alicia Wanless 氏は、新しい「Institute for Research on the Information Environment」(IRIE) を開設する計画を策定しました。マイクロソフト、Knight Foundation、Craig Newmark Philanthropies からの支援を受けた IRIE は、欧州原子核研究機構 (CERN) の後にモデル化された包括的なマルチステークホルダー研究機関を創設する予定です。データの処理と分析に関する専門知識を組み合わせて、この分野における新たな発見を加速させ、拡大していきます。調査結果は、政策立案者、テクノロジ企業、消費者に対して広範囲に報告されます。

防御

2 つ目の戦略の柱は、民主的な防御を強化することです。これは、投資とイノベーションが必要な長年にわたる優先事項です。これは、テクノロジが民主主義にもたらした課題と、民主主義的な社会をより効果的に守るためにテクノロジがもたらした機会を考慮に入れる必要があります。

マイクロソフトの戦略フレームワークは、分野横断的なステークホルダーがプロパガンダ (特に国外の攻撃者によるキャンペーン) を検出、妨害、防御、阻止できるようにすることを目的としています。

現代のテクノロジに関する大きな課題の 1 つである、インターネットとデジタル広告が従来のジャーナリズムに及ぼす影響から始めるのが適切です。1700 年代以降、自由で独立した報道は、地球上のあらゆる民主主義を支える点で特別な役割を果たしてきました。腐敗を明らかにして、戦争を文書化し、現在も過去も最大の社会的課題に光を当ててきました。しかし、インターネットは広告収入を吸い上げて有料購読者を遠ざけることにより、ローカル ニュースを骨抜きにしてきました。多くの地方紙が破綻しています。マイクロソフトが最近得た数多くのインサイトの 1 つは、新聞のない町が必然的結果として、平均的な量より多くの国外からのプロパガンダに無意識のうちにさらされているということです。こうした理由から、民主主義の重要な防衛策の 1 つは、従来のジャーナリズムと自由な報道を特に地方レベルで強化することです。これには、継続的な投資とイノベーションが必要であり、さまざまな国や大陸の現地のニーズを反映させる必要があります。これは簡単な問題ではありません。マルチステークホルダーのアプローチが必要なため、マイクロソフトやその他のテクノロジ企業が支援を強化しています。

さらに、公共政策における新たなイノベーションも必要で、公共の優先事項とする必要があります。これには、出版社が集団でテクノロジ企業と広告収入を交渉できるようにする法律や、地方のニュース編集室で雇用されるジャーナリストに対して所得税の一部を軽減するための税控除を認める法律が含まれます。ジャーナリストには、合法的な情報源からのコンテンツと不正な情報源からのコンテンツを分ける機能など、多くのツールを使えるようにする必要があります。

さらに、消費者が国家主導の情報操作を見分けるより高度な能力を育成できるようにするというニーズも急速に高まっています。これは手ごわい問題に見えるかもしれませんが、他のサイバー脅威に対抗するため、テクノロジ部門が長年にわたって追求してきた作業に似ています。スパムや他の不正なコミュニケーションを見つけるため、メール アドレスを注意深く確認するよう消費者を教育ことを検討してください。米国のイニシアチブ (News Literacy Project や Trusted Journalism)。

より長期的で狡猾な脅威は、見て聞いたものを信頼できなくなった場合に何が真実であるかを理解できなくなることです。

サイバー影響工作から保護するための包括的なアプローチ

(続き)

Program など) は、ニュースや情報をより的確に理解するよう消費者を育成するのに役立ちます。世界的には、NewsGuard のブラウザー プラグインのような新しいテクノロジにより、この取り組みをよりすばやく進めることができます。

これはまた、市民の教育が民主主義の基盤の一部であることも私たちに思い起こさせてくれます。やはり、この取り組みは学校で始める必要があります。しかし、私たちは生涯を通して公民教育を継続的に受けなければならない世界に住んでいます。Center for Strategic and International Studies が主導し、マイクロソフトが就任署名者およびパートナーとなった「Civics at Work」という新しい誓約は、企業コミュニティ内における市民リテラシーの再活性化を目指しています。これは、民主的な防御を強化するための幅広い機会として良い例です。

中断

近年、マイクロソフトのデジタル犯罪対策ユニット (DCU) は、ランサムウェアからボットネット、国家レベルの攻撃に至るまで、サイバー脅威を妨害するための戦術を調整し、ツールを開発しました。さまざまなサイバー攻撃に対抗する点での積極的な妨害の役割を始めとして、多くの重要な教訓が得られました。

サイバー影響工作への対抗について考えると、妨害はさらに重要な役割を担う可能性があり、妨害へのベストなアプローチがより明確になっています。まん延するごまかしに対する最も効果的な対抗手段は、透明性です。マイクロソフトが、国外からのサイバー影響工作の検出と対応に特化した大手サイバー脅威分析および研究企業である Miburo Solutions を買収することによって、国家レベルの影響工作を検出および妨害する能力を強化したのはそのためです。

マイクロソフトの経験によると、政府、テクノロジ企業、NGO は、サイバー攻撃を十分な証拠に基づいて慎重に特定する必要があります。こうした妨害の影響を理解することは非常に重要であり、サイバー影響工作の妨害にさらに貢献する可能性もあります。フェイクのグラフィック動画を使用する企てのように、特定のキャンペーンを含むロシアの計画を暴くなど、ロシアによるウクライナ侵攻の準備において透明性を確保した米国政府の情報共有をご覧ください。

ジュネーブの CyberPeace Institute がウクライナ国内外における継続的なサイバー攻撃について昨年の夏発表したように、幅広い市民社会と民間組織がサイバー影響工作に関する透明性を高める機会があります。新たに発見され、適切に文書化された工作活動に関する信頼性の高いレポートは、特にインターネット上で読んだり見たり聞いたりした情報を適切に評価するのに役立ちます。この目的を達成するため、マイクロソフトは既存のサイバー レポートを構築して拡張し、必要に応じて特定に関する声明を含む、サイバー影響工作に関する新しいレポート、データ、最新情報をリリースします。データ主導型のアプローチを使った年次報告書を発行し、国外における情報操作のまん延や、段階的な改善を確実に行うための次のステップについて、社内全体を見渡します。さらに、この種の透明性を基に構築される追加のステップについても検討します。

デジタル広告の役割は特に重要です。たとえば、広告は国外の事業に資金を提供できると同時に、他の国家が支援しているプロパガンダ サイトが合法であるかのように見せることもできます。このような財務フローを妨害するには、新たな取り組みが必要となります。

阻止

最後の点として、国際ルールへの違反に対する説明責任がない場合、国家が行動を変えることは期待できません。そのような説明責任を果たすことは、もっぱら政府の責任です。それでも、マルチステークホルダーの行動は、国際規範の強化と拡大において重要な役割を担っています。30 を超えるオンライン プラットフォーム、広告主、出版社 (マイクロソフトを含む) は、最近更新された欧州委員会の偽情報に関する行動規範に署名しており、重要さを増すこの課題に対処するための取り組みの強化に合意しています。最近のパリ コール宣言、クライストチャーチ コール宣言、未来のインターネットに関する宣言のように、多国間およびマルチステークホルダーの行動によって、民主主義国家間で政府と国民をまとめることができます。その後、政府はそれらの規範と法律に基づいて、世界の民主主義が必要としている説明責任を前進させることができます。

徹底的な透明性を迅速に実現する民主主義的な政府と社会は、国家レベルの攻撃の発生源を特定して、国民に情報を提供し、公的機関への信頼を築くことによって、影響工作キャンペーンを効果的に阻止することができます。

マイクロソフトは、国外からの影響工作を検出して阻止する技術的能力を高めており、サイバー攻撃に関する報告など、それらの工作活動について透明性を確保しながら報告することを約束しています。

実用的なインサイト

1. 組織全体に強力なデジタル衛生対策を導入します。
2. 意図しないサイバー影響工作キャンペーンの発生を、社員やビジネスの慣行により減らす方法を検討します。これには、国外の既知のプロパガンダ サイトへの供給を減らすことが含まれます。
3. 情報リテラシーと市民エンゲージメント キャンペーンを重要な要素として支援し、社会がプロパガンダや外国の影響から防御することができます。
4. 業界に関連するグループと直接関わり、影響工作に対処します。

巻末注

1. https://mitsloan.mit.edu/ideas-made-to-matter/mit-sloan-research-about-social-media-misinformation-and-elections?msclkid=8dc75d6abcfe11ecad9946a058d581c9
2. https://news.gallup.com/poll/355526/americans-trust-media-dips-second-lowest-record.aspx
3. ウクライナ防衛 : サイバー戦争から得られた初期の教訓 (microsoft.com)
4. https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022 Edelman Trust Barometer_FullReport.pdf
5. ロシア外務省の広報担当 Maria Zakharova 氏 : https://tass.com/politics/1401777; Lavrov: https://www.cnn.com/2022/05/05/opinions/sergey-lavrov-hitler-comments-ukraine-kauders/index.html,Kirill Kudryavtsev/Pool/AFP/Getty Images
6. https://apnews.com/article/conspiracy-theories-iran-only-on-ap-media-misinformation-bfca6d5b236a29d61c4dd38702495ffe
7. https://www.justice.gov/opa/pr/united-states-seizes-websites-used-iranian-islamic-radio-and-television-union-and-kata-ib
8. https://www.presstv.ir/Detail/2020/02/04/617877/Is-the-coronavirus-a-US-bioweapon
9. https://www.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf
10. https://www.rt.com/news/482405-iran-coronavirus-us-biological-weapon/
11. https://web.archive.org/web/20220319124125/https://twitter.com/RT_com/status/1233187558793924608?s=20
12. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
13. Russia’s Kremenchuk Claims Versus the Evidence—bellingcat
14. https://t.me/oddr_info/39658
15. https://t.me/voenacher/23339
16. Fact check: “Drunk” Nancy Pelosi video is manipulated | Reuters
17. https://lawcat.berkeley.edu/record/1136469
18. https://carnegieendowment.org/2020/07/08/deepfakes-and-synthetic-media-in-financial-system-assessing-threat-scenarios-pub-82237
19. Deepfake Detection Challenge Results: An open initiative to advance AI (facebook.com)
20. Deepfakes 2020: The Tipping Point、Johannes Tammekänd、John Thomas、Kristjan Peterson、2020 年 10 月

サイバー レジリエンス

最新化のリスクとメリットを理解することは、レジリエンスへの包括的なアプローチにとって非常に重要です。

サイバー レジリエンスの

概要

サイバー セキュリティは、テクノロジが成功を収める上で重要な要素となります。イノベーションと生産性向上を実現するには、最新の攻撃からの回復力をできる限り高めるセキュリティ対策を導入することが必要です。

パンデミックは、マイクロソフトの社員がどこで仕事をしていても保護できるよう、セキュリティ プラクティスとテクノロジを転換させる点で挑戦となりました。この 1 年間、脅威アクターは、パンデミック時に露呈した脆弱性と、ハイブリッド作業環境への移行を利用し続けてきました。それ以降、さまざまな攻撃方法の蔓延や複雑さと国家活動の増加に対応することがマイクロソフトの主な課題となってきました。

効果的なサイバー レジリエンスには、コア サービスとインフラへの進化する脅威に耐える包括的で適応性の高いアプローチが求められます。

詳しくは 89 ページをご覧ください

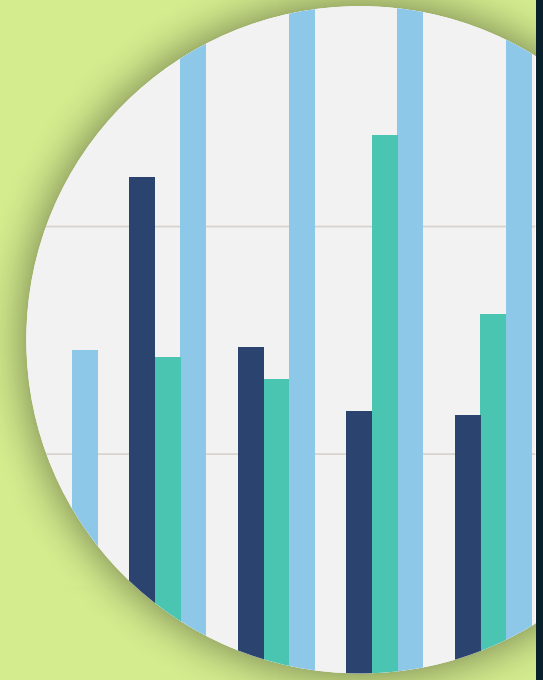
最新化されたシステムとアーキテクチャは、ハイパーコネクテッドな世界で脅威を管理するために重要です。

詳しくは 90 ページをご覧ください

基本的なセキュリティ対策は、高度なソリューションの有効性を決める要素です。

詳しくは 92 ページをご覧ください

パスワードベースの攻撃は依然として ID 侵害の主な原因ですが、他の種類の攻撃も発生しています。



詳しくは 93 ページをご覧ください

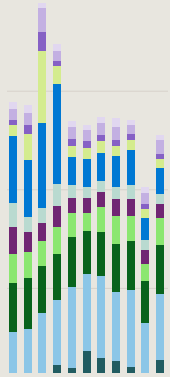
サイバー影響工作に対するレジリエンスの人的側面は、コラボレーションと協力を行う能力です。

詳しくは 102 ページをご覧ください

サイバー攻撃の成功の大部分は、基本的なセキュリティ対策を使って阻止できます。

詳しくは 108 ページをご覧ください

過去 1 年間、ボリューム、複雑さ、頻度の点で前例のない DDoS アクティビティが世界で発生しました。



詳しくは 98 ページをご覧ください

はじめに

パンデミックは、マイクロソフトの社員がどこで仕事をしていても保護できるよう、セキュリティ プラクティスとテクノロジを転換させる点で挑戦となりました。この 1 年間、脅威アクターは、パンデミック時に露呈した脆弱性と、ハイブリッド作業環境への移行を利用し続けてきました。それ以降、さまざまな攻撃方法の蔓延や複雑さと国家活動の増加に対応することがマイクロソフトの主な課題となってきました。

デジタル脅威に関連する活動とサイバー攻撃の巧妙さは日々高まっています。今日の複雑な攻撃の多くは、さまざまなレベルのセキュリティ制御を使って、ID アーキテクチャ、サプライ チェーン、サードパーティを侵害することに重点を置いています。特に、マイクロソフトの観察によると、ID フィッシング攻撃は明確に存在している脅威です。ただし、それらの種類の攻撃は通常、適切な ID 管理、フィッシング制御、エンドポイント管理のプラクティスによって防ぐことができます。そのため、攻撃の 98% は基本的な衛生対策を講じて阻止することができる、という基本を覚えておく必要があります。マイクロソフトは、ID とデバイスをゼロ トラスト アプローチの一環として管理しています。これには、最小特権アクセスとフィッシング耐性のある資格情報が含まれており、脅威アクターを効果的に阻止し、データを保護された状態に維持できます。

現在、高度な技術的スキルがない脅威アクターでも、高度な戦術、手法、手順へのアクセスをサイバー犯罪経済で広範に入手できるため、かなり破壊的な攻撃を仕掛けることができます。ウクライナにおける戦争は、ランサムウェアの使用を増やすことで、国家レベルのアクターが攻撃的なサイバー作戦をどのようにエスカレートさせたかを示しました。ランサムウェアは今、脅威アクターが二重三重の脅迫戦術を使って金銭を報酬を引き出し、開発者がサービスとしてのランサムウェアを (RaaS) 提供している高度な業界になりました。RaaS を使うと、脅威アクターはアフィリエイト ネットワークを利用して攻撃を行い、スキルの低いサイバー犯罪者が侵入するハードルを下げることができ、最終的には攻撃者プールの拡大につながっています。

そのため、マイクロソフトはランサムウェア除去プログラムを設計しました。このプログラムの目的は、制御と範囲のギャップを修正して、サービスの機能拡張に貢献し、ランサムウェア攻撃が発生した場合にマイクロソフトのセキュリティ オペレーション センターやエンジニアリング チームが使用する回復プレイブックを作成することです。

サプライ チェーンとサードパーティ サプライヤーに対する最近の攻撃は、業界の大きな転換点を示しています。こうした攻撃がお客様、パートナー、政府、マイクロソフトに与えている妨害は増え続けています。これは、セキュリティ ステークホルダー間のサイバー レジリエンスとコラボレーションに焦点を当てることの重要性を示しています。さらに、敵対者はオンプレミス システムを標的にしているため、インフラを最新化してセキュリティがより堅牢なクラウドに移行することで、レガシー システムによってもたらされる脆弱性を組織が管理する必要性が高まっています。

今は、セキュリティがテクノロジの成功の鍵となっている時代です。イノベーションと生産性向上を実現するには、最新の攻撃からの回復力をできる限り高めるセキュリティ対策を導入することが必要です。デジタルの脅威が増加して進化するにつれて、あらゆる組織のファブリックにサイバー レジリエンスを構築することが重要です。

Bret Arsenault
最高情報セキュリティ責任者 (CISO)

サイバー レジリエンス: コネクテッドな社会の重要な基盤

デジタル テクノロジの革命により、組織は、業務の方法と提供するサービスの両方において、より多くのつながりを持つようになりました。サイバー環境の脅威が増加するにつれて、組織のファブリックにサイバー レジリエンスを組み込むことは、財務や業務のレジリエンスと同じくらい重要です。

デジタル トランスフォーメーションは、組織が顧客、パートナー、社員、他のステークホルダーとやり取りする方法を絶えず変えてきました。新しいテクノロジによって、人と関わり、製品を変革し、業務を最適化するための大きな機会が生じています。パンデミックでは、あらゆる場所から新しい方法で共同作業できるようにするため、革新的なテクノロジを推し進めることによってデジタル トランスフォーメーションが加速しました。

サイバー脅威がまん延するにつれて、「いつでもつながっている」世界では、組織の侵害を防ぐのが難しくなっています。サイバー レジリエンスは、攻撃を受けても業務を継続し、成長のスピードを維持する組織の能力を表しています。予防は、生存能力と回復能力のバランスが取れている必要があります。政府と企業は、セキュリティとプライバシーにとどまらない包括的なモデルを開発し、資産、データ、他のリソースをサイバー レジリエンスの一部として保護しています。

サイバー レジリエンスに対する包括的なアプローチの策定

サイバー レジリエンスには、コア サービスとインフラへの進化する脅威に耐えることができる包括的で適応性の高いグローバルなアプローチが求められます。たとえば、次のとおりです。

- サイバー レジリエンスの正規分布に示されている基本的なサイバー衛生対策。
- デジタル トランスフォーメーションのリスク / メリットのトレードオフに対する理解と管理。
- 脅威と脆弱性のプロアクティブな検出を可能にするリアルタイム対応機能。
- 既知の攻撃からの保護と、新たな攻撃ベクトルや予測される攻撃ベクトルの予防アクティビティ (自動的に修復する機能など)。
- 障害の切り分けと分割による、攻撃と災害の影響の緩和。
- 中断が発生した場合の自動復旧と冗長性。
- ギャップを見つける運用テストの優先順位付けと、クラウドベースのセキュリティ ソリューションなどの外部リソースにおける共同責任と依存関係の把握。

効果的なサイバー レジリエンス プログラムでは、利用できるサービスを理解したり、中断が発生した場合に呼び出すことができるリソースの信頼できるカタログを用意したりするなど、リソースの基礎から始めます。この基礎を構築するには、独自の有効性の評価、重要なサービスのパフォーマンスとその依存関係の測定、オンプレミス サービスおよびクラウドサービス間での機能のテストと検証、組織のデジタル ライフサイクル全体での継続的な改善をプログラムが行える必要があります。

包括的なアプローチを実現するため、マイクロソフトは組織と提携し、最も重要なオンプレミス サービスとオンライン サービス、ビジネス プロセス、依存関係、担当者、ベンダー、サプライヤーを特定しています。さらに、お客様と市場の期待、規制および契約上の義務、社内業務に関連する資産とリソースを特定します。これらの重要なリソースを特定したら、脅威、中断、潜在的な攻撃ベクトル、システムおよびプロセスの脆弱性を検出して監視する取り組みを同時に行う必要があります。現在のスキル不足な状態でこれを行うには、組織に及ぶ全体的なリスクに基づいて厳しく優先順位を付ける必要があります。

この種類の包括的なアプローチは、継続的に進化する脅威の状況に合わせて適応させる必要があります。その際、測定可能なパフォーマンスの向上、検出、対応、復旧にかかる時間の短縮、中断が発生した場合に影響が及ぶ範囲の削減を目標とします。このアプローチでは、増え続ける脅威のつながりも認識する必要があります。たとえば、セキュリティ インシデントによってプライバシーに影響を与えるデータ侵害が発生した結果、社内外の多くのチームが連携してすばやく対応し、影響を最小限に抑える必要が生じる可能性があります。

サイバー レジリエンスは、企業が業務を継続し、サイバー攻撃などにより中断が発生しても成長スピードを維持する能力です。

実用的なインサイト

1. 侵害の影響を制限し、侵害が成功した場合でも安全かつ効果的に運用を継続できるようにするテクノロジ システムを構築して管理します。重要な共通資産に重点を置いて、俊敏性をサポートし、適応の高い設計 (ハイブリッドとマルチクラウド、マルチプラットフォームなど) を行って、攻撃対象を減らします (たとえば、使用していないアプリケーションや過剰にプロビジョニングされたアクセス権を削除するなど)。また、リソースの侵害を想定し、敵対者の進化を予測します。
2. デジタル プロジェクトを計画する際は、機会だけでなく潜在的な脅威や、デジタル テクノロジ サプライ チェーン (クラウドベースのセキュリティ ソリューションなど) 全体のレジリエンスに対する共同責任をも考慮に入れます。
3. セキュリティを意図的に組み込んだシステムを構築し、将来の進化する脅威に対して予測、検出、抵抗、適応、対応を行うための対策を講じます。
4. 新しい開発に伴うリスクを把握するため、ビジネス リーダーが必要に応じてセキュリティ チームに相談するようにします。同様に、セキュリティ チームは、ビジネスの目標について考え、目標を安全を追求する方法についてリーダーにアドバイスする必要があります。
5. サイバー インシデントに対する組織のレジリエンスを確保するための明確な運用プラクティスと手順を確実に導入します。

システムとアーキテクチャを最新化することの重要性

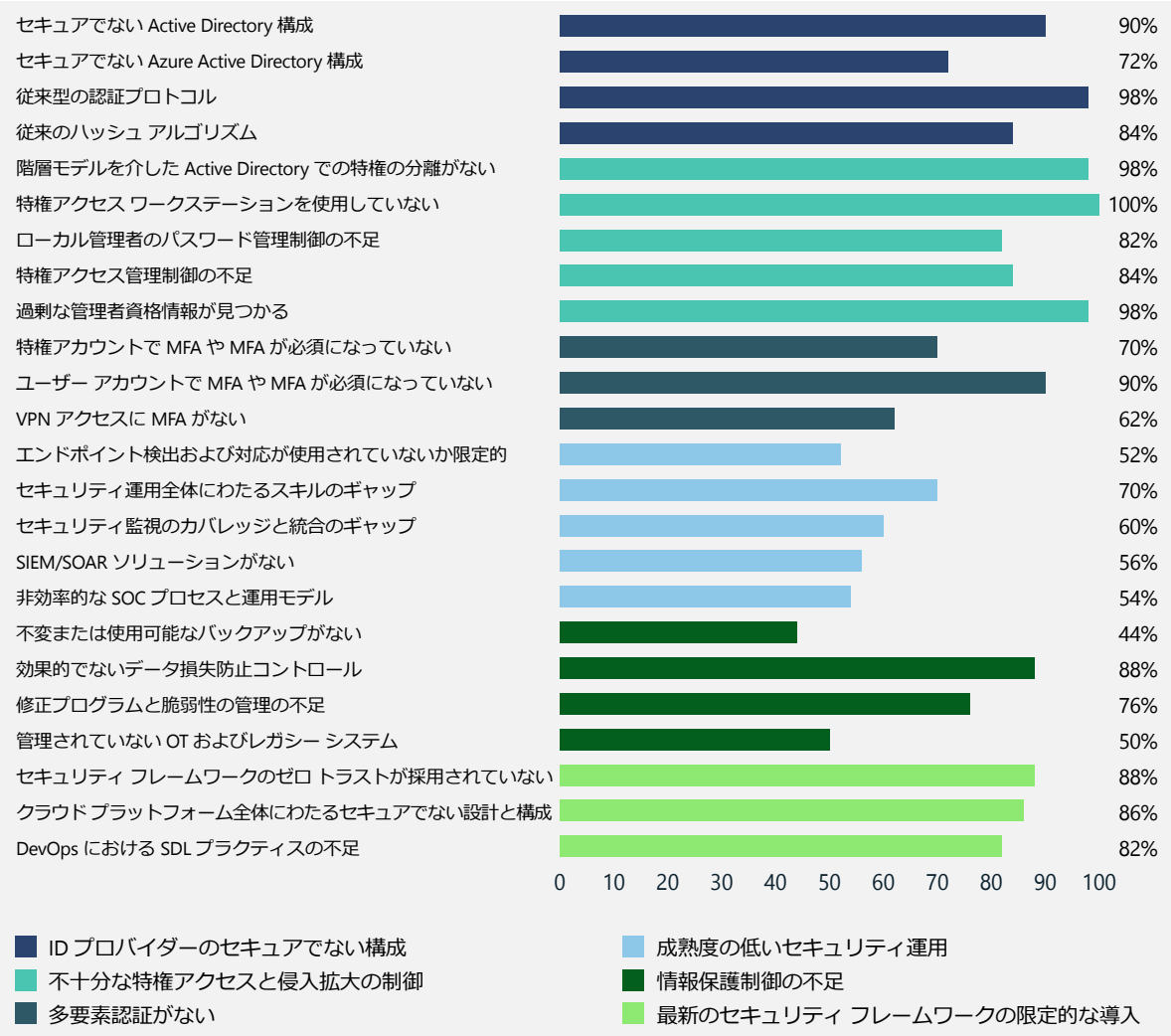
ハイパーコネクテッドな世界で新たな機能を開発するには、レガシー システムとソフトウェアによってもたらされる脅威に対処する必要があります。

レガシー システム (スマートフォン、タブレット、クラウド サービスなどの最新の接続ツールより前に開発され、標準になったシステム) は、まだ使用している組織にリスクをもたらします。このリスクの影響は、お客様が攻撃に対応して復旧できるように支援するセキュリティ担当者のグループである、Microsoft Security Services for Incident Response チームの調査結果によって裏付けられています。

過去 1 年間、攻撃から復旧したお客様の間で見つかった問題は、このページのグラフに示されている 6 つのカテゴリに関連していました。次のページでは、レジリエンスを向上させるための実行につながるステップについて概要を説明します。

セキュリティ インシデントの 80% 超は、最新のセキュリティ アプローチを通じて対処可能ないくつかの不足要素までたどることができます。

サイバー レジリエンスに影響を与える主な問題



このグラフは、影響を受けたお客様のうち、組織のサイバー レジリエンスを高めるのに不可欠となる、基本的なセキュリティ制御が不足しているお客様の割合を示しています。調査結果は、マイクロソフトによる過去 1 年間のエンゲージメントに基づいています。

「リーダーたちは、サイバー レジリエンスをビジネス レジリエンスの重要な側面として考える必要があります。自然災害や他の不測の事態に対処するのと同じ方法でサイバー障害を計画し、業務、通信、法務などの社内ステークホルダーを集めて戦略を立案する必要があります。そうすることで、組織は重要なビジネス システムをできるだけすばやくオンラインに戻し、通常業務を再開することができます。

ただし、それで終わるわけではありません。多くの組織がサードパーティのサプライヤーやサービス プロバイダーに依存しているため、リーダーたちは、サイバー レジリエンス計画をエンド ツー エンドのバリュー チェーンに拡張し、ビジネスの継続性とレジリエンスをさらに強化する必要があります。」

Ann Johnson、
セキュリティ、コンプライアンス、ID、および管理ビジネス開発コーポレート バイス プレジデント

システムとアーキテクチャを最新化することの重要性

(続き)

アプローチを最新化し、脅威から保護するために組織が対処できる明確な分野があります。

課題	実行につながるステップ
ID プロバイダーのセキュアでない構成 ID プラットフォームとそのコンポーネントの構成ミスと露出は、権限が高いアクセスを許可なしに獲得するための一般的なベクトルです。	AD や Azure AD インフラなどの ID システムを展開および維持するときは、セキュリティの構成ベースラインとベスト プラクティスに従ってください。 特権の分離、最小特権アクセスを適用したり、ID システムを管理する特権アクセス ワークステーション (PAW) を利用することで、アクセス制限を実装します。
不十分な特権アクセスと侵入拡大の制御 管理者がデジタル環境全体に対して過剰な権限を持ち、ワークステーションで管理者の資格情報を公開して、インターネットや生産性のリスクにさらされることがよくあります。	環境のレジリエンスを高めて攻撃の範囲を制限するため、管理アクセスを保護し、制限します。適時適切なレベルの管理だけでなく、特権アクセス管理制御を利用します。
多要素認証 (MFA) の不使用 最近の攻撃者は侵入するのではなく、ログオンします。	MFA は、重要かつ基本的なユーザー アクセス制御であり、すべての組織が有効にする必要があります。MFA を条件付きアクセスと組み合わせることにより、サイバー脅威との闘いにおいて非常に有効になります。
成熟度の低いセキュリティ運用 影響を受ける組織のほとんどは、従来の脅威検出ツールを使用しており、タイムリーな対応と修復に関する適切なインサイトを持っていませんでした。	包括的な脅威検出戦略には、機械学習を使ってシグナルからノイズを分離する、拡張検出および応答 (XDR) と最新のクラウド ネイティブ ツールへの投資が必要です。デジタル環境全体にわたる詳細なセキュリティ インサイトを提供する XDR を組み込むことにより、セキュリティ運用ツールを最新化します。
情報保護制御の不足 組織は、データの場所全体が対象となり、情報ライフサイクル全体で有効性が維持されて、データのビジネス上の重要度に沿っている、包括的な情報保護制御を構築するのに苦労しています。	重要なビジネス データとその場所を特定します。情報ライフサイクル プロセスを見直し、データ保護を実施すると同時に、ビジネス継続性を確保します。
最新のセキュリティ フレームワークの限定的な導入 ID は、さまざまなデジタル サービスやコンピューティング環境へのアクセスを可能にする新しいセキュリティ境界です。ゼロ トラストの原則、アプリケーション セキュリティ、他の最新のサイバー フレームワークを統合することで、組織は他の組織が予測するのに苦労しているかもしれないリスクにプロアクティブに対応することができます。	ゼロ トラスト フレームワークでは、最小特権の概念を適用し、すべてのアクセスを明示的に検証して、常に侵害を想定します。さらに、組織は、DevOps とアプリケーション ライフサイクル プロセスにおいて、ビジネス システムの保証レベルを高めるためのセキュリティ コントロールとプラクティスを実装する必要があります。

基本的なセキュリティ対策は、高度なソリューションの有効性を決める要素

マイクロソフトの分析を通じて、高度なセキュリティ ソリューションが存在する場合でも、攻撃者が初期アクセスを取得し、足がかりを得て攻撃を実施できるようになる盲点が、組織の防御にはよく存在することがわかりました。

多くの場合、サイバー攻撃の結果は攻撃開始かなり前に決まります。攻撃者は脆弱な環境を利用して、初期アクセスを取得し、監視を行い、侵入拡大、暗号化、または引き出しによって大損害を与えます。攻撃者を初期段階で阻止すれば、全体的な影響を軽減する可能性が大幅に高まります。

マイクロソフトでは、そのような環境で実際に適用されるプラクティスに最もよくある欠点を特定するため、セキュリティ対策の特定の構成を調査しました。その結果、人の手で操作されるランサムウェア攻撃の際に最もよく悪用される脆弱性を特定することができました。その脆弱性により、脅威アクターはネットワーク経由でアクセスして移動できるようになります。

基本的なセキュリティ構成を有効にする必要がある

オンボーディングされていないか、古くなっている組織のデバイス (脆弱性にもセキュリティ エージェントの状態にも関連している) は、攻撃者にとって潜在的なエントリ ポイントとアクセス確立ルートとなります。更新済みのエンドポイント検出および応答[1] (EDR) とエンドポイント保護プラットフォーム[2] (EPP) ソリューションを使って組織のデバイスをオンボーディングするのは重要なステップですが、ランサムウェアの停止は保証されないことがわかっています。

EDR や EPP などの高度なソリューションは、攻撃の早い段階で攻撃者を検出し、自動修復および保護を実現にする上で非常に重要です。しかし、これらの高度なソリューションは攻撃を検出する基本的な機能に依存しているため、基本的なセキュリティ構成を有効にする必要があります。実際、基本的なセキュリティ構成がないために攻撃された高度なソリューションで、このようなシナリオがよく見られました。

セキュリティ構成のベスト プラクティスは、セキュリティ オペレーション センター (SOC) アナリストの対応時間よりも高いレジリエンスを示します。

マイクロソフトは、お客様およびパートナーの集団全体において、SOC アナリスト 6 か月間に関連するアラートを確認して行動するのにかかる時間が 70% 削減されたことを観察しました。このような意識の向上は良い兆候です。しかし、セキュリティ構成の可視性によって SOC アナリストのパフォーマンスは向上しましたが、組織のデバイスのオンボーディングと更新によって製品の可視性を実現することは、効果的な予防のより大きな予測因子でした。

未知のデバイスによってもたらされるリスク

どの資産がどのオペレーティング システムで実行されているかを顧客が把握しているクラウド ネットワークとは対照的に、オンプレミス ネットワークには、組織によって監視または管理されていない、IoT、デスクトップ、サーバー、ネットワーク デバイスなどのさまざまなデバイスが存在することがあります。

平均的なエンタープライズ ネットワークには、EDR エージェントによって保護されていないコネクテッド デバイスが 3,500 台以上あり、エンタープライズ リソースや価値の高い資産にもアクセスできる可能性があります。Microsoft Defender for Endpoint (MDE) は、ネットワーク検出を使ってデバイスを検出し、デバイス名、オペレーティング システムのディストリビューション、デバイスの種類など、ネットワークに接続されているデバイスの分類に関する情報を提供します。

3,500

エンドポイント検出および応答エージェントによって保護されていない、企業内のコネクテッド デバイスの平均台数。

EDR エージェントによってサポートされていないデバイスについては、少なくともその存在を認識し、脆弱性を評価してネットワーク アクセスを制限することによって保護する行動を取る必要があります。

実用的なインサイト

1. 高度なソリューションであっても、基本的なセキュリティ構成がなければ攻撃される可能性があります。
2. 将来の攻撃から保護するため、セキュリティ対策構成のベスト プラクティスに投資します。これらの基本的な設定により、組織が攻撃から防御できるという点で、投資収益率が大幅に向上します。
3. 該当するすべてのデバイスを EDR ソリューションにオンボーディングします。
4. 必ず、セキュリティ エージェントを更新し、改ざんから保護して、製品の可視性と強化された保護のメリットを高めてください。

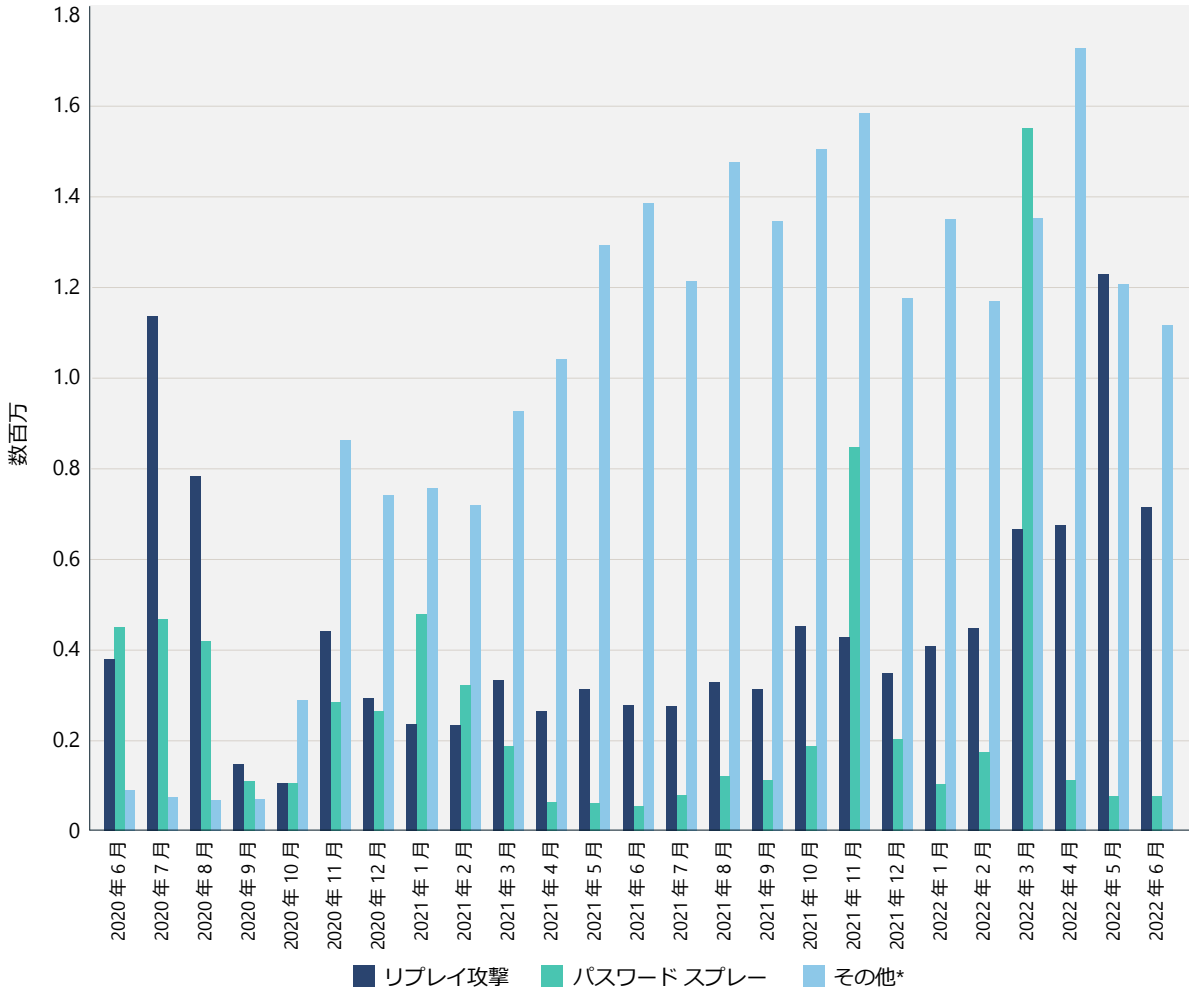
ID の正常性維持は組織の安心の基盤である

ID の保護は現在、かつてないほどの重要性を帯びた課題となっています。パスワードベースの攻撃は依然として ID 侵害の主な原因ですが、他の種類の攻撃も発生しています。巧妙な攻撃の量は、パスワード スプレーとリプレイ攻撃以前の基準と比べて増え続けています。

パスワードベースの攻撃は依然として一般的であり、この方法で侵害されるアカウントの 90% 以上は強力な認証で保護されていません。強力な認証では複数の認証要素 (パスワードに加えて SMS や FIDO2 セキュリティ キーなど) を使用します。

標的型パスワード スプレー攻撃の増加が見られており、数千もの IP アドレスで攻撃者トラフィックの量が急増しています。

侵害されたユーザー数 (攻撃カテゴリ別)



1 か月あたりの侵害されたユーザー数 (攻撃カテゴリ別) です。パスワード スプレー攻撃の量は、2021 年 11 月と 2022 年 3 月の急増に見られるように、大きく変動しました。これらの急増は、何千ものユーザーと何千もの IP アドレスに攻撃が試みられたことを表しています。*「その他」とは、フィッシング、マルウェア、中間者、オンプレミス トークン発行者侵害などを含む、パスワード スプレーやリプレイ攻撃以外の攻撃を指します。出典: Azure AD Identity Protection。

4,500

このステートメントを読んでいる間に、4,500 件のパスワード攻撃が防御されています。

ID の正常性維持は組織の安心の基盤である

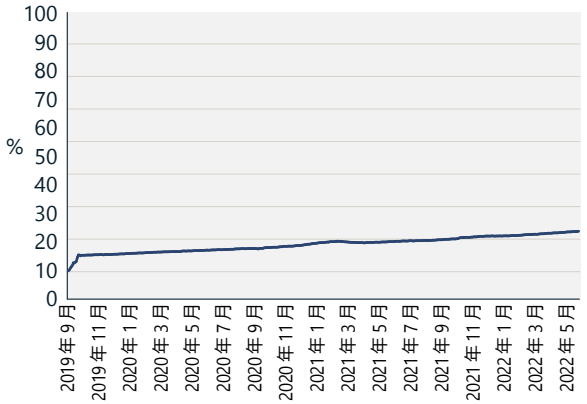
(続き)

強力な認証の導入

ポジティブな面としては、Azure Active Directory (Azure AD) のエンタープライズ カスタマー ベースでは強力な認証の採用が着実に増加しています。Azure AD では、強力な認証の月間アクティブ ユーザー数 (MAU) は、昨年 19% から 26% に増加しましたが、管理者アカウントに対する強力な認証の MAU は 30% から約 33% に増加しました。

これはポジティブな傾向ですが、強力な認証が過半数を占めるにはまだかなり増加が必要です。環境内で強力な認証をまだ使用していないお客様は、ユーザーを保護するための強力な認証の計画と展開を開始する必要があります。[3] 強力な認証の展開を設計する際は、最もセキュアで使いやすいエクスペリエンスを提供すると同時にパスワード攻撃のリスクをなくすため、パスワードレス認証を考慮してください。

強力な認証の使用
(2019 年 9 月～ 2022 年 5 月)

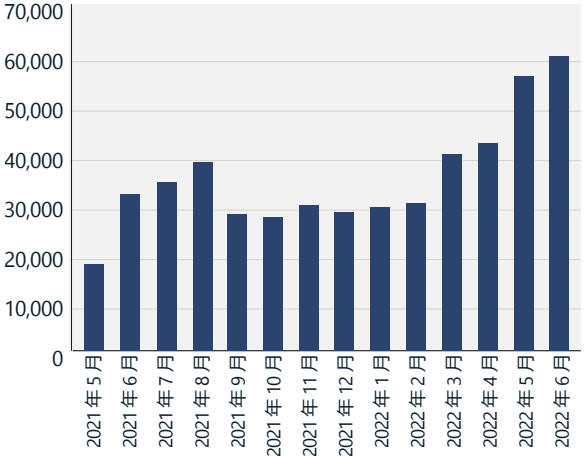


2019 年以降、強力な認証の使用率は 2 倍になりましたが、ユーザーのわずか 26%、管理者の 33% が強力な認証を使用しているにすぎません。出典 : Azure Active Directory。

トークン リプレイ攻撃の着実な増加

2022 年、他の形態の攻撃の割合が増加しました。パスワードベースの認証を明確に回避して検出の可能性を減らす、標的型攻撃が増加しました。それらの攻撃は、ブラウザーのシングルサインオン (SSO) Cookie を利用したり、マルウェア、フィッシング、その他の方法で取得した更新トークンを利用したりします。場合によっては、攻撃者は標的ユーザーの地理的な場所に近い場所にあるインフラを選択して、検出の可能性をさらに減らしています。トークン リプレイ攻撃は着実に増加しており、Azure AD Identity Protection で 1 か月あたり 4 万件以上が検出されています。トークン リプレイとは、前述のトークンを所持している攻撃者が、正当なユーザーに発行されたトークンを使用することです。トークンは一般に、ユーザーのブラウザーから Cookie を盗み出したり、高度なフィッシング手法を使ったりし、マルウェアを介して取得されます。

検出されたトークン リプレイ攻撃の量



1 か月あたりに検出されたトークン リプレイ攻撃の件数です。出典 : Azure AD Identity Protection (異常なトークン検出によってフラグが付けられた固有のセッション)。

ID の正常性維持は組織の安心の基盤である

(続き)

トークンの抽出

マルウェアだけでなく、攻撃者は目標を達成するために資格情報を必要としています。実際、人の手で操作されるランサムウェア攻撃の 100% に盗まれた資格情報が含まれています。巧妙な侵入の多くには、ダーク Web から購入した資格情報が含まれています。最初は、あまり高度でなく広範に分散している資格情報盗難マルウェアから盗まれたものです。このクラスのマルウェアは進化し、セッション情報や MFA クレームなどのトークンを盗み出せるようになりました。これは、ユーザーが企業資産にログインする際に使用するホーム システムが感染すると、企業ネットワーク上の重大なインシデントにつながる可能性があることを意味します。

攻撃者は、中間者攻撃を通じて被害者のデバイスからトークンを抽出することもできます。被害者は、フィッシング メールやインスタント メッセージ内の悪意のあるリンクをクリックし、ID プロバイダーの正規のサインイン ページと似ている Web サイトに誘導されます。実際には、これは攻撃者が稼働している Web サービスであり、ユーザーと ID プロバイダーの間のすべてのトラフィックを中継して傍受します。攻撃者は、ユーザー名とパスワードを傍受したり、MFA チャレンジを中継したりすることができます。ID プロバイダーによって発行され、攻撃者によって傍受された最終的なトークンには、MFA 要件を満たすために攻撃者が使用できる MFA クレームが含まれる場合があります。

Microsoft Defender for Cloud Apps は、2022 年の初頭から 1 か月あたり平均 895 件の攻撃を検出しました。この形式の攻撃は、証明書ベースの認証、Windows Hello for Business、FIDO2 セキュリティ キーなど、MFA のフィッシング耐性のある要素を使って防止できます。

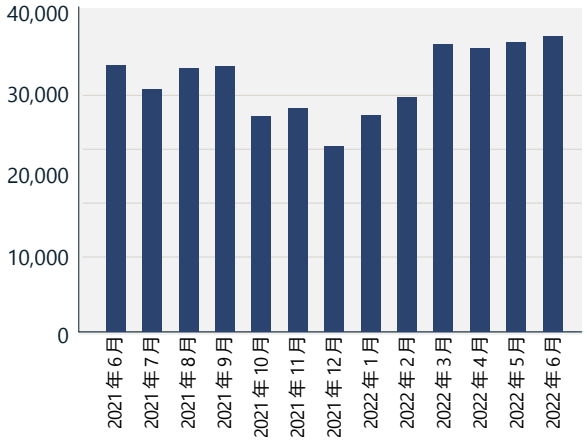
パスワードベースの攻撃は、アカウント侵害の主な方法です。

MFA 疲労

攻撃者は「MFA 疲労」という概念を利用し、被害者のデバイスに複数の MFA リクエストを生成します。被害者がうっかり、または疲れてリクエストを承諾することを期待したものです。この攻撃は、Microsoft Authenticator などの最新の認証アプリを、番号照合[4] や追加コンテキスト有効化[5] などの機能と組み合わせることで回避できます。Azure AD Identity Protection では、1 か月あたり 3 万件の MFA 疲労攻撃が行われたと推定されました。

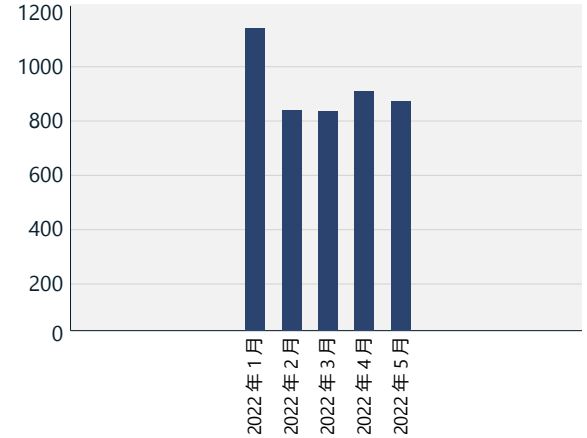
巧妙な攻撃の割合は増え続けており、多要素認証のフィッシング耐性のある要素の必要性が高まっています。

MFA 疲労攻撃の推定インスタンス数



出典 : Azure AD Identity Protection。

検出されたフィッシング インスタンスの後行われた中間者攻撃



出典 : Microsoft Defender for Cloud Apps。

実用的なインサイト

1. 組織のすべてのアカウントが強力な認証手段で保護されていることを確認します。
2. パスワードレス認証は、最もセキュアでユーザー フレンドリなエクスペリエンスを提供すると同時に、パスワード攻撃のリスクをなくします。
3. 組織全体でレガシー認証を無効にします。
4. フィッシング耐性のある形式の強力な認証によって、価値の高い情報と管理アカウントを保護します。
5. オンプレミス ID プロバイダーからクラウド ID プロバイダーへと最新化を行い、すべてのアプリをクラウドベースの ID プロバイダーに接続して、一貫性のあるユーザー エクスペリエンスとセキュリティを実現します。

詳しい情報のリンク

› 世界パスワードの日にパスワードの完全に捨てることを検討する | Microsoft Security

オペレーティング システムの既定のセキュリティ設定

セキュリティ脅威の状況は継続的に進化しているため、サイバー レジリエンスを高めるために、コンピューター セキュリティを既定で構成することがますます求められるようになっています。オペレーティング システムのセキュリティはかつてないほど緊急性が高く、複雑で、ビジネス クリティカルですが、十分に理解して管理するのが難しいことがあります。

これまで、コンピューターとデバイスのセキュリティにはセキュリティ機能が搭載されていましたが、お客様や IT 担当者が必要なレベルまで構成する必要がありました。このアプローチはもはや適切ではありません。攻撃者は、自動化、クラウド インフラ、リモート アクセス テクノロジを利用したより高度なツールを使って目的を達成しているからです。チップからクラウドまで、すべてのセキュリティ層が既定で構成されていることが重要になりました。マイクロソフトは、Windows オペレーティング システムのセキュリティが既定で構成されるように進化させました。[6]

多層的なセキュリティ対策、新しいセキュリティ機能、定期性と一貫性のある修正プログラムの適用、セキュリティ トレーニング、フィッシングやその他の詐欺を報告する意識など、お客様が防御を十分に認識していればマルウェアを減らすことができます。

多層防御を簡素化するため、Windows 11 では、メモリの整合性、セキュア ブート、トラステッド プラットフォーム モジュール 2.0 など、緊密に統合されたハードウェアおよびソフトウェア保護が既定で有効になっています。対応ハードウェアを利用している Windows 10 ユーザーも、Windows の設定アプリまたは BIOS メニューでこれらの機能を有効にできます。

それ古いデバイスでは通常、ハードウェアのセキュリティ技術とソフトウェアのセキュリティ技術の連携があまり強力ではありません。セキュリティが既定で有効になっていないデバイスの場合、可能であれば設定を使って手動で構成してください。[7]

セキュリティが既定で有効になっていないデバイスの場合、可能であれば設定を使って手動で構成することをお勧めします。

ハードウェアとソフトウェアのライフサイクル全体にわたって保護を実現するため、継続的なオペレーティング システムの更新プログラムとセキュリティ修正プログラムをプロアクティブに適用してください。

実用的なインサイト

1. トラステッド プラットフォーム モジュールでサインオン資格情報をバインドするパスワードレス ソリューションを使用します。具体的には、Faster Identity Online (FIDO) Alliance[8] 業界標準に準拠したパスワードレス ソリューションを採用してください。
2. 組織のデバイスに存在する、未使用の古い実行可能ファイルはタイムリーにクリーンアップします。
3. 既定で有効になっていない場合はメモリの整合性、セキュア ブート、トラステッド プラットフォーム モジュール 2.0 を有効にして (最新の CPU に搭載された機能を使って起動が強化されます)、高度なファームウェア攻撃から保護します。
4. データ暗号化と資格情報保護を有効にします。
5. アプリケーションとブラウザーのコントロールを有効にし、信頼できないアプリケーションからの保護や他の搭載されたエクスプロイト保護を強化します。
6. メモリ アクセス保護を有効にし、悪意のあるデバイスを外部からアクセス可能なポートに差し込むなど、無計画な物理的攻撃から保護できるようにします。

詳しい情報のリンク

- Windows Security Book | Commercial
- Windows 11 の新しいセキュリティ機能はハイブリッド ワークを保護するのに役立つ | マイクロソフト セキュリティブログ

ソフトウェア サプライ チェーンの中心性

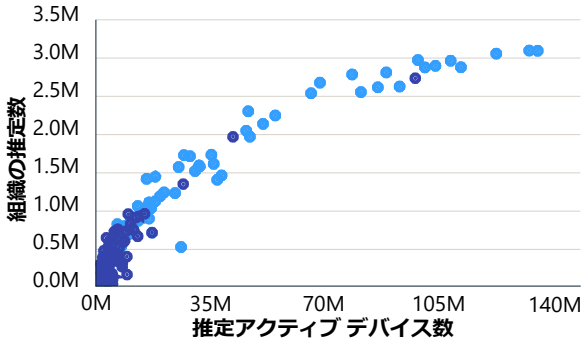
サードパーティ アプリ、プラグイン、拡張機能に対する攻撃によって、サプライ エコシステムにおいて中心的な役割を担うサプライヤーが顧客からの信頼を損なう可能性があります。ネットワーク理論を使ってソフトウェアの中心性を確認すると、修正プログラム適用の重要性 (特にセントラル アプリに関して) をよく理解できます。

1,800 万件のアプリケーション実行可能ファイルからなる Windows アプリ ネットワークは、500 万の組織でインストールおよび使用されているため、マイクロソフトのソフトウェア エコシステムを俯瞰的に把握することができます。最も使用されている 10 万件のアプリケーションのうち 97% は、サードパーティ組織によって生成されており、それらの組織が更新プログラムとセキュリティ修正プログラムを管理しています。これは、マイクロソフトの商用アプリケーション エコシステムについて 2 つの重要な特徴を意味しています。

1 つ目は、Windows の商用アプリケーション エコシステムの中心性です。(1,800 万件中) 上位 10 万件のアプリケーションだけが 1,000 を超えるデバイスで使用されています。言い換えると、デバイス エコシステムの中でそのような広範囲に及ぶ影響力を持っているのはこれらのアプリケーションの 0.5% 超にすぎません。

2 つ目に、それらのアプリケーションの管理しやすさにおける多様性です。上位 1 万件のアプリケーション サプライヤーは、最も使用されている商用アプリケーションの更新プログラムとセキュリティ修正プログラムを管理しています。これは、1 つの会社がソフトウェア サプライヤーの多様なセキュリティ、コンプライアンス、管理コントロールに相互依存していることを示しています。

最も使用されているアプリケーションの商業的普及



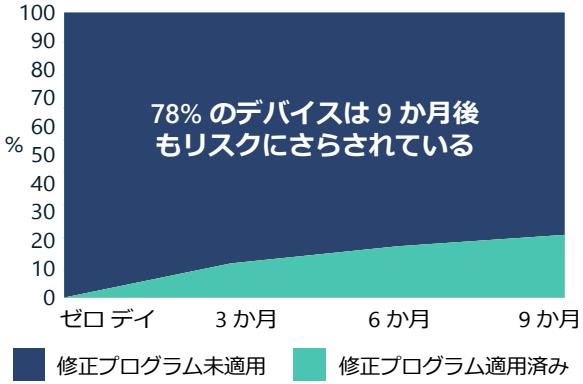
上位のアプリケーションは、何百万もの組織と何千万ものデバイスで使用されています。ほぼどこにでもあるため、攻撃者はそれらの上位アプリケーションの脆弱性を悪用しようとしており、ユーザーベースの何百万台ものデバイスに影響を与える可能性があります。

マイクロソフトは、修正プログラムがリリースされてから数か月経過した後も、あるいは製品サポート終了後から数年経過した後であっても、何百万台もの商用デバイスが脆弱なアプリケーション バージョンを使用しているのを観察しています。たとえば、2017 年以降サポートされていないバージョンの PDF リーダーを実行しているアクティブな Windows 商用デバイスは 100 万台以上あります。

サポートされていない古いバージョンのアプリケーションが、何百万台もの商用デバイスで今でもアクティブに使用されています。そのため、組織は修正プログラムが適用されない脆弱性というリスクにさらされています。

サポート対象のアプリケーション バージョンでは、重要な修正プログラムの適用スピードが頭打ちになっていることが観察されていますが、これではレジリエンスを促進することができません。むしろ、必要なレジリエンスを実現するため、1 か月あたりの修正プログラム適用数を大幅に増やす必要があります。

重要な修正プログラムの展開率



一連のブラウザーの 134 バージョンに影響を及ぼす重大な脆弱性を調査したところ、78% (つまり何百万台ものデバイス) が修正プログラムのリリースから 9 か月経過しても影響を受けるバージョンを使用していることがわかりました。

マイクロソフトは、InterpretML[9] ツールキットを使って、古いバージョンのアプリが搭載されたデバイスを使用している可能性が高い組織に関連する特性を特定しました。これらの予測因子の中で重要なものとして、デバイスでのエンゲージメントの時間が短い、アジア太平洋や中南米などの地理的地域、自動車、化学、電気通信、運輸およびロジスティクス、医療保険 (請求処理担当者)、保険などの業界がありました。

ソフトウェア レジリエンスの維持には、未使用のアプリケーションの定期的な無効化またはアンインストールを含める必要があります。

組織のセキュリティとコンプライアンスは、自組織の取り組みとソフトウェア サプライヤーの取り組みに依存しています。

実用的なインサイト

1. 組織全体ですべてのアプリケーションとエンドポイントにタイムリーな更新を実行します。
2. 組織のデバイスに存在する、未使用の古い実行可能ファイルはタイムリーにクリーンアップします。

詳しい情報のリンク

- Microsoft Intune ドキュメント | マイクロソフト ドキュメント
- アプリの管理 | マイクロソフト ドキュメント
- Microsoft Defender for Endpoint | Microsoft Security
- OSS セキュア サプライ チェーン フレームワーク | Microsoft Security Engineering
- Microsoft Open Source Software Secure Supply Chain Framework | GitHub

新しい DDoS、Web アプリケーション、ネットワーク攻撃に対するレジリエンスの構築

デジタル トランスフォーメーションの加速は、従来のネットワークおよびセキュリティ境界モデルに終焉をもたらしました。クラウドに移行に伴い、企業はデジタル資産を保護するためにクラウド ネイティブのネットワーク セキュリティを採用する必要があります。

攻撃の複雑さ、頻度、量は増え続けており、休暇シーズンに限ったものではなくなりました。これは、年間を通じた攻撃に移行したことを示しています。このことから、従来のようなピーク トラフィック シーズンではなく、継続的な保護の重要性を理解できます。

分散サービス拒否 (DDoS) 攻撃

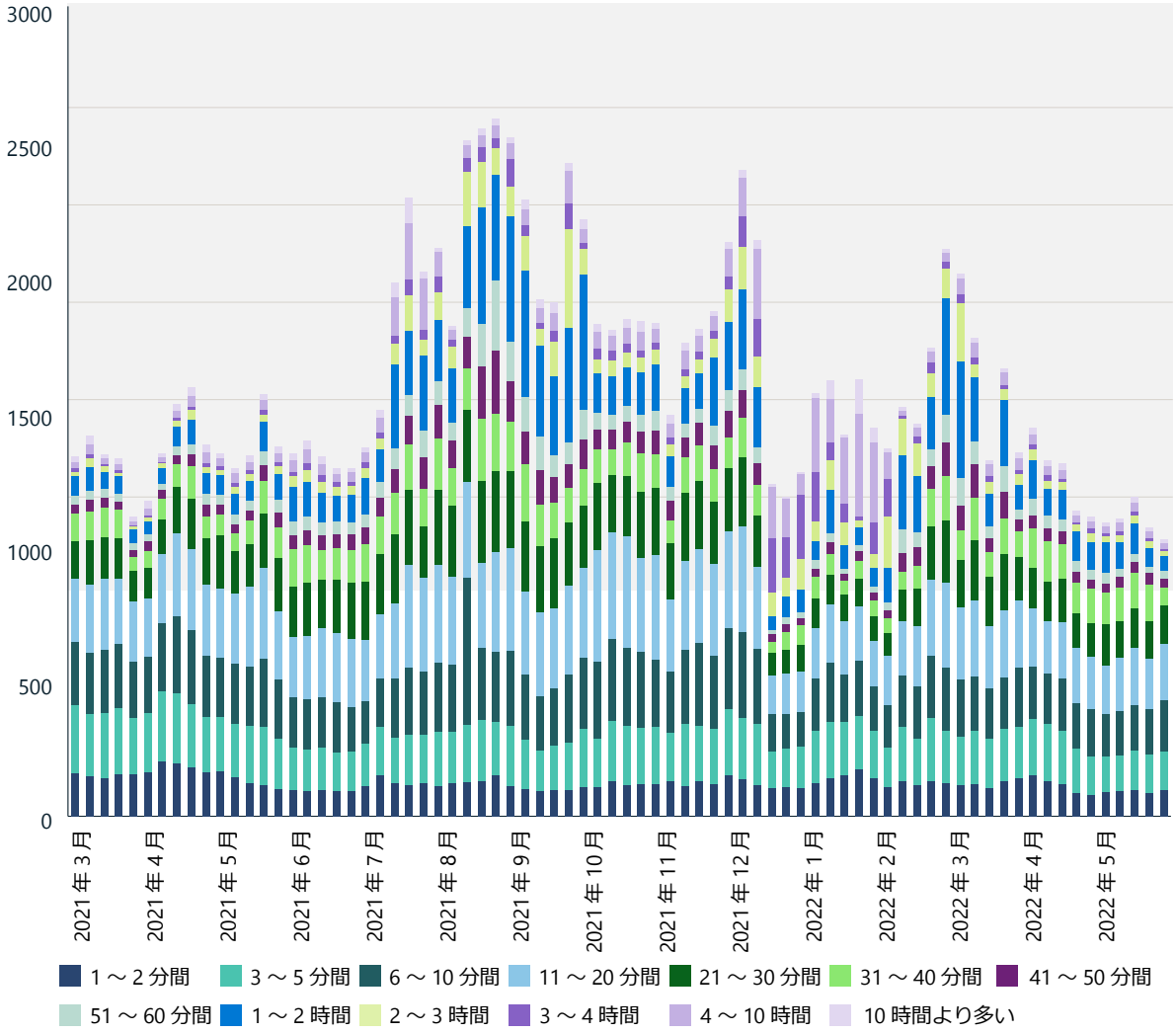
過去 1 年間、ボリューム、複雑さ、頻度の点で前例のない DDoS アクティビティが世界で発生しました。このような DDoS の急増は、国家レベルの攻撃の大幅な増加と、低コストの DDoS 請負サービスの広がりの結果生じました。マイクロソフトは、1 日あたり平均 1,955 件の攻撃を修正しており、前年比で 40% の増加です。これまで、攻撃の数がピークとなるのは通常、年末年始のシーズン中でした。しかし、今年は 1 日に最も多く記録を残したのは 2021 年 8 月 10 日です。これは、年間を通じた攻撃に移行したことを示している可能性があり、従来のようなピーク トラフィック シーズンではなく、継続的な保護の重要性を理解できます。

2021 年 11 月、マイクロソフトは、複数の国にまたがる約 1 万のソースから 3.4 テラビット / 秒 (Tbps) のスループットで実行された大量の DDoS 攻撃を阻止しました。似たような 2 Tbps 以上の大量攻撃は、2022 年に緩和されました。これは、攻撃の複雑さと頻度が高まっているだけでなく、攻撃の量 (帯域幅) も増えていることを強調しています。

攻撃の継続時間

この 1 年間に観測された攻撃のほとんどは短期間で終わりました。攻撃の約 28% は 10 分もかからず、26% は 10 ～ 30 分、14% は 31 ～ 60 分間でした。1 時間以上かかったのは、攻撃の 32% でした。

DDoS 攻撃の数と継続期間の分布
(2021 年 3 月～ 2022 年 5 月)



昨年の攻撃のほとんどは短時間で終わりました。攻撃の約 28% は 10 分もかかりませんでした。

新しい DDoS、Web アプリケーション、ネットワーク攻撃に対するレジリエンスの構築

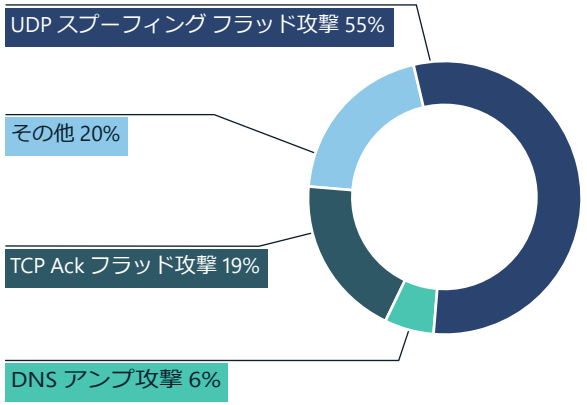
(続き)

DDoS 攻撃ベクトル

過去 1 年間よく利用された攻撃ベクトルは、ポート 80 におけるユーザー データグラム プロトコル (UDP) リフレクションであり、簡易サービス検出プロトコル (SSDP)、コネクションレス ライトウェイト ディレクトリ アクセス プロトコル (CLDAP)、ドメイン ネーム システム (DNS)、ネットワーク タイム プロトコル (NTP) を使って単一のピークを構成していました。さらに、Web サイトを標的としたアプリケーション レイヤーの DDoS 攻撃も増加し、ピーク RPS (1 秒あたりのリクエスト) は 1,630 万、ピーク トラフィックは 9.89 Tbps でした。

2022 年、マイクロソフトはほぼ 2,000 件の DDoS 攻撃を毎日修正し、史上最大の DDoS 攻撃を阻止しました。

DDoS 攻撃ベクトル



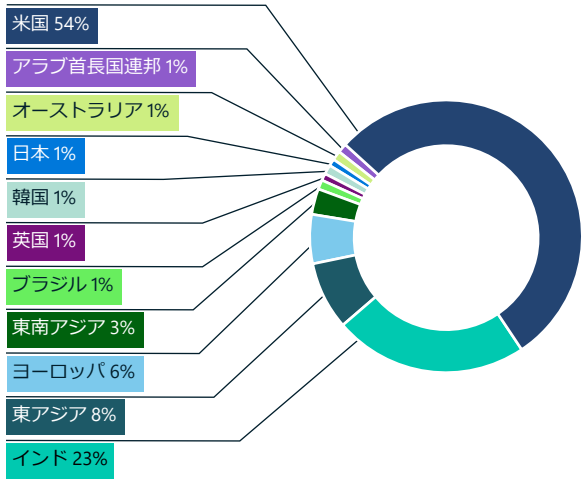
UDP スプーフィング フラッド攻撃は、2022 年前半の上位ベクトルへと上昇し、16% から 55% に増加しました。TCP Ack フラッド攻撃は、54% から 19% に減少しました。

ゲーム業界は、依然として DDoS 攻撃の主な標的となっています。ほとんどが Mirai ボットネットの変異体と少量の UDP プロトコル攻撃によるものです。UDP は一般的にゲームやストリーミング アプリケーションで使用されるため、攻撃のベクトルの圧倒的大部分は UDP スプーフィング フラッドであり、UDP リフレクションとアンプ攻撃は少数でした。

標的の地理的分布

過去 1 年間に検出された DDoS 攻撃のうち、54% は米国の標的に対して実行されました。この傾向は、Azure とマイクロソフトのほとんどのお客様は米国を拠点にしているという事実によって部分的に説明できるかもしれません。さらに、インドに対する攻撃も急激に増加し、2021 年後半は全攻撃のわずか 2% でしたが、2022 年前半には 23% になりました。東アジア (特に香港) は 8% の割合を維持しています。ヨーロッパでは、アムステルダム、ウィーン、パリ、フランクフルトの地域に攻撃の集中が見られました。

DDoS 攻撃の標的となった地域

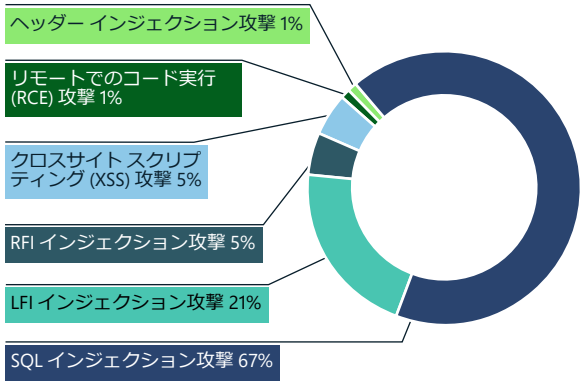


アジアにおける大量の攻撃は、ゲームのフットプリントが非常に大きい地域 (特に中国、日本、韓国、インド) が理由と考えられます。スマートフォンの普及によってモバイル ゲームの人気が高まるにつれ、このフットプリントは拡大していくでしょう。これは、この地理的標的はひたすら増加を続けることを示唆しています。

Web アプリケーションの悪用

Web アプリケーション ファイアウォール (WAF) と DDoS 保護を組み合わることで、Web およびアプリケーション プログラミング インターフェイス (API) の資産を保護する多層防御戦略の不可欠な部分が形成されます。マイクロソフトは、Azure WAF を介して 1 か月あたりにトリガーされた WAF ルールが 3,000 億件上昇したのを観察しました。

最も多く見られる攻撃の種類の分布



Azure WAF は、Open Web Application Security Project (OWASP) の攻撃トップ 10^{10} を毎日数十億件検出しています。マイクロソフトのシグナルによると、攻撃者が最も多く試みたのは SQL インジェクション攻撃で、その後にローカル ファイル インジェクション攻撃とリモート ファイル インジェクション攻撃が続きます。これは、件数の多い上位 3 つの Web 攻撃の種類としてインジェクション攻撃を示している OWASP トップ 10 リストと一致しています。

さらに、Azure Web アプリケーションに対するボット攻撃も増加しており、ボット リクエストは 1 か月あたり平均 17 億件で、悪意のあるボットで構成されるトラフィックの割合は 4.6% です。

新しい DDoS、Web アプリケーション、ネットワーク攻撃に対するレジリエンスの構築

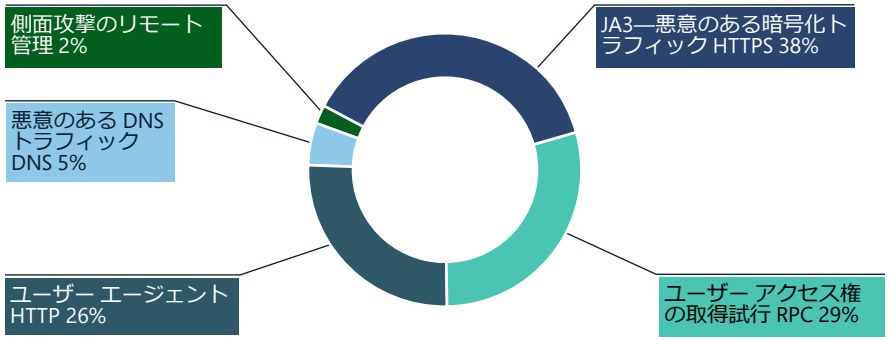
(続き)

資格情報スタッフィング攻撃、クレジット カード詐欺、サイバー影響工作キャンペーン、サプライ チェーン攻撃を実行するボットの数が増えているため、Web アプリケーションに対するボット攻撃が着実に増えることが予想されます。

ネットワーク侵入 : 検知と防止

2022 年は、ネットワーク レイヤーの悪用、特にマルウェアの大幅な増加が見られました。Azure Firewall の侵入検知および防止システム (IDPS) は、6 月だけで 1 億 5,000 万件以上の接続をブロックしました。

IDPS 拒否トラフィックの理由



IDPS トラフィック アラートの理由

IDPS アラートおよび拒否トラフィックの分析は、攻撃者によって以下のアプローチが使用されていることが示されています。拒否トラフィックでは、攻撃者が SSL を使ってアクティビティを隠しており、リモート実行攻撃がより一般的になっていることが確認されています。アラート トラフィックでは、リモート実行攻撃を実行するために SMB/SMB2 プロトコルが使用されていることが確認されています。

実用的なインサイト

1. データ センターまたはクラウド サービス内のシステム間のすべてのトラフィックと、それらにアクセスしようとしているトラフィックを検査します。
2. 年間を通じた堅牢なネットワーク セキュリティ対応戦略を策定します。
3. クラウド ネイティブ セキュリティ サービスを使って、堅牢なゼロ トラスト ネットワーク セキュリティ対策を導入します。

詳しい情報のリンク

- Azure Firewall でランサムウェア攻撃のセキュリティ防御を強化する | Azure ブログと最新情報 | Microsoft Azure
- DDoS アンプ攻撃の徹底分析 | マイクロソフト セキュリティ ブログ
- Azure Web Application Firewall によるエッジからクラウドへのインテリジェントなアプリケーション保護 | Azure ブログと最新情報 | Microsoft Azure

データ セキュリティとサイバー レジリエンスに対するバランスのとれたアプローチの策定

デジタル トランスフォーメーションにより、データ資産が大幅に増加し、セキュリティ、コンプライアンス、プライバシーのリスクが高まりました。サイバー レジリエンスのある組織は、データ保護、コンプライアンス、修復機能への投資をバランスよく行い、それらを専門的な規制対応プロセスと統合して、さまざまな種類の侵害に対処する必要があります。

データ侵害の問題は、起きるかどうかではなく、いつ起きるか、というものです。IBM と Ponemon Institute の調査「Cost of a Data Breach, 2021」では、全世界の平均データ侵害コストが 424 万米ドル (前年比 10% 増)、米国でのコストが 905 万米ドルと報告されています。コストを増幅させる最も大きな要素は、コンプライアンス違反であることが判明しました。逆に言うと、インシデント対応 (IR) 計画、ゼロ トラスト展開の成熟化、セキュリティ AI および自動化、暗号化の使用などのベスト プラクティスを実践すれば、侵害コストを削減できます。

データ侵害は避けられません。バランスのとれたレジリエンス アプローチを取る組織は、侵害の頻度、影響、コストを削減できます。

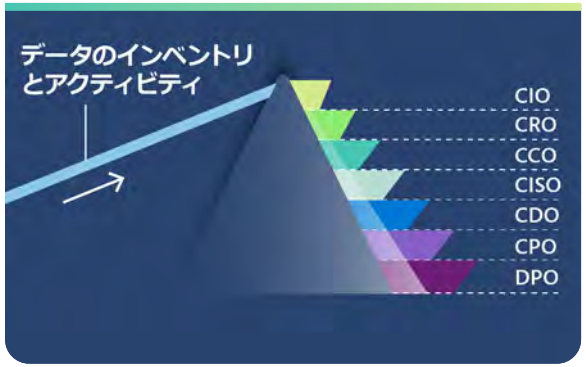
データ ガバナンス、セキュリティ、コンプライアンス、プライバシーは相互に依存している

近年、企業にとって重要な価値創造の原動力として、データ ゲインが目立っています。同時に、データ ガバナンスとセキュリティの両方を求めるプライバシー規制が登場したことで、リスクに関連する役割の境界があいまいになっています。最高データ責任者 (CDO) や最高プライバシー責任者 (CPO) などの新しい経営幹部レベルの役割は、セキュリティとコンプライアンスに対して既得権を持っていますが、データ保護の実装と運用化は多くの場合、最高情報責任者 (CIO) や最高情報セキュリティ責任者 (CISO) が率いるチームに依存しています。CDO が主導するデータ ガバナンスのイニシアチブにはセキュリティ上のメリットもあるため、一方通行ではありません。このような相互関連性があるため、IT、データ ガバナンス、セキュリティ、コンプライアンス、プライバシーの各チームは、効率を高めてリスクを管理するために、これまで以上に密接に協力する必要があります。

今後は組織全体のデータ資産に統合データ リスク管理プラットフォームが利用される

IT、データ ガバナンス、セキュリティ、コンプライアンス、プライバシー管理プロセスを連携させることは、分野ごとに特注したアプリケーションが使用されている環境では難しく、ハイブリッドでマルチクラウドなデータが不規則に拡大する一般的な組織では一貫性のある方法で対応できません。マイクロソフトは、データの特定と把握、データの保護、データのアクセス / 使用 / ライフサイクルの管理、データ資産でのデータ損失防止を行うことができる 1 つの画面が必要であると考えています。

同じデータ インベントリとアクティビティ情報を利用することで、チームをまたいだプロセスを円滑に進め、リスクをより包括的に把握できるようになり、組織は侵害への対応をより適切に準備して、合理化できるようになります。



「1 つの画面」はプリズムとして機能する必要があります。データのセキュリティ、コンプライアンス、プライバシーを担当する各チームには、連携してコラボレーションを行うため、同じデータ インベントリとアクティビティに関する一貫性のある別個のビューが必要です。データ アクティビティには、データのアクセス、変更、移動の各イベントが含まれ、これはデータ セキュリティ方程式の重要な部分です。

効果的なデータ ガバナンス、セキュリティ、コンプライアンス、プライバシーは相互に依存しており、チーム間のコラボレーションが必要です。

実用的なインサイト

1. コンプライアンス、データ保護、対応機能に投資することで、防御と修復を両立させ、データ侵害の影響を最小限に抑えます。
2. データ リスクのサイロにまたがるプロセスとツールを開発して導入し、データ資産全体をカバーします。

詳しい情報のリンク

- Microsoft Purview—データ保護ソリューション | Microsoft Security
- コンプライアンスとデータ ガバナンスの未来 : Microsoft Purview の導入 | マイクロソフト セキュリティ ブログ

サイバー影響工作へのレジリエンス : 人的側面

過去 5 年間、グラフィックと機械学習の進歩により、高品質でリアルなコンテンツをすばやく生成し、数秒でインターネットに広めることができる使いやすいツールが登場しました。

テキスト、音声、ビジュアル コンテンツを介して報告された出来事に関しては、人間もアルゴリズムも事実とフィクションを区別することができないところまで来ています。そのようなツールと出力が広まったため、すべてのデジタル メディアの信頼性に対する疑念が投げかけられており、地域や世界の出来事への理解が妨げられています。テクノロジの進歩によって可能になった新しい形の影響工作は、民主的プロセスにとって大きな意味を持っています。[11]

これらのサイバー攻撃工作に対してより回復力のある未来を作るために何ができるか、という疑問が生じています。テクノロジはパズルの 1 ピースにすぎません。メディア リテラシー、意識、用心を目的とした教育、質の高いジャーナリズムへの投資 (現場、現地、国内、国外の信頼できる記者)、影響工作に関する情報を共有して警告し合うネットワーク、欺くことを目的としたデジタル メディアを生成または操作した悪意のあるアクターを罰する新しい種類の規制など、さまざまな取り組みが行われています。

さらに、マイクロソフトは、デジタル コンテンツへの信頼を取り戻すことは、多様な視点と関与が求められる野心的な目標であると認識しています。これらの脅威を単独で解決できる企業、機関、政府はありません。人間の優れた能力は、コラボレーションと協力の能力です。これが特に重要なのは、すべての人 (世界中の政府、業界、学界、そして特にニュース、ソーシャル、メディアの各組織) が社会の改善と健康のために協力することが求められるからです。

詳しい情報のリンク

- 国防総省のサイバー ミッションにおける AI (人工知能) の適用 | Microsoft On the Issues
- Artificial Intelligence and Cybersecurity: Rising Challenges and Promising Directions. Hearing on Artificial Intelligence Applications to Operations in Cyberspace before the Subcommittee on Cybersecurity、上院軍事委員会、第 117 議会 (2022 年 5 月 3 日、Eric Horvitz 氏の証言)

スキル向上による人的要素の補完

人的要素への対応は、あらゆるサイバーセキュリティ スキル向上戦略の重要な要素です。Kaspersky の調査「Human Factor in IT Security」[12] によると、サイバーセキュリティ インシデントの 46% には、不注意や制服を着たスタッフが関与し、気づかないうちに攻撃を助長しています。

マイクロソフトのデジタル セキュリティおよびレジリエンス組織の教育および意識向上チームは、社員が自分自身とお客様のシステムおよびデータを保護できるようにすることで、サイバーセキュリティの人的要素を補完する責任を負っています。次のような目標を持っています。

- 全社規模で一元化されたコア セキュリティ スキルを全従業員に構築することで、マイクロソフトとお客様のリスクを軽減する。
- 求められる行動の結果を後押しする多段階のトレーニング強化アプローチによって、社員のセキュリティに関する知識を強化する。
- 毎年開催される必須のセキュリティ トレーニングとイベントを通じて、セキュリティの考え方をマイクロソフトの文化の本質的な部分にすることにより、文化の変化を促す。
- サイバーセキュリティ関連のあらゆる事柄について、ベスト プラクティス、会社のポリシー情報、インシデント レポートのための一元化されたワンストップの Web リソースを推進する。

ターゲットを絞った集中型のサイバーセキュリティ教育プログラムは、少なくとも年に 1 回すべてのマイクロソフト社員が受講しています。提供されるトレーニングは、現在のサイバーセキュリティ イニシアチブをサポートし、測定可能な行動の結果を生み出すことができるように最適化されています。マイクロソフトの情報リスク管理評議会 (IRMC) は、トレーニングによって対処すべき、サイバーセキュリティ行動の変化がもたらす重要な結果を特定する上で重要な役割を果たしています。

マイクロソフトは、すべてのサイバーセキュリティ教育プログラムを通じて、ソリューションの効率、有効性、結果をできる限り測定しています。たとえば、マイクロソフトのインサイダー脅威スキル向上プログラムは、トレーニング コンプライアンスが 95% であり、受講者の満足度が非常に高くなっています。また、社内の Report It Now ツールを使って潜在的なインサイダー脅威のケースを報告するマネージャーが大幅に増加しました。次のようなプログラムがあります。

セキュリティ基盤 : コア セキュリティとプライバシー プラクティスに対処する、全社規模で一元化されたサイバーセキュリティ意識向上およびコンプライアンス トレーニング。特に期待されているこのトレーニング シリーズでは、エデュテインメント モデルが採用されており、サイバーセキュリティに関する学習が興味深いものになっています。

STRIKE: 基幹業務ソリューションを構築して管理している技術者に必須となっている、マイクロソフトの技術トレーニング。この招待者制トレーニングでは、サイバーセキュリティ対策のベスト プラクティスに関するタイムリーで重要な分野が扱われ、オーディエンスのニーズに合わせてカスタマイズされたライブ ハイブリッド配信モデルが使用されています。

プログラム固有 : シャドー IT、インサイダーの脅威、Microsoft Federal など、特定のサイバーセキュリティ イニシアチブをサポートするターゲットを絞ったトレーニング プログラム。これらのプログラムは、「ボックスをチェックする (Check-The-Box)」トレーニング アプローチを防ぐため、エグゼクティブ スポンサーシップとスコアカード レポートを通じて、各サイバーセキュリティ イニシアチブの全体的なエンゲージメント戦略に緊密に統合されており、

MSProtect: サイバーセキュリティ関連のあらゆる事柄について、ベスト プラクティス、会社のポリシー情報、インシデント レポートを提供するマイクロソフトの一元化された Web リソース。このオンデマンド リソースは、正式なトレーニング プログラムの外で社員が利用できます。

セキュリティのスキル向上は、コンプライアンスの Check-The-Box アクティビティと見なすべきではありません。むしろ、行動の変化に焦点を当てて、特定されたターゲットの行動に関する結果を監視し、プログラムの効果を判断するリスニング システムを確立してください。

実用的なインサイト

1. セキュリティ トレーニングとリソースを、必要なときに必要な場所で社員に提供します。
2. 社内全体のステークホルダーからの情報に基づいた一元化されたスキル向上戦略を策定します。
3. 効率 (量)、有効性 (質)、結果 (ビジネスへの影響) に関する、トレーニングの効果を追跡して分析します。

詳しい情報のリンク

- マイクロソフトは、3,000 万人の社員を支援するスキル イニシアチブの次の段階に進む

ランサムウェア除去プログラムから得られたインサイト

マイクロソフトは、ID とデバイスが確実に管理され、正常な状態に維持されるように、過去 5 年間に独自のゼロ トラストの取り組み[13] を行ってきました。ランサムウェアのリスクが高まるにつれて、自社とお客様を保護するアプローチをサポートする深い視点を育成してきました。

マイクロソフトは、詳細な内部評価の後、制御と範囲のギャップのギャップを修正するランサムウェア除去プログラムを構築し、Defender for Endpoint、Azure、M365 などのサービスの機能強化を行って、ランサムウェア攻撃が発生した場合の復旧方法について、SOC およびエンジニアリング チーム向けのプレイブックを作成しました。

最初のステップは、マイクロソフトを標的としたランサムウェア攻撃に対するマイクロソフトの保護の範囲を把握することでした。Defender for Endpoint を展開し、すべてのデバイスを管理してゼロ トラスト信頼ポリシーに準拠するための取り組みは既に順調に進められていましたが、攻撃から効果的に回復できるかという大きな疑問のあらゆる側面を把握する方法を見つける必要がありました。インサイトを得るため、NIST 8374: ランサムウェア リスク管理 : サイバーセキュリティ フレームワーク (CSF) プロファイル[14] を評価しました。このプロファイルは、既知のコントロール リストに対するマイクロソフトのエンタープライズ ポリシーに沿っています。この分析により、範囲のギャップがすぐに特定されました。

次に、CSF の機能の識別、検出、保護、対応、回復に存在するギャップを優先しました。ゼロ トラストと他のプログラムに対する戦略的な連携を見出し、既存のワークストリームが存在していなかったギャップも発見しました。これらのギャップを修正するのに必要な作業と労力の量を評価し、2 つの柱に分けました。

- **エンタープライズの保護 (PtE):** 企業として自社を保護し、攻撃が成功した場合はそこから回復できるようにするために必要な作業項目を定義します。
- **お客様の保護 (PtC):** お客様とマイクロソフトのビジネスを保護するため、マイクロソフトのサービスに機能を組み込みます。

自社への調査結果の組み込み

上位のリスクを緩和し、重要なサービスをランサムウェア攻撃から保護するため、マイクロソフトは今後 6 ～ 12 か月間、専用のランサムウェア プログラムの一部として、次の 5 つのシナリオの達成に投資する予定です。各シナリオに成功したら、プログラムの範囲を徐々に拡大し、社内のすべての部分まで広げます。

シナリオ 1: セキュリティ チームのメンバーが、ランサムウェア攻撃に伴うリスク全体を把握し、制御上のギャップやリスクの状況について、経営陣に認識を提供するプロセスを確立している。

シナリオ 2: セキュリティ チームのメンバーが、自分たちとマイクロソフト内の他のチームがランサムウェア攻撃に対応して重要なサービスを回復できるようにするために用意されたプレイブックにアクセスできる。

シナリオ 3: エンタープライズ レジリエンス チームのメンバーが、重要なシステムのバックアップを行うために従うべき基準を持っている。プレイブックが存在しており、ランサムウェア攻撃が発生した場合にデータを確実に回復できるように、バックアップと回復の定期的な演習が実施される。

シナリオ 4: サービス所有者が、マイクロソフトの重要なサービスとして優先順位が付けられたサービスに特に重点を置き、ランサムウェア攻撃からサービス、お客様のデータ、エンドポイント、ネットワーク資産を保護するのに必要なセキュリティおよび運用コントロールとポリシーを理解して導入している。

シナリオ 5: すべての社員が、ランサムウェア攻撃を認識する方法と、セキュリティ チームに知らせて対応を開始する方法について説明された、教育およびトレーニング リソースにアクセスできる。

実用的なインサイト

1. 重要なサービスに対するランサムウェア攻撃に関連する、エンド ツー エンドの復旧および修復アクティビティを文書化して検証します。
2. ステークホルダーにエンタープライズ危機管理プレイブックの更新に加わってもらい、ランサムウェア固有のアクティビティと、ランサムウェアに身代金を支払うかどうかを判断するための意思決定プロセスとガイダンスを追加します。
3. 展開されたセキュリティ製品で利用可能な機能を有効にすることで、検出と保護の適用範囲を広げます (例 : Defender for Endpoint の攻撃対象領域の縮小ルール)。
4. ランサムウェア攻撃から保護するためのベースラインを定義し、ランサムウェア攻撃から保護する方法に関するトレーニングとドキュメントをエンジニアリング チームに提供する点で、セキュリティ標準チームと協力します。
5. 自動化を導入して、DevOps チームのセキュリティおよび運用ポリシーの展開をより簡単にし、システムがコンプライアンスから逸脱した場合にすばやくフラグを付けて修正されるようにします。

詳しい情報のリンク

- マイクロソフトがランサムウェアから保護している方法を共有する | Microsoft Inside Track

量子セキュリティの影響に対してすぐに行動を取る

現在の暗号とそれによって保護されているすべてのデータに対して、量子コンピューティングがもたらす脅威に対処するプレッシャーが高まっています。最近発行された「Memorandum on Improving the Cybersecurity of National Security Department of Defense and Intelligence Community Systems」[15] は、米国の国家サイバーセキュリティの改善に関する大統領令 (EO 10428)[16] に基づいており、今後の国家レベルの攻撃に対処するため、ソフトウェア サプライ チェーンのセキュリティを重要なものとして強調しています。

量子コンピューターとは

量子コンピューターは、量子物理学の特性を利用してデータを保存し、計算を行うコンピューターです。特定のタスクにメリットがあり、最高のスーパーコンピューターよりもパフォーマンスが大幅に高くなる可能性があります。量子コンピューティングは、既にデータの暗号化と処理にとって新たな境地を開いています。調査によると、量子コンピューティングの量子業界は、早ければ 2030 年に数十億ドル (米ドル) 規模になると予測されています。[17] 事実、量子コンピューティングと量子通信は、医療やエネルギー、金融、セキュリティに至るまで、さまざまな業界に革新的な影響をもたらすと思われます。

量子コンピューティングは、現在の暗号とそれによって保護されているすべてのデータにとって脅威です。

現在の暗号に対する脅威

1994 年のショアのアルゴリズムと、数百万の物理量子ビットを搭載した産業規模の量子コンピューターを使って、現在広く展開されている公開鍵暗号アルゴリズムが効率的に突破されました。攻撃者による量子ベースの攻撃に対して効率的かつアジャイルで安全な「量子セーフ」暗号システムを検討、評価、標準化することが重要です。「ポスト量子暗号」(つまり、量子攻撃に強い既存の古典的なアルゴリズムとプロトコル) にソフトウェアを移行するには、実現するまでに何年も (10 年以上でなければ) かかります。[18]

これは、現在の暗号とそれによって保護されているすべてのデータに対する脅威に対処するプレッシャーが高まっていることを意味します。攻撃者は、暗号化されたデータをすぐに記録し、後で量子コンピューターが利用可能になったら悪用することができます。暗号の影響に対処するまで量子コンピューティングの攻撃を待っているのでは遅すぎます。

暗号はサイバー エコシステム全体で使用されているため、暗号ベースのセキュリティ サービスが侵害される可能性があります。たとえば、通信用サービス (TLS、IPSec)、メッセージング (メール、Web 会議)、ID およびアクセス管理、Web ブラウジング、コード署名、支払いトランザクション、保護のための暗号に依存する他のサービスが含まれます。

量子コンピューターが現実になると、暗号アルゴリズムと機能の実装を含むサードパーティのソフトウェア コンポーネントも、さらに精査が必要となります。これには、バリュー チェーンに含まれるすべての組織がその役割を担い、チェーンをしっかり保護する必要があります。業界の組織や政府は、ソフトウェア サプライ チェーンのセキュリティ要件を定義する取り組みを強化しており、場合によってはチェーンを保護するための新しい規制を導入しています。National Security Memorandum NSM-8[19] は、国家安全保障システム (NSS) におけるポスト量子暗号を実装するための要件とタイムラインを定めています。「最新化計画、サポートされていない暗号化の使用、承認済みのミッション固有のプロトコル、量子耐性のあるプロトコル、必要に応じて量子耐性のある暗号を使用する計画」について、期待される時間を 180 日以内と定義しています。

標準化は、量子セーフ暗号への移行におけるリードタイムの長い活動です。公開鍵暗号を使用した標準を扱っている標準化団体は、ポスト量子アルゴリズムの試験と適応を今すぐ開始する必要があります。

新しいポスト量子暗号 (PQC) アルゴリズム (量子攻撃に対して強いと考えられている古典的なアルゴリズム) は、NIST のポスト量子標準化プロジェクトを通じて検討中です。[20] この作業は、標準化団体内の世界的な取り組みに影響を及ぼします。米国政府が選択したアルゴリズムと重複するものもありますが、選択される準拠アルゴリズムが国家 / 規制ごとに異なるため、国際的な課題が生じる可能性があります。この分断化によって、製品とサービスのエンジニアリングが複雑になります。

新たなポスト量子暗号アルゴリズムは、NIST のポスト量子暗号標準化プログラムを通じて検討中です。この作業は、標準化団体内の世界的な取り組みに影響を及ぼします。

実用的なインサイト

業界は、PQC 移行に備えるため、SAFECode や提携メンバーと一緒に短期的な活動をすぐに行う必要があります。[21] たとえば、次のとおりです。

1. 暗号を使用する製品 / コードの在庫を取得します。
2. 暗号が変更されたときに必要なコード チャーンを最小限に抑えることができる、暗号アジリティ戦略を組織全体で実装します。
3. 暗号を使用する製品またはサービスで、量子セーフ アルゴリズム候補の使用をパイロット展開します。
4. 暗号化、キー交換、署名に異なる公開鍵アルゴリズムを使用する準備を行います。
5. アプリケーションをテストし、非常に大きなキー サイズ、暗号、署名の影響を確認します。

詳しい情報のリンク

- マイクロソフトは新しい種類の量子ビットを作成するのに必要な基盤となる物理学を実証した | Microsoft Research

ビジネス、セキュリティ、IT を統合してより高いレジリエンスを実現する

堅牢なサイバー レジリエンスを実現するには、ビジネス リーダーがセキュリティ チームと連携してセキュリティを実装する必要があります。マイクロソフトの経験によると、セキュリティ リーダーシップは、最も効果的に企業を保護するには組織のリーダーからのサポートを必要とする難しい分野です。

セキュリティ リーダーは、リスク、テクノロジ、経済学、組織プロセス、ビジネス モデル、文化の変革、地政学的利益、スパイ活動、国際制裁コンプライアンスに関連するトピックにまたがる、変化の激しいさまざまな課題を取り扱っています。それぞれに理解して細かく管理すべきニュアンスがあります。

さらに、セキュリティ リーダーには、インテリジェントで資金豊富かつ意欲的な人間の攻撃者と、スキルが低いものの効果的なサイバー犯罪者の両方を阻止する任務があります。そのチームは、セキュリティの優先順位が低いか存在していなかった 30 年以上前から段階的に構築されてきた複雑な技術資産を防御する必要があります。何年も前に行われた意思決定は、技術的な負債を清算してセキュリティのギャップに対処しなければ、今はリスクとなる可能性があります。

組織のリーダーや政策立案者は、セキュリティ リーダーを積極的にサポートし、統合されたセキュリティと組織の他の部門を橋渡しできるようにすることで、セキュリティに大きなプラスの影響を及ぼすことができます。このような連携を実現しているお客様とマイクロソフトが協力すれば、よりレジリエンスのある組織を構築し、アジリティとイノベーションを強化することができます。

組織のリーダーシップは、次の 3 つの主要分野に重点を置いてセキュリティ リーダーをサポートできます。

1. セキュリティを意図的に構築する

セキュリティは、ビジネス プロセスでは障害や補足と見なされることがあります。多くの場合、リスクを回避したり、コストをかけずに簡単に修正したりするには遅すぎるときになって初めて、意思決定が考慮されます。

組織のリーダーと政策立案者は、次の点を確認する必要があります。

新しいイニシアチブの早い段階でセキュリティを組み込みます。新しいデジタル イニシアチブとクラウドの導入時は、セキュリティを優先し、新しいアプリケーションやデジタル機能によって組織のリスクが高まらないようにする必要があります。セキュリティが確実に組み込まれたら、それらのプロセスを使ってレガシー システムを最新化し、セキュリティと生産性の両方を同時に高めることができます。

セキュリティの予防保守を正規化します。セキュリティ更新プログラムや修正プログラムの適用、構成の保護など、基本的なセキュリティ メンテナンスを組織全体がサポートするようにします (予算、計画されたダウンタイム、ベンダー製品サポートの取得要件など)。

残念ながら、多くの組織はこれらの一般的なプラクティスを遅らせたり、部分的にのみ適用したりしています。その結果、攻撃者が悪用する可能性が高まります。セキュリティの正規化の必要性は、米国の NIST 800-40 に記載されています。[22]

2. セキュリティに関与する

組織のリーダーは、リソースの優先順位付けとセキュリティ障害への備えを行うため、重要なセキュリティ プロセスに積極的に参加して支援する必要があります。これには、以下のことが含まれます。

重要なビジネス資産を特定します。セキュリティ リーダーとチームは、ビジネス クリティカルな資産を把握し、セキュリティ リソースを最も重要なものに集中させる必要があります。これは多くの場合、それまで対処したことのない新しい質問について考え、答えを見つける新しい形の練習です。

サイバーセキュリティにおけるビジネス継続性と障害復旧の練習。サイバー攻撃は、事業運営の大部分または全体を中断させたり停止させたりする重大なイベントになる可能性があります。組織全体のチームがこの状況に対応できるよう備えることにより、事業運営の復旧にかかる時間が短縮され、組織の損害が小さくなり、顧客、市民、有権者からの信頼を維持することができます。これは、既存のビジネス継続性と障害復旧プロセス内に統合してください。

セキュリティ リスクに関する決定は、すべてのリスクと機会を十分に把握しているビジネス オーナーまたはミッション オーナーが行うのが最善です。

ビジネス、セキュリティ、IT を統合してより高いレジリエンスを実現する

(続き)

3. セキュリティを適切に位置づける

組織がセキュリティ リスクの説明責任を構成する方法は多くの場合、セキュリティ リスクに関する意思決定が適切でない場合に影響を与えます。リスクに関する意思決定は、あらゆるリスクと機会を十分に把握しているビジネス オーナーまたはミッション オーナーが行うのが最善ですが、組織はセキュリティ リスクの説明責任をセキュリティ チームの専門家に割り当てる (暗黙的または明示的に) ことがよくあります。そうすると、セキュリティ チームにとって大きな負担となる一方、ビジネス オーナーがビジネスにとって重要なリスクを把握および制御できなくなります。組織は、次の方法でこれを解決できます。

ビジネス オーナーを備えさせる : セキュリティ リスク全体について、それらの脅威がビジネスに及ぼす影響について、ビジネス オーナーに教育を行います。この取り組みにセキュリティ チームを直接関与させることで、セキュリティと全体的なビジネス アジリティの協調関係も向上します。

セキュリティ リスクをビジネス オーナーに割り当てる : ビジネス オーナーがセキュリティ リスクを把握して受け入れるのに十分な情報を得たら、組織はセキュリティ リスクの説明責任を明示的にビジネス オーナーに移行すると同時に、そのリスクを管理し、情報に基づく専門知識とガイダンスをオーナーに提供する責任はセキュリティ チームに維持する必要があります。

「サイバー レジリエンスは、従来のビジネス継続と障害復旧からスライド式で構築されます。まず、優れたデータ バックアップから始め、プロセス、テクノロジ、およびその依存関係 (人物やサードパーティなど) の復旧機能に移ります。その後、常時オン、セルフ ヒーリング サービス、重要な役割のレジリエンス、重要なサードパーティのフェールオーバーへと進みます。最もレジリエンスの高い組織は、IT、ビジネス マネージャー、セキュリティ担当者間の統合を促進します。高いレジリエンスには、最初からのレジリエンス設計、安全な変更管理、細かい障害切り分けなどが含まれます。サイバー レジリエンスは、優れたオール ハザード計画プログラムの 1 つのシナリオに過ぎません。サイバー リスクが増加し、サイバーセキュリティとレジリエンスの関わりがより重要になるにつれて、最高情報セキュリティ責任者 (CISO) とエンタープライズ レジリエンス プログラムとのつながりが強くなっていきます。全社規模のレジリエンスを主導する CISO が年々増えています。」

Lisa Reshaur
ゼネラル マネージャー、リスク管理、マイクロソフト

詳しい情報のリンク

- レジリエンスからデジタルへの忍耐 : デジタル テクノロジを使って前例のない時代の危機を脱する方法 | マイクロソフト公式ブログ
- IT およびセキュリティ チームが連携してエンドポイント セキュリティを向上させる方法 | Microsoft Security

サイバー レジリエンスの正規分布

あらゆる組織が採用すべきレジリエンスの成功要因

これまで見てきたように、基本的なセキュリティ対策が守られていないため、多くのサイバー攻撃が成功を収めています。あらゆる組織が採用すべき最小限の基準は次のとおりです。

- **多要素認証 (MFA) を有効にする：**侵害されたユーザー パスワードから保護し、ID のレジリエンスを高めます。
- **ゼロ トラストの原則を適用する：**組織への影響を軽減するレジリエンス計画の基礎。原則は次のとおりです。

1 – 明示的に検証する—リソースへのアクセスを許可する前に、ユーザーとデバイスの状態が良好であることを確認します。

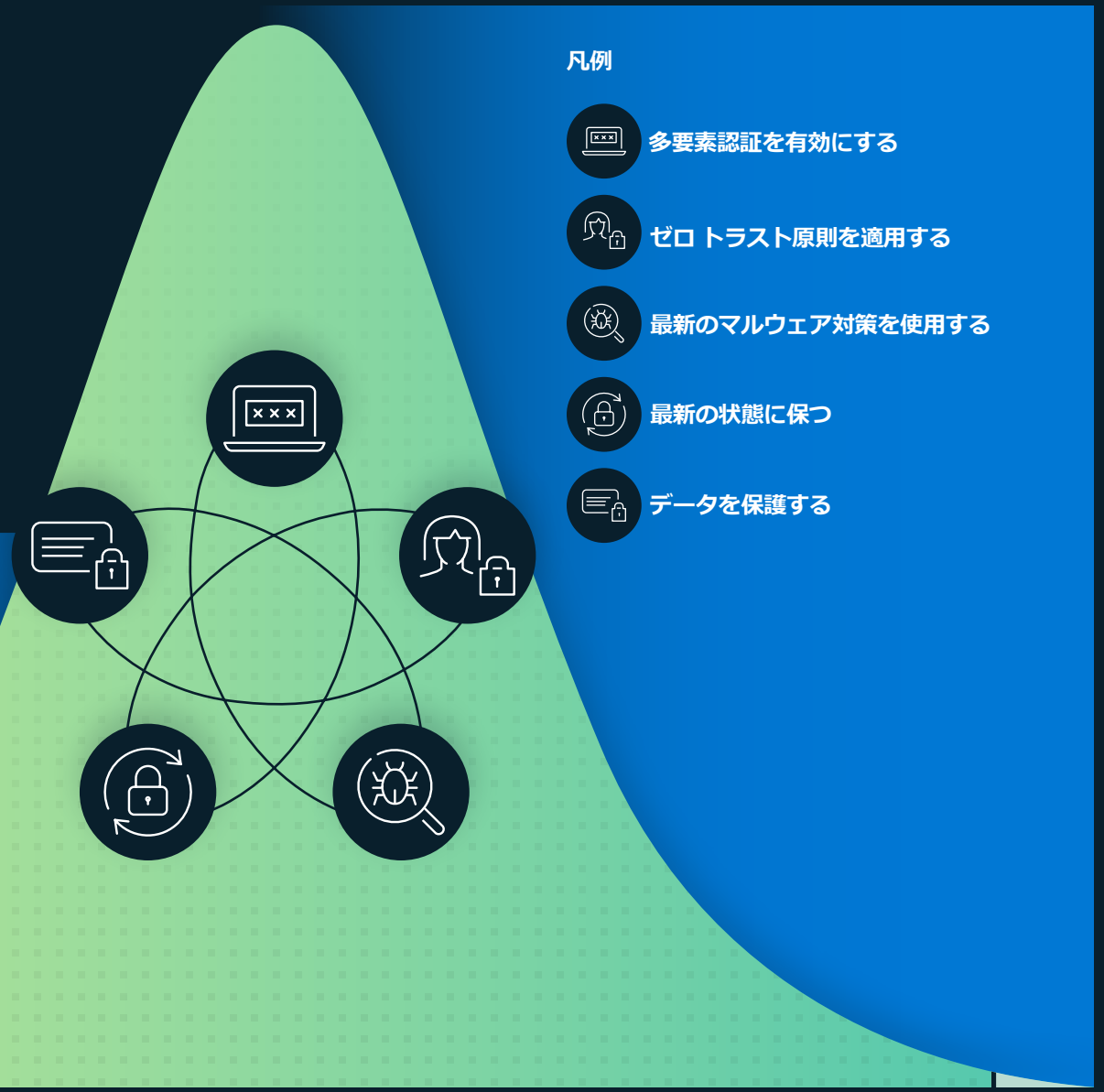
2 – 最小特権アクセスを使用する—リソースへのアクセスに必要な特権のみ許可し、それ以上は許可しません。

3 – 侵害を想定する—システムの防御が破られ、システムが侵害される可能性があることを想定します。これは、攻撃を受ける可能性がある環境を絶えず監視することを意味します。

- **拡張検出および応答マルウェア対策を使用する：**攻撃を検出して自動的にブロックし、セキュリティ操作に関するインサイトを提供するソフトウェアを実装します。脅威検出システムからのインサイトを監視することは、脅威にすばやく対応するために不可欠です。
- **最新の状態に維持する：**修正プログラムが適用されていない古いシステムは、多くの組織が攻撃の被害を受けている主な理由になっています。ファームウェア、オペレーティング システム、アプリケーションなど、すべてのシステムが最新の状態に保たれていることを確認します。
- **データを保護する：**重要なデータとそれ存在する場所、適切なシステムが実装されているかどうかを把握することは、適切な保護を実施するうえで非常に重要です。

98%

基本的なセキュリティ対策は依然として 98% の攻撃から保護できます。



巻末注

1. エンドポイント検出および対応 (EDR) は、企業ネットワークで高度な脅威に対する防止、検出、調査、対応を行えるように設計された、エンタープライズ エンドポイント セキュリティ プラットフォームです。エンドポイント検出および対応機能によって、ほぼリアルタイムで実用的な、高度な攻撃検出が実現します。セキュリティ アナリストは、アラートの優先順位を効果的に設定し、侵害の全範囲の可視性を得て、脅威を修復するための対応策を講じることができます。
2. エンドポイント保護プラットフォーム (EPP) は、エンドポイント デバイス上に展開されるソリューションであり、ファイルベースのマルウェアを阻止し、信頼されていないアプリケーションからの悪意のあるアクティビティを検出してブロックします。また、セキュリティ インシデントやアラートに動的に対応するのに必要な調査および修復機能を提供します。
3. https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted
4. https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match
5. https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-additional-context
6. Windows Security Book: Commercial
7. Windows 11 の新しいセキュリティ機能はハイブリッド ワークを保護するのに役立つ | マイクロソフト セキュリティブログ
8. FIDO Alliance: Open Authentication Standards More Secure than Passwords
9. https://interpret.ml/
10. OWASP Top Ten | OWASP Foundation
11. https://blogs.microsoft.com/on-the-issues/2022/05/03/artificial-intelligence-department-of-defense-cyber-missions/
12. https://www.kaspersky.com/blog/the-human-factor-in-it-security/
13. https://aka.ms/ZTatMSFT
14. https://csrc.nist.gov/publications/detail/nistir/8374/final
15. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/
16. 米国の国家サイバーセキュリティの改善に関する大統領令 14028
17. https://thequantumdaily.com/2020/02/18/the-quantum-computing-market-size-superpositioned-for-growth
18. 「The Long Road Ahead to Transition to Post-Quantum Cryptography」、https://cacm.acm.org/magazines/2022/1/257440-the-long-road-ahead-to-transition-to-post-quantum-cryptography/fulltext
19. https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/
20. https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization
21. https://safecode.org/blog/preparing-for-post-quantum-cryptography-roadmap-initial-guidance/
22. https://csrc.nist.gov/publications/detail/sp/800-40/rev-4/final

作成チーム

作成チーム

このレポートのデータとインサイトは、セキュリティを重視するさまざまな専門家のグループによって提供されており、マイクロソフトのさまざまなチームが関わっています。このレポートの目標は、サイバー攻撃の脅威からマイクロソフト、そのお客様、そして全世界を保護することです。マイクロソフトでは、透明性を重視し、世界をすべての人にとってより安全な場所にするという共通の目標を掲げて、さまざまなインサイトを皆様に提供しています。

AI for Good Research Lab: データと AI を活用して、世界の多くの課題に対処しています。このラボでは、マイクロソフト外の組織と連携し、AI を活用して生活と環境を改善しています。重点を置いている分野には、オンラインの安全性 (偽情報、サイバーセキュリティ、子供の安全)、災害対応、持続可能性、AI for Health などがあります。

Azure Edge & Platform、Enterprise & OS Security: Windows、Azure、および他のマイクロソフト製品にわたるコア OS とプラットフォームのセキュリティを担当しています。このチームは、業界をリードするセキュリティおよびハードウェア ソリューションをマイクロソフト プラットフォームに組み込み、チップからクラウドまで悪用、ID、マルウェアによる侵害を軽減しています。PC、エッジ、サーバー、Microsoft Pluton セキュリティ プロセッサなどにまたがる、マイクロソフトのセキュア コア プラットフォームのクリエイターたちです。

Azure ネットワーク コア : Microsoft WAN、データ センター ネットワーク、および DDoS プラットフォーム、ネットワーク エッジ プラットフォーム、ネットワーク セキュリティ製品 (Azure WAF、Azure Firewall、Azure DDoS Protection Standard など) など、Azure のソフトウェア定義のネットワーク インフラに重点を置くクラウド ネットワーキング チーム。

クラウド セキュリティ調査チーム : このチームは、マイクロソフト クラウドを保護し、革新的なセキュリティ機能と製品を構築し、調査を実施することにより、マイクロソフトのお客様を保護し、組織を安全に変革しています。

Customer Security and Trust (CST): マイクロソフトの製品とオンライン サービスでのお客様のセキュリティの改善を継続的に進めているチーム。CST は、会社のエンジニアリング チームおよびセキュリティ チームと協力して、コンプライアンスを確保し、セキュリティと透明性を強化して、お客様を保護すると共に、全世界でのマイクロソフトへの信頼を促進しています。

カスタマー サクセス : カスタマー サクセスのセキュリティ チームは、お客様と直接連携し、ベスト プラクティス、得られた教訓、ガイダンスを共有して、セキュリティの変革と最新化を加速させています。このチームは、マイクロソフト (およびお客様) の取り組みから得られたベスト プラクティスと教訓を、リファレンス戦略、リファレンス アーキテクチャ、リファレンス計画などにまとめて整理しています。

Cyber Defense Operations Center (CDOC): マイクロソフトの企業インフラとお客様がアクセスできるクラウド インフラを保護するために、企業全体のセキュリティ専門家を結集した、サイバーセキュリティと防衛のための施設。インシデント対応担当者は、マイクロソフトの各種サービス、製品、デバイス グループに所属するデータ サイエンティストやセキュリティ エンジニアと共に、24 時間年中無休体制で脅威に対する保護、検出、対処を支援しています。

民主主義推進イニシアチブ : 健全な情報エコシステムを推進し、オープンで安全な民主的プロセスを保護して、企業の市民としての責務を擁護することにより、民主主義の基盤を維持、保護、推進しているマイクロソフトのチーム。

デジタル犯罪対策ユニット (DCU): テクノロジ、フォレンジック、民事訴訟、刑事告発、官民の両方のパートナーシップを利用して、世界規模でサイバー犯罪に対抗することに専念している弁護士、捜査官、データ サイエンティスト、エンジニア、アナリスト、ビジネス プロフェッショナルのチーム。

Digital Diplomacy: 増加する国家間の対立に立ち向かって、平和的で安定した安全なサイバースペースを推進している元外交官、政策立案者、法務専門家の国際的なチーム。

Digital Security & Resilience (DSR): 企業の安全を確保しながら、最も信頼性の高いデバイスとサービスを構築し、マイクロソフトとお客様のデータの両方を保護することを目的とした組織。

Digital Security Unit (DSU): マイクロソフトとそのお客様を保護するため、法的、地政学的、技術的な専門知識を提供するサイバーセキュリティ専門の弁護士およびアナリストのチーム。DSU は、世界中の高度なサイバー攻撃者に対するマイクロソフトのエンタープライズ セキュリティ防御に対する信頼を築き上げています。

デジタル脅威分析センター (DTAC): サイバー攻撃や影響工作など、国家レベルの脅威を分析して報告する専門家チーム。このチームは、情報とサイバー脅威インテリジェンスを地政学的分析と組み合わせて、お客様とマイクロソフトにインサイトを提供し、効果的な対応と保護の方法に関する情報を知らせています。

Enterprise and Security: インテリジェントなクラウドとインテリジェントなエッジのための、最新かつ安全で管理可能なプラットフォームを提供することに重点を置いているチーム。

Enterprise Mobility: クラウドとオンプレミスで最新の職場環境と最新の管理機能を実現し、データの安全を確保するチーム。エンドポイント マネージャーには、モバイル デバイス、デスクトップ コンピューター、仮想マシン、埋め込みデバイス、サーバーの管理および監視にマイクロソフトとお客様が使用するサービスとツールが含まれています。

作成チーム

(続き)

エンタープライズ リスク管理 : マイクロソフトのシニア リーダーシップによりリスクに関する議論の優先順位付けを行う、ビジネス部門全体に関与するチーム。ERM は、複数のオペレーショナル リスク チームを結び付けて、マイクロソフトのエンタープライズ リスク フレームワークを管理し、NIST Cybersecurity Framework を使って社内のセキュリティ評価を促進します。

グローバル サイバーセキュリティ ポリシー : 政府、NGO、業界パートナーと協力して、サイバーセキュリティの公共政策を推進するチーム。マイクロソフト テクノロジを採用するお客様のためのセキュリティと回復性の向上を図っています。

ID およびネットワーク アクセス (IDNA) セキュリティ : マイクロソフトすべてのお客様を不正なアクセスや詐欺から保護することに取り組んでいるチーム。IDNA Security は、エンジニア、製品マネージャー、データ サイエンティスト、セキュリティ調査担当者で構成されるの分野横断的なチームです。

M365 セキュリティ : 企業のお客様を保護するた め、Microsoft Defender for Endpoint (MDE)、Microsoft Defender for Identity (MDI) などのセキュリティ ソリューションを開発している組織。

Microsoft AI, Ethics and Effects in Engineering and Research (AETHER): 新しいテクノロジの開発と提供を責任ある方法で確実に行うことを使命としているマイクロソフトの諮問委員会。

Microsoft Bing Search and Distribution: 世界クラスのインターネット検索エンジンを提供するチーム。トピックの追跡や、自分にとって重要なテーマのトレンド化、ユーザーによるプライバシーの管理など、世界中のユーザーが信頼できる検索結果と情報をすばやく見つけることができるようにしています。

マイクロソフトのお客様とパートナー向けソリューション : マイクロソフトの統合企業市場開拓組織であり、セキュリティ、テクニカル セールス スペシャリスト、アドバイザーなどのお客様対応を担っています。

Microsoft Defender Experts: 製品に焦点を当てたセキュリティ研究者、応用科学者、脅威インテリジェンス アナリストから成るマイクロソフト最大のグローバル組織。Defender Experts は、Microsoft 365 セキュリティ製品と Microsoft Defender Experts マネージド サービスで革新的な検出および対応機能を提供しています。

Microsoft Defender for IoT: IoT/OT のマルウェア、プロトコル、ファームウェアのリバースエンジニアリングに特化した、ドメイン エキスパートの研究者で構成されるチーム。このチームは、悪意のある傾向やキャンペーンを明らかにするため、IoT/OT の脅威を調査しています。

Microsoft Defender 脅威インテリジェンス (RiskIQ): マイクロソフトの広範な外部テレメトリ コレクションの分析を通じて戦術的なインテリジェンスを生み出すチーム。未知の脅威インフラを発見できるように脅威の状況をグラフ化したり、脅威アクターやキャンペーンにコンテキストを追加したりしています。このチームは、重要な戦術インテリジェンスを防御者に提供するため、タイムリーな独特調査を定期的に公開しています。

Microsoft Security Business Development Team: マイクロソフトのサイバーセキュリティ成長戦略、パートナーシップ、戦略的投資をリードするチーム。

マイクロソフト セキュリティ レスポンス センター (MSRC): マイクロソフトのお客様とパートナー エコシステムを保護することに取り組んでいるセキュリティ研究者と協力するチーム。Microsoft Cyber Defense Operations Center (CDOC) に不可欠な部分として、MSRC は、セキュリティ対応の専門家を募り、脅威をリアルタイムで検出および対応しています。

Microsoft Security Services for Incident Response: 調査から封じ込めおよび復旧関連活動まで、サイバー攻撃全体を通じてお客様を支援するサイバーセキュリティ専門家のチーム。このサービスは、2 つの高度に統合されたチームを通じて提供されます。復旧のための調査と基盤に重点を置く Detection and Response Team (DART)、封じ込めと復旧の側面に重点を置く Compromise Recovery Security Practice (CRSP) です。

Microsoft Threat Intelligence Center (MSTIC): 国家レベルの脅威、マルウェア、フィッシングなど、マイクロソフトのお客様に影響を与える、特に巧妙化な攻撃者に関連するインテリジェンスの特定、追跡、収集に取り組むチーム。

One Engineering System (1ES): マイクロソフトの開発者が可能な限り生産性とセキュリティを向上できるように、世界クラスのツールを提供する使命を持つチーム。このチームは、マイクロソフトのエンドツーエンドのソフトウェア サプライ チェーンを保護するための中心的な戦略をリードしています。

Operational Threat Intelligence Center (OpTIC): Microsoft Cyber Defense Operation Center (CDOC) の使命をサポートしてマイクロソフトとお客様を保護する、サイバー脅威インテリジェンスの管理と普及を担当するチーム。

Microsoft

脅威の状況を明確に示し、デジタル防衛の強化方法を提示する

- 詳細情報 : https://microsoft.com/mddr
- 深く掘り下げる : https://blogs.microsoft.com/on-the-issues/
- 最新情報を入手 : @msftissues and @msftsecurity